



3Com Router Configuration Guide

<http://www.3com.com/>

Published March 2004
Part No. 10014299

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

Copyright © 2004, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

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.

GETTING STARTED 1

SYSTEM MANAGEMENT 33

INTERFACE 121

LINK LAYER PROTOCOL 183

NETWORK PROTOCOL 335

ROUTING 423

MULTICAST 517

SECURITY 543

VPN 615

RELIABILITY 665

QoS 681

DIAL-UP 721

ABOUT THIS GUIDE

This guide describes 3Com routers and how to configure them.

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

Table 2 Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+), for example: Press Ctrl+Alt+Del
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
Words in <i>italics</i>	Italics are used to: Emphasize a point. Denote a new term at the place where it is defined in the text. Identify command variables. Identify menu names, menu commands, and software button names. Examples: From the <i>Help</i> menu, select <i>Contents</i> . Click <i>OK</i> .
Words in bold	Boldface type is used to highlight command names. For example, "Use the display user-interface command to..."





GETTING STARTED

Chapter 1 3Com Router Introduction

Chapter 2 3Com Router User Interface

1

3COM ROUTER INTRODUCTION

This chapter includes information on the following topics:

- Overview of the 3Com Router System
- Architecture of the 3Com Router
- Features of the 3Com Router Version 1.10
- New Features of the 3Com Router 1.x

Overview of the 3Com Router System

The 3Com Router OS is the network operating system platform. With TCP/IP protocol stack as the core, the 3Com Router integrates data communication essentials such as routing technology, multicast technology, QoS technology, VPN technology, security technology in the operating system and provides excellent data transmission capability.

The 3Com Router can run on multiple hardware platforms with consistent network interface, user interface and management interface, providing flexible and multiple application solutions for users.



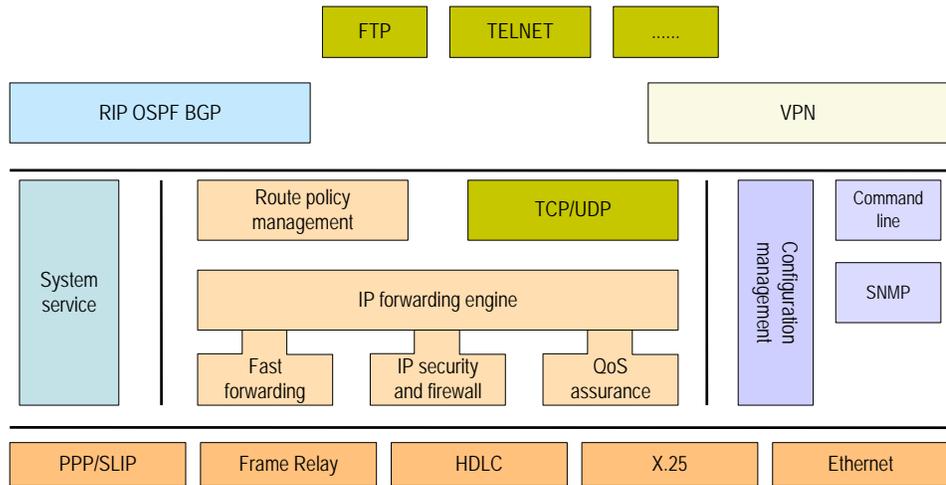
This manual describes features and functions of the 3Com Router 1.x system software platform series of low end and middle range routers. In this manual the 3Com Router is also referred to as the 3Com Router 1.x software version. You should make sure that the 3Com Router you use is operating with the software version documented in this manual.

The software specification is different between various types of products. Product specification related matters should be confirmed with the 3Com Technical Support Department.

Architecture of the 3Com Router

With TCP/IP model as its reference, the 3Com Router implements data link layer, network layer, and application layer protocols, as per the architecture shown in the following diagram:

Figure 1 Schematic diagram of the 3Com Router architecture



Features of the 3Com Router Version 1.10

The following table lists the basic features of the 3Com Router 1.x:

Table 3 List of the 3Com Router 1.x features

Attribute	Description
Interconnection protocol	LAN <ul style="list-style-type: none"> ■ Supports Ethernet_II and Ethernet_SNAP frame structure ■ Follows IEEE 802.2 and IEEE 802.3 regulations
	WAN <ul style="list-style-type: none"> ■ Supports Frame Relay and Frame Relay switching ■ Supports FRoIP, FRoISDN ■ Supports Multi-link Frame Relay (MFR), FR compression ■ Supports FR Traffic Shaping (FRTS) to ensure even traffic over the VCs on FR ■ Supports X.25 and X.25 switching, X.25 Over TCP (XOT) ■ Supports HDLC, SDLC and LAPB regulations ■ Supports SLIP, PPP and MP ■ Supports PPPoE Client ■ Supports ITU-T Q.921 and Q.931 regulations, ISDN (ITU-T Q.921, Q.931) and ISDN semi-permanent connection ■ Supports bridging technology
	Dial-up network <ul style="list-style-type: none"> ■ Manages Modem through the AT command and configures script to dial up. ■ Supports dial demand Routing (dialer profiles and legacy BDR) ■ Supports Callback (PPP callback and ISDN Calling Line Identification callback) ■ Provides ISDN leased line, automatic dialing, and cyclic dial queue backup ■ Provides Dial interface backup
	VPN <ul style="list-style-type: none"> ■ Supports L2TP, implements VPDN (Supports DNIS user, domain name user, and full name user) ■ Supports L3 channel protocol GRE

Attribute	Description	
Network protocol	IP service	<ul style="list-style-type: none"> ■ Supports ARP ■ Supports Static domain name resolution ■ Supports IP Address Unnumbered ■ Supports DHCP Server and DHCP relay ■ Supports VLAN ■ Supports IP Accounting
	Non-IP service	<ul style="list-style-type: none"> ■ Supports Novell IPX protocol, provide RIP and SAP to maintain the database of Internetwork routes and service information ■ Supports DLSw of SNA system, implementing SNA through WAN transmission
	IP performance	<ul style="list-style-type: none"> ■ Supports IP fast forwarding ■ Supports Van Jacobson TCP message header compression
	IP routing	<ul style="list-style-type: none"> ■ Supports Static route management ■ Supports Dynamic route protocol ■ RIP-1/RIP-2 ■ OSPF ■ BGP ■ Supports IP routing policy ■ Supports IP policy-based routing
	Multicast routing	<ul style="list-style-type: none"> ■ Supports Internet Group Management Protocol (IGMP) ■ Supports Multicast routing protocol ■ PIM-DM ■ PIM-SM

Attribute	Description	
Network security	Authentication, Authorization and Accounting (AAA) service	<ul style="list-style-type: none"> ■ Provides PPP and login user authentication ■ Supports RADIUS, provides RADIUS authentication/accounting ■ Provides local authentication ■ Supports CHAP and PAP authentication
	Firewall	<ul style="list-style-type: none"> ■ Supports standard access control list ■ Supports extended access control list ■ Supports interface-based access control list ■ Supports time segment based access control list
	NAT	<ul style="list-style-type: none"> ■ Supports the users in LAN to access external networks by using the IP address in a configured address pool. ■ Supports to configure relationship between access control list and address pool. ■ Supports to configure relationship between access control list and interface. ■ Supports the host of external network to access the internal server ■ Supports to configure valid period for address translation
	Data security	<ul style="list-style-type: none"> ■ Supports terminal access security (user classification protection, user login authentication) ■ Supports IPSec, provides tunnel and transmission encapsulation modes and supports AH and ESP security authentication ■ Supports network data encryption card and provide IPSec encryption/decryption ■ Supports IKE, automatically negotiates on security key and create the security federation
Network reliability	Backup center	<ul style="list-style-type: none"> ■ Can back up any physical interface or sub-interface on the router and an X.25 or frame relay virtual circuit on the interface as well. ■ Barring the Ethernet interface, any physical interfaces or virtual interface templates on the router can be used as backup interfaces. An X.25 or frame relay virtual circuit on the interface or a dialer route on the dial interface can be used as backup interface as well. ■ Provides multiple backup interfaces for one main interface. These backup interfaces will be used according to their priorities. ■ Backs up multiple main interfaces of the interfaces with multiple physical channels ■ Supports to configure the conditions to switch the main/standby interfaces
	Hot backup	<ul style="list-style-type: none"> ■ Supports VRRP

Attribute	Description	
Quality of service (QoS)	Traffic classification and flow control	<ul style="list-style-type: none"> ■ Supports CAR (Committed Access Speed) and packet priority, monitoring the network traffic entering ISP ■ Supports LR (Line Rate of physical interface) to limit the total speed of packet transmission on physical interface
	Traffic shaping	<ul style="list-style-type: none"> ■ Uses buffer and token bucket to support general traffic shaping (GTS).
	Congestion management	<ul style="list-style-type: none"> ■ Supports FIFO (first-in-first-out queue) ■ Supports PQ (priority queue) ■ Supports CQ (customization queue) ■ Supports WFQ (Weighted Fair queue)
	Congestion Avoidance	<ul style="list-style-type: none"> ■ Supports WRED (Weighted Random Early Detection), implementing flow-based congestion avoidance
Configuration management Terminal server	Command line interface	<ul style="list-style-type: none"> ■ Prompts provide information in English ■ Prompt command line hierarchical protection, to ensure that the unauthorized users cannot access the router. ■ Prompt Detailed debugging information, helpful for diagnosis of network faults ■ Provides network test tools such as tracer and ping commands, to quickly diagnose whether the network is normal. ■ Info-center loghost configuration
	Terminal service	<ul style="list-style-type: none"> ■ Performs local or remote configuration via the console port, asynchronous serial port, X.25 PAD, Telnet and Reverse Telnet etc. ■ Logs on the UNIX host via Rlogin ■ Configures router via the dumb terminal service ■ Provides dumb terminal service via PRI port ■ Supports the send function and provide the information interaction between terminal subscribers ■ Terminal access via asynchronous serial port ■ Supports dial-up POS and network POS accessing based on the shared POS access technology, which improves card account processing
	System Management	<ul style="list-style-type: none"> ■ Supports to upload and download programs/configuration files via FTP ■ Supports to upload and download programs/configuration files via TFTP ■ Supports on-line upgrade of the cards.
	Network management	<ul style="list-style-type: none"> ■ Supports SNMP (Simple Network Management Protocol) ■ Supports RMON (Remote Monitor)

New Features of the 3Com Router 1.x

New features have been added to the 3Com Router1.10.

Support New Interfaces

E3 and CE3 Interfaces

Both E3 and E1 are part of the ITU-T digital carrier architecture and are used in most regions beyond North America. The data transmission speed of E3 is 34.368 Mbps and the line code is HDB3. E3/CE3 interfaces support the link layer protocols including PPP, HDLC, Frame Relay, LAPB, and X.25, as well as the network protocol such as IP. Similar to E1/CE1, E3/CE3 interfaces can work in two operating modes, namely, E3 mode and CE3 mode.

- When working in E3 mode, an E3/CE3 interface is a timeslot-less interface of the bandwidth of 34.368 Mbps.
- When working in CE3 mode, it can multiplex/demultiplex 16 channels of E1 signals. The E3-to-E1 multiplexing is compliant with the G.751 and G.742 provisions of ITU-T. In addition, each E1 interface can be divided into 32 timeslots.

E1-F/T1-F Interface

E1-F and T1-F interfaces refer to the fractional E1 and T1 interfaces, which are equivalent to the simplified CE1/PRI and CT1/PRI interfaces. In essence, they are a low-cost approach to E1/T1 access. In a simple E1 or T1 access application requiring neither division of multiple channel groups nor ISDN PRI, either the E1-F or T1/F interface will be a good choice.

Null Interface

The functions of the Null interface are similar to those of null devices supported by many operating systems. It is always in UP status, but cannot forward data packets or configure IP addresses or encapsulate other protocols. Null interface is a virtual interface with software characteristics. Any network data packet sent to this interface will be dropped.

FRoIP and FRoISDN

Frame Relay over IP

As IP networks have gained wider acceptance, Frame Relay (FR) applications have relied on IP networks for data communication and interconnection between networks. FRoIP technology enables IP networks to carry FR data by establishing a GRE tunnel across the IP network to connect the two FR networks at both ends of the IP network.

Frame Relay over ISDN

Frame Relay over ISDN provides a method for accessing the Frame Relay network based on ISDNs and the related devices. This shortens the time for users to access and lowers the cost of leased lines.

The Frame Relay over ISDN is mainly used in the following two aspects:

- The simplest application is to take Frame Relay over ISDN as the main communications method. That is, all the routers support Frame Relay over ISDN, and the individual routers can directly access the Frame Relay networks (without TA adapters) to communicate.

- Combined with BDR, Frame Relay over ISDN can be taken as the backup communication method for Frame Relay.

Multilink Frame Relay	The Multilink Frame Relay (MFR) feature introduces functionality based on the Frame Relay Forum Multilink Frame Relay UNI/NNI Implementation Agreement (FRF.16). This feature provides a cost-effective way to increase bandwidth for particular applications by enabling multiple serial links to be aggregated into a single bundle of bandwidth. MFR is supported on User-to-Network Interfaces (UNI) and Network-to-Network Interfaces (NNI) in Frame Relay networks.
FR Compression	FR compression technology is used to compress the FR packets for the purpose of effectively saving the network bandwidth and decreasing the network load, and hence to implement data transmission over FR networks with high efficiency. 3Com Routers follow the FRF.9 standard for FR compression. FR compression can achieve a significant effect on a FR line with low bandwidth. FR interfaces fall into two categories, namely, point-to-point interface and multipoint interface.
Bridge	<p>Bridges are a type of network devices that connect LANs at the data link layer for data transmission among them. For some small or remote networks, a bridge can reduce the network maintenance cost and free the network terminal subscribers from making special settings for the devices. In addition, its network connection is no difference from a HUB.</p> <p>3Com Routers support transparent bridging and are compatible with IEEE 802.1d. The routers support the STP and bridging functions defined in IEEE 802.1d and support bridging on the links encapsulated with PPP, HDLC, X.25, or Frame Relay, as well as bridging on VLAN sub-interfaces and BDR. Furthermore, the routers can implement multi-port binding and load sharing.</p>
IP Count	IP count implements accounting on the incoming and outgoing packets as well as the packets denied by the firewall on the routers. When implementing IP count, whether the packets match the count list rules and whether the packets are denied by the firewall, are two standards by which the router sorts the bidirectional packets for count. When making data statistics, both the number of packets and the total bytes are recorded.
Virtual Router Redundancy Protocol (VRRP)	Virtual Router Redundancy Protocol (VRRP) is a fault tolerant protocol. Normally, the default route set for a host in a network takes the GW route of the network as the next hop. Through the default route, the host can carry out the communications with the external networks. If the GW route fails to work, all the hosts that take it as the next hop on the segment will be unable to communicate with the outside. VRRP can fulfill the router redundancy by assigning multiple routers into a router group. Thus, whenever a member fails to work, a backup router will take up the work of the failed router and thus can ensure the normal communications between the hosts on the network and the outside.

2

3COM ROUTER USER INTERFACE

This chapter includes information on the following topics:

- Establish Configuration Environment
- Command Line Interface (CLI)
- User Identity Management
- Basic Configuration and Management of the System

Establish Configuration Environment

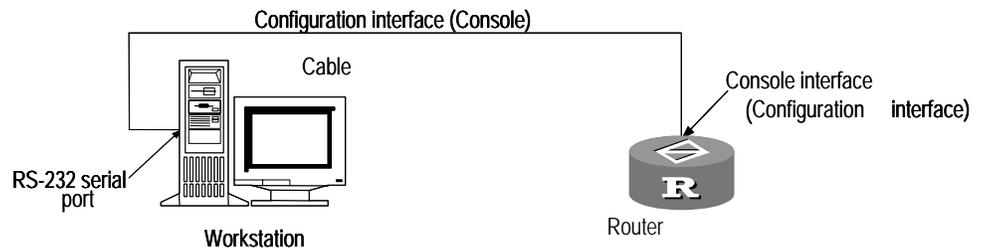
The 3Com Router 1.x supports local and remote configuration, and the configuration environment can be established in the following ways:

Local Configuration Environment via Console Port

The local configuration environment can be established via the console port (configuration interface).

- 1 As shown in Figure 2, the local configuration environment can be established via the console port just by connecting the serial port of the computer with the console port of the router via a standard RS-232 cable.

Figure 2 Establish a local configuration environment via configuration interface



On 3Com modular routers the CONSOLE port and AUX port are on the front of the unit, while other ports are on the rear of the unit. The above diagram shows the rear of the unit. For details, please refer to the 3Com Installation Guide.

- 2 Run a terminal emulator application such as HyperTerminal of Win9X on the computer to establish a new connection. Select an RS-232 serial port on the computer, set the terminal communication baudrate parameters as 9600 bps, 8 data bits, 1 stop bit, no parity and no flow control, and select the terminal emulation type as VT100, as shown in the following diagram ("HyperTerminal" setting interface in Windows 9X).

Figure 3 Establish a new connection

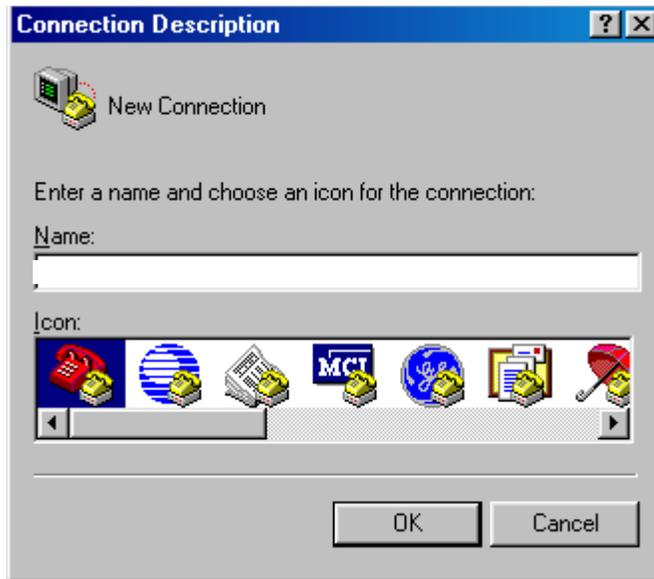


Figure 4 Select the computer serial port for actual connection

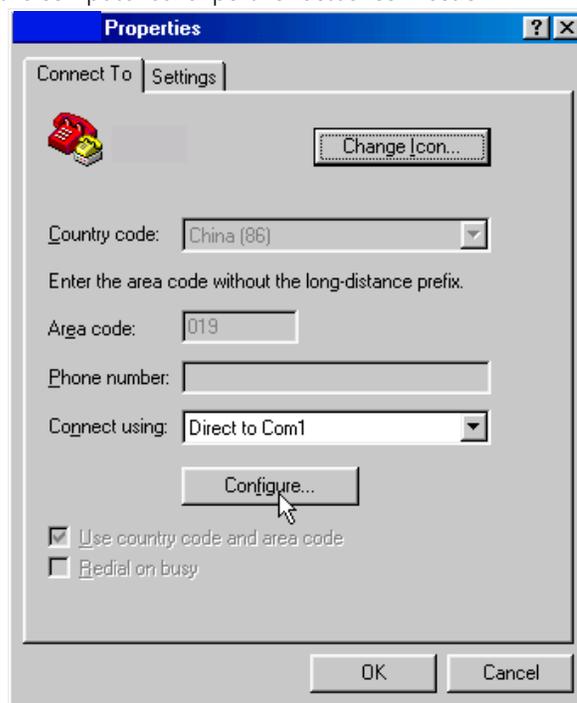


Figure 5 Set port communication parameters

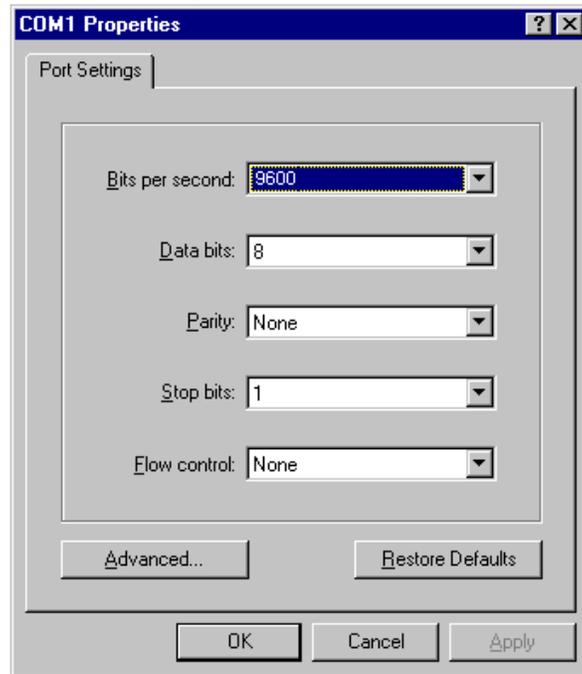
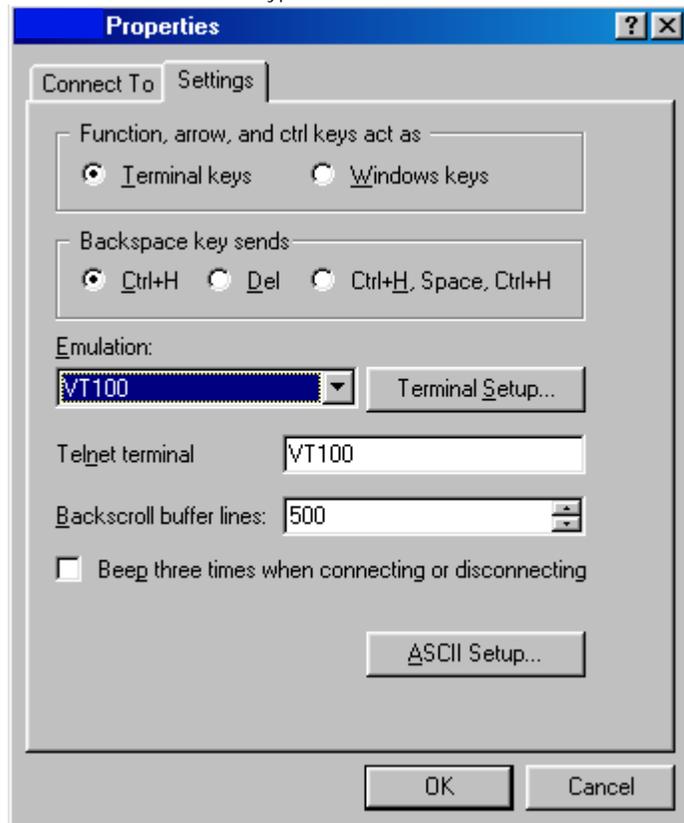


Figure 6 Select terminal emulation type



- 3 Power on the router to display the self-test information of the router. Press *Enter* after the self-test to display the prompt "Username:" and "password:". Type in the correct username and the password, then enter the system view of Router.

- 4 Enter the command to configure the router or view the running status of the router. Enter "?" to get help when necessary. For details of specific commands, please refer to the following chapters.

Remote Configuration Environment via Async Serial Port

The router powers on, then creates a remote configuration environment by connecting to the asynchronous serial ports of the router (including synchronous/asynchronous serial port, AUX interface, i.e., auxiliary interface, etc.) via modem dial-up. Detailed below is the description on how to establish a remote configuration environment via asynchronous serial port, with AUX interface as an example.



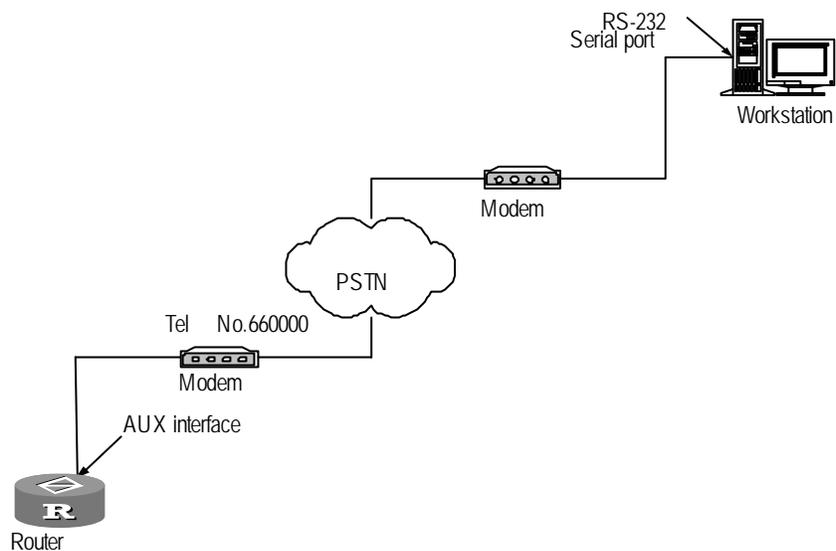
To establish a remote configuration environment via an asynchronous serial port of the router, pre-configure it to flow mode. For specific setting method, please refer to the Terminal Service chapter in this manual.



The modem connected to the asynchronous serial interface should be set to auto-answer mode.

- 1 As shown in Figure 7, connect a modem to computer serial port and another modem to the routers asynchronous serial port (AUX interface in the diagram).

Figure 7 Establish a remote configuration environment

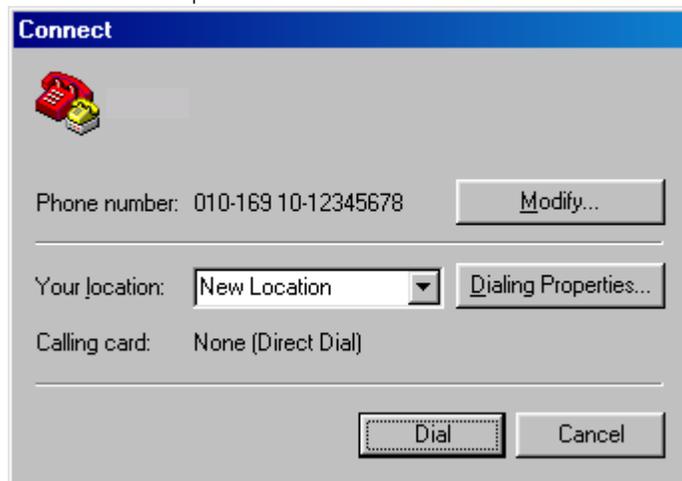


- 2 Run a terminal emulator application, such as HyperTerminal of Win9X, on the computer to establish a new connection. Select the RS-232 serial port on the computer for actual connection; set the terminal communication parameters to 9600 baud rate, 8 data bits, 1 stop bit, no parity, no flow control or hardware flow control, and select the terminal emulation type as VT100, the same as the connection established via the console port.
- 3 Before powering on the router, power on its external modem. Initialize the router via AT command, and then dial on the remote computer to establish a connection with the router, as shown in the following figure.

Figure 8 Establish a dial-up connection via “HyperTerminal”



Figure 9 Dial on remote computer



- 4 If a dial-up connection is established, then press *Enter* after the self-test to display the prompt “Username:” and “password:” . Enter the correct username and the password, then enter the system view of Router.
- 5 Enter command to configure the router or view running status of the router. Enter ? to get help when necessary. For details of specific commands, please refer to the following chapters.

Local/Remote Telnet Connection Configuration Environment

After the router powers on, and IP addresses of the interfaces have been properly configured on the router, you can use the Telnet client program to establish a connection with the router and log in the router via LAN or WAN. Then configure the router.

- 1 As shown in the following two figures, connect the Ethernet port adapter on the computer with the Ethernet interface of the router. To establish a remote

configuration environment, connect the computer with the router via the WAN interface.

Figure 10 .Establish configuration environment of local telnet connection

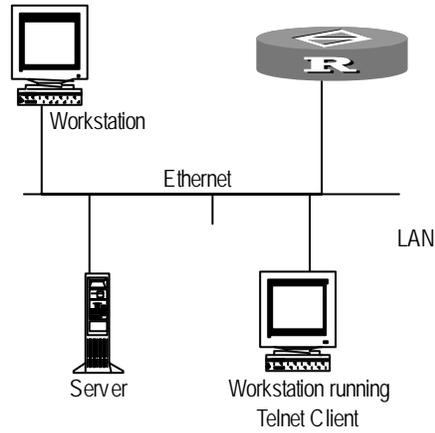
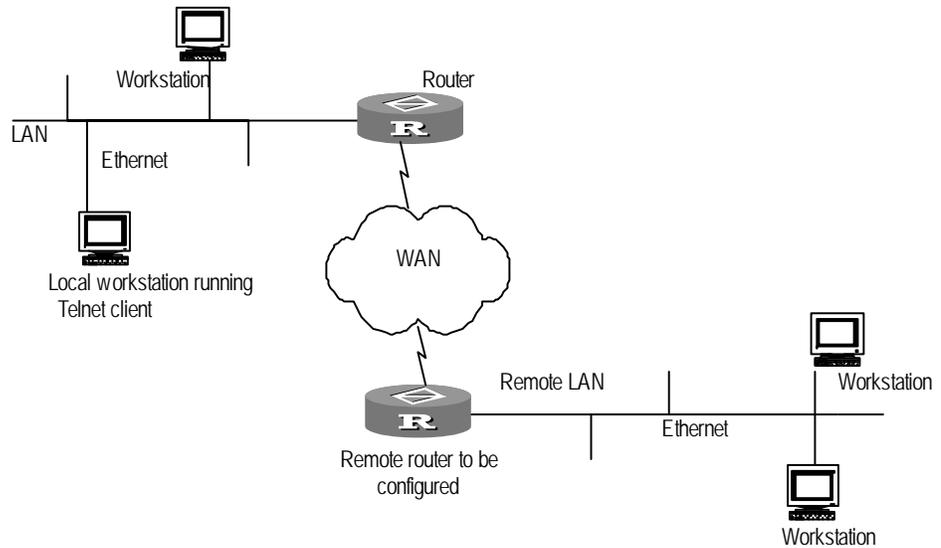


Figure 11 Establish a configuration environment of a remote telnet connection



- 2 As shown in the following two figures (Telnet client program interface in Windows 9X), run the Telnet client program on the computer and set its terminal emulation type as VT100.

Figure 12 Run a telnet program

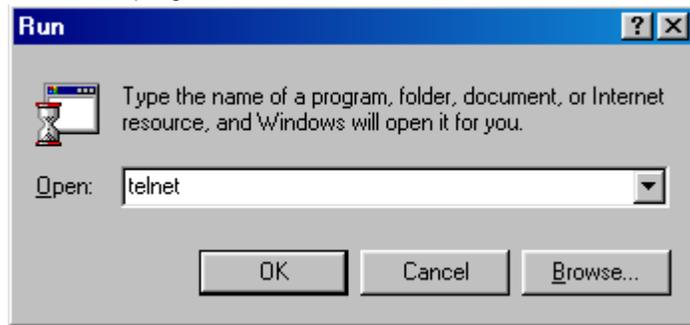
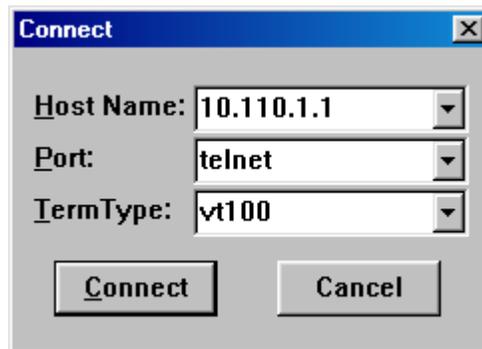


Figure 13 Establish a telnet connection with router



The host name in the above figure is the name or IP address of a router interface of the remote connection.

- 3 If connection is established, press *Enter* after the self-test to display the prompt "Username:" and "password:". Enter the correct username and the password, then enter the system view of the router. If the prompt of `Too many users!` appears, try to connect later. Usually, there should be no more than five Telnet users at any one time.
- 4 Enter the command to configure the router or view running status of the router. Enter `?` to get help if necessary. For details of specific commands, please refer to the following chapters.



In router configuration via Telnet connection, the Telnet connection will be disabled if you change the IP address of the router interface. So please enter the new IP address of the router interface at the Telnet client prompt after any changes in address, so as to re-establish the connection.

Command Line Interface (CLI)

The 3Com Router 1.x provides a series of configuration commands for the user to configure and manage network equipment via command line interface. The command line interface can accomplish the following:

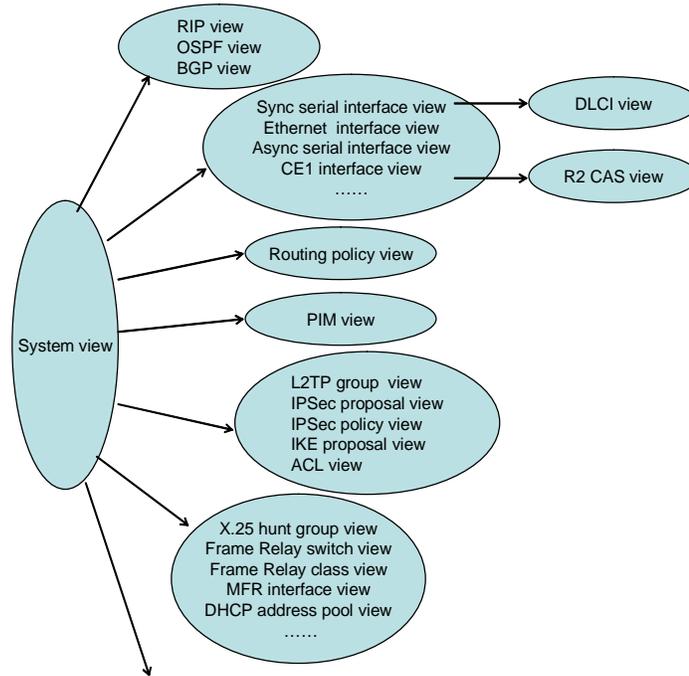
- Perform local or remote configuration via the console port.
- Log in the router through modem dial-up with asynchronous serial port and perform remote configuration.
- Perform local or remote configuration via Telnet connection
- Provide terminal access service.
- Configure command hierarchical protection to reject the illegal users.

- Provide online help any time the user keys in "?".
- Provide network test commands, such as **tracert** and **ping**, etc. to quickly diagnose whether the network is normal.
- Provide rich and detailed debugging information for diagnosis of network faults.
- Use telnet command to directly log in and manage other routers
- Support TFTP service, convenient for users to upload or download the 3Com Router main program files and configuration files.
- Provide FTP service, convenient for users to upload or download the 3Com Router main program files and configuration files.
- Provide function similar to DosKey to execute a history command.
- Searches the key word via command line interpreter with an incomplete match method. Interpretation will be available just by entering non-conflict key words. For example, enter abbreviated "**dis**" for **display** command.

View View is the interface of the 3Com Router command. Different commands are implemented in different views, and different views are realized according to different function requirements. For example, the RIP view can configure corresponding commands.

The views in the 3Com Router are in a hierarchical structure. You can enter the function views in system view and the sub-function views in the function views. The following figure shows the view structure of the 3Com Router.

Figure 14 Hierarchical view structure of the 3Com Router



The following table gives some details of the functionality features of the command views as well as the commands for entering these views.

System view Table 4 Views and their prompts

View name	Function	Prompt	Enter command	Exit command
system view	Configures the system parameters	[Router]	Directly enter the view upon the login of subscribers	Enter logout to disconnect the connection with the Router
RIP view	Configures the RIP parameters	[Router-rip]	Enter rip in system view	Enter quit to return to the system view
OSPF view	Configures the OSPF parameters	[Router-ospf]	Enter ospf in system view	Enter quit to return to the system view
BGP view	Configures the BGP parameters	[Router-bgp]	Enter bgp in system view	Enter quit to return to the system view
routing policy view	Configures the routing policy parameters	[Router-route-policy]	Enter route-policy abc permit 1 or route-policy abc deny 1 in system view	Enter quit to return to the system view
PIM view	Configures the multicast routing parameters	[Router-pim]	Enter pim in system view	Enter quit to return to the system view
sync serial interface view	Configures the synchronous serial interface parameters	[Router-Serial0]	Enter interface serial 0 in any views	Enter quit to return to the system view

View name	Function	Prompt	Enter command	Exit command
async serial interface view	Configures the asynchronous serial interface parameters	[Router-Async0]	Enter interface async 0 in any views	Enter quit to return to the system view
AUX interface view	Configures the AUX interface parameters	[Router-Aux0]	Enter interface aux 0 in any views	Enter quit to return to the system view
AM interface view	Configures the AM interface parameters	[Router-AM0]	Enter interface am 0 in any views	Enter quit to return to the system view
Ethernet interface view	Configures the Ethernet interface parameters	[Router-Ethernet0]	Enter interface ethernet 0 in any views	Enter quit to return to the system view
loopback interface view	Configures the loopback interface parameters	[Router-LoopBack1]	Enter interface loopback 0 in any views	Enter quit to return to the system view
ISDN BRI interface view	Configures the ISDN BRI interface parameters	[Router-Bri0]	Enter interface bri 0 in any views	Enter quit to return to the system view
CE1 interface view	Configures a time slot binding method on the CE1 interface and the physical layer parameters	[Router-E1-0]	Enter controller e1 0 in any views	Enter quit to return to the system view
CT1 interface view	Configures a time slot binding method on the CT1 interface and the physical layer parameters	[Router-T1-0]	Enter controller t1 0 in any views	Enter quit to return to the system view
CE3 interface view	Configures a time slot binding method on the CE3 interface and the physical layer parameters	[Router-E3-0]	Enter controller e3 0 in any views	Enter quit to return to the system view
CT3 interface view	Configures a time slot binding method on the CT3 interface and the physical layer parameters	[Router-T3-0]	Enter controller t3 0 in any views	Enter quit to return to the system view
E1-F interface view	Configures the physical layer parameters for the E1-F interface	[Router-Serial0]	Enter interface serial 0 in any views	Enter quit to return to the system view
T1-F interface view	Configures the physical layer parameters for the T1-F interface	[Router-Serial0]	Enter interface serial 0 in any views	Enter quit to return to the system view
dialer interface view	Configures the dialer interface parameters	[Router-Dialer0]	Enter interface dialer 0 in any views	Enter quit to return to the system view
virtual template interface view	Configures the virtual template parameters	[Router-Virtual-Template1]	Enter interface Virtual-Template 1 in any views	Enter quit to return to the system view
tunnel interface view	Configures the tunnel interface parameters	[Router-Tunnel0]	Enter interface tunnel 0 in any views	Enter quit to return to the system view
NULL interface view	Configures the null interface parameters	[Router-Null0]	Enter interface null 0 in any views	Enter quit to return to the system view
logical channel view	Configures the AUX interface parameters	[Router-logic-channel1]	Enter logic-channel 1 in any views	Enter quit to return to the system view
bridge template interface view	Configures the virtual Ethernet interface parameters	[Router-Bridge-Template1]	Enter interface Bridge-Template 0 in any views	Enter quit to return to the system view

View name	Function	Prompt	Enter command	Exit command
X.25 hunt group view	Configures the X.25 hunt group parameters	[Router-x25-huntgroup-abc]	Enter x25 hunt-group abc round-robin in system view	Enter quit to return to the system view
Frame Relay class view	Configures the FR class parameters	[Router-fr-class-abc]	Enter fr class abc in system view	Enter quit to return to the system view
DLCI view	Configures the DLCI parameters	[Router-fr-dlci-100]	Enter fr dlci 100 in synchronous serial interface view. (The link layer protocol encapsulated on the interface should be FR.)	Enter quit to return to the synchronous serial interface view
Frame Relay switch view	Configures the FR switch parameters	[Router-fr-switch-abc]	Enter fr switch abc in system view	Enter quit to return to the system view
MFR interface view	Configures the MFR interface parameters	[Router-MFR0]	Enter interface mfr 0 in any views	Enter quit to return to the system view
L2TP group view	Configures L2TP group	[Router-l2tp1]	Enter l2tp-group 1 in system view	Enter quit to return to the system view
IPSec proposal view	Configures a security proposal	[Router-ipsec-proposal-abc]	Enter ipsec proposal abc in system view	Enter quit to return to the system view
IPSec policy view	Configures a security policy	[Router-ipsec-policy-abc-0]	Enter ipsec policy abc 0 in system view	Enter quit to return to the system view
IKE proposal view	Configures an IKE proposal	[Router-ike-proposal-0]	Enter ike proposal 0 in system view	Enter quit to return to the system view
ACL view	Configures ACL rules	[Router-acl-1]	Enter acl 1 in system view	Enter quit to return to the system view
DHCP address pool view	Configures a DHCP address pool	[Router-dhcpabc]	Enter dhcp server ip-pool abc in system view	Enter quit to return to the system view



The command line prompt character consists of the network device name (Router by default) and the command view name, such as [Router-rip].



The commands are divided according to view. In general, in a certain view, only the commands defined by the view can be executed, but some widely used commands (including ping, display, debugging, reset, save, interface, logic-channel, and controller) can be executed in all views



For some views listed in the above table, you must enable the corresponding functions before you can enter the views. To enter some other views, however, you should configure the related restriction conditions. For more information, see the related chapters in this manual.



In all views, you can use the quit command to return to the superior-level views, and the return command to the system view directly.

Command Line Online Help

The command line interface of the 3Com Router provides the following online helps:

- Full help
- Partial help

- The help information obtained via the above-mentioned online help is described as follows:
- 1 Full help: Enter “?” in any view, all the commands in this view and their brief descriptions can be obtained.

```
[Router]?
aaa-enable Enable AAA (Authentication, Authorization and Accounting)
acl Specify structure of access-list configure information
arp Add a ARP entry
bgp Enable/disable BGP protocol
bridge Bridge Set
clock Set system clock
copy Copy config or system file to remote tftp server
configfile Select config file stored in flash or NVRAM
controller Set a E1/T1 entry
.....
```

- 2 Partial help: Enter a command followed by “?” separated with the space key, and if parameters are available, descriptions of related parameters will be listed.

```
[Router] display ?
aaa AAA information
aaa-client Display the buffered voice information
acl Display access-list information
arp ARP table information
bgp BGP protocol information
bridge Remote bridge information
.....
```

- 3 Partial help: Enter a character string followed by “?”, and descriptions of all the commands beginning with this character string will be listed.

```
[Router] di?
dialer dialer-rule display
```

- 4 Partial help: Enter a command and a character string, followed by “?”, and all the key words beginning with this character string will be listed.

For example:

```
[Router] display a?
aaa aaa-client acl arp
```

Command Line Error Message

In the 3Com Router, all the commands entered by users will be accurately executed if they pass the syntax check. Otherwise, users will be informed by an error message. The following table shows common error messages.

Table 5 List of common command line error messages

Common error message	Causes
Incorrect command	No command has been found.
	No key word has been found.
	Wrong parameter type
Incomplete command	The command input is incomplete.
Invalid parameters	Parameter value beyond limit
Too many parameters	Too many parameters are input.

History Command The command line interface of the 3Com Router 1.x provides a function similar to DOSKey by automatically saving the history of commands inputted users. Users can check the history of commands saved in the command line to repeat execution. 10 history commands can be saved at the most for each user. The configuration steps are shown in the following two tables.

1 Display history command

The following command can be used in all views to display the command recently input:

Table 6 Display history command

Operation	Command
Display history command	display history-command

2 Check history command

The following keys can be used in all views to check recent commands:

Table 7 Check history command

Operation	Keys	Result
Go to the previous history command	<i>Ctrl+E</i> (in Windows 9x)	If there are earlier inputted commands, fetch the previous one. Otherwise, the alarms rings.
Go to the next history command	<i>Ctrl+R</i> (in Windows 9x)	If there are later inputted commands, fetch the next one. Otherwise, clear the commands and the alarms rings.

Edit Features of Command Line

The command line of the 3Com Router 1.x provides basic command edit functions and supports multi-line editing. The maximum length of each command is 256 characters, as shown in the following table:

The following keys can be used in all views to edit commands:

Table 8 Edit function table

Key	Function
Any key on board	If the edit buffer is not full, insert the character at the cursor and move the cursor to the right.
Backspace key: BackSpace	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.
Delete key: Delete	Delete the character at the cursor and the alarm rings when the cursor gets to the end of the command line.
Left cursor key	The cursor moves one character to the left, and the alarm rings when the cursor gets to the beginning of the command line.
Right cursor key	The cursor moves one character to the right, and the alarm rings when the cursor gets to end of the command line.

Display Features of Command Line

The command line interface of the 3Com Router 1.x provides the following display features:

Provide pause function when the information displayed exceeds one screen page, and three options are available for users.

Table 9 Display function table

Operation	Commands or keys
Stop display information on terminal	Press <i>Ctrl+C</i> when display information pauses.
Continue to display information of next screen page	Press <i>Space</i> when display information pauses.
Continue to display information of next line	Press <i>Enter</i> when display information pauses.

User Identity Management

The 3Com Router sets three kinds of router management users: administrator user, operator user and guest user. Different kinds of users have different rights to execute commands.

- 1 An administrator user has the right to execute all the commands of the router. Only the administrator user can configure all the functions and parameters and can enter all views.
- 2 An operator user can monitor and maintain the router, they can also obtain the debugging information of the router. The operator user can only execute the following commands.

```

debugging Enable system debugging functions
display Display system running information
language Switch language mode (English)
logout logout
pad Try to open a PAD connection
ping Send ICMP ECHO_REQUEST packets to network hosts
reboot Reboot the router under certain condition
reset Reset operation
rlogin Log in remote UNIX host
send Send a message to other terminals
telnet Telnet to a remote host
tracert Trace the route taken by packets to reach a network host
undo Cancel current setting
    
```

- 3 A guest user has no right to manage the router, but only has the right to perform a remote test on the router. The guest user can only execute the following commands.

```

language Switch language mode (English, Chinese)
logout logout
pad Try to open a PAD connection
ping Send ICMP ECHO_REQUEST packets to network hosts
rlogin log in remote UNIX host.
telnet Telnet to a remote host
tracert Trace the route taken by packets to reach a network host
    
```

Please perform the following commands in system view.

Table 10 Configure the user

Operation	Command
Configure a user	<code>local-user user-name service-type type [password { simple cipher } password]</code>
Delete a user	<code>undo local-user user-name</code>

By default, no user is set on the router. In this case, the user can log onto the router without username and password, operating as the administrator user and have the right to execute all commands.



The router should be configured with at least one administrator user. This is because any user can log onto the router as the administrator user if no user is set on the router which could lead to a breach in network security.

If a user is configured on the router, no matter what type of user they are, when that user logs onto the router, it will prompt them to input the username and password. Only after the username and password are input correctly can the user log onto the router, and the system will give the user the corresponding access rights.



The router can only be configured with the operator user and guest user after an administrator user has been configured.



If an operator user forgets their password, the administrator user can help them to modify the password. Also, they can enter into the boot menu (only on the HyperTerminal connected to the Console port) to clear the application password, and then reboot the router. At this time, the operator user can log onto the router without username and password.



If an administrator user forgets their password, they can modify the password through another administrator user identity. If there is no other administrator user, they can only enter into the boot menu (only on the HyperTerminal connected to the Console port) to clear the application password, and then reboot the router. In this case, the router will restore the default configuration, that is, no user is set on the router. Because the operation clears the configuration, the administrator must reconfigure all the functions and parameters.

Basic Configuration and Management of the System

Basic configuration and management of the system includes:

- Configure the router name
- Set the system clock
- Reboot the system

1 Configure the router name

Please perform the following command in all views.

Table 11 Configure the router name

Operation	Command
Configure the router name	<code>sysname sysname</code>

By default, the router name is " Router" .

2 Set the system clock

Please perform the following command in all views.

Table 12 Set the system clock

Operation	Command
Set the system clock	<code>clock hour:minute:second day month year</code>

By default, the system clock is 08:00:00 1 1 1997.



*The system clock will reset to the initial number when the configuration is deleted by using the **delete** command or is deleted at the boot menu.*

3 Reboot the system

Please perform the following commands in all views.

Table 13 Reboot the system

Operation	Command
Reboot the system right now	reboot [reason <i>reason-string</i>]
Reboot the system after a specified time	reboot mode interval { <i>hh:mm</i> <i>time</i> } [<i>string</i>]
Reboot the system at the specified time	reboot mode time <i>hh:mm</i> [<i>dd/mm/yy</i>] [<i>string</i>]
Cancel the reboot task	reboot cancel



*Before rebooting the system, make sure to save the current configuration by using the **save** command, or some configuration may be lost.*

Display the System Information of the Router

Execute the following commands in all views.

Table 14 Display the information of the Router

Operation	Command
Displays the current date and clock of the router	display clock
Displays the duration between the startup of the Router and the execution of the command	display duration
Displays the router name	display sysname
Displays the use information of the CPU	display processes cpu
Displays the use information of the router memory	display processes memory { <i>all</i> <i>blksize size</i> } [<i>detail</i>]
Displays the basic information of the Router	display base-information [<i>page</i>]
Displays the software version information of the Router	display version



SYSTEM MANAGEMENT

- Chapter 3 System Management
- Chapter 4 Terminal Service
- Chapter 5 Configuring Network Management
- Chapter 6 Display and Debugging Tools
- Chapter 7 POS Terminal Access Service

3

SYSTEM MANAGEMENT

This chapter includes information on the following topics:

- Storage Media and File Types Supported by the System
- Upgrade Boot ROM Software
- Upgrade the 3Com Router Main Program Software
- Configure On-Line Upgrading of the Card
- Configuration File Management
- Configure FTP

Storage Media and File Types Supported by the System

The 3Com Router series has three types of storage media:

- DRAM (Dynamic Random Access Memory), where the 3Com Router main program executes.
- Flash memory, to save the 3Com Router main program/configuration file, etc.
- NVRAM (Non-Volatile Random Access Memory) can be used to save configuration file but not program file.

The 3Com Router series manage three types of software:

- Boot ROM file
- Program file
- Configuration file

Upgrade Boot ROM Software

This section contains information to assist you with upgrading the Boot ROM software.



Upgrade router software carefully and under the guidance of technical support personnel. In addition, please refer to the release notes (in the software upgrade file packet) to make sure that the Boot ROM software version matches the 3Com Router main software version.

Router software includes Boot ROM software and the 3Com Router main program software, both of which can be upgraded by XModem only when the router is powered on for self-test. In Boot ROM software upgrade, first connect a computer external to the Console port of the router and run the terminal emulator on the computer. The specific upgrading procedure is:

- 1 Power on the router for self-test, and the following information displays:

```
3Com Router start booting
```

Quickly input *Ctrl+D* to enter the Boot ROM menu. If *Ctrl+D* is not input within three seconds, the system will restart the router and the following prompt information displays:

```
*****
*
* 3Com Router Series Bootrom, V4.25 *
*
*****
```

```
3Com Corporation Copyright(C) Reserved.
Compiled at 09:06:32 , Jun 13 2003.
```

```
Now testing memory...OK!
256M bytes DRAM
8192k bytes flash memory
Press ENTER key to get start when you see ATSO=1.
System now is starting... ATSO=1
```

2 Input *Ctrl+D*, and the following prompt information displays:

```
Please input Bootrom password:
```

Input the Boot ROM password (directly key in *Enter* since there is no factory-set password for the routers). If the Boot ROM password has already been modified, input the correct one. If your attempts to input the correct password fail three times, the system will halt, and you must power off and then power on the router.

3 If the input Boot ROM password is correct, the system will prompt:

```
Boot Menu:
1: Download Bootrom program
2: Modify Bootrom password
3: Reboot
Enter your choice (1-3):
```

In the above prompt:

- Select 1 to use XModem protocol to load router Boot ROM software.
- Select 2 to modify the Boot ROM password, and the system displays the following prompt:

```
Please input new password:*****
Retype the new password: *****
Saving the password... #
```

The system returns to the prompt displayed at step 3.

- Select 3 to restart the router.

4 If 1 is selected, the system prompts you to select a baud rate for software loading.

```
Please choose your download speed:
1: 9600 bps
2: 19200 bps
3: 38400 bps
4: 57600 bps
5: 115200 bps
6: Exit and Reboot
Enter your choice (1-6):
```

- 5 Example: if you select baud rate 115200 bps, the system will prompt you to modify the baud rate and select XMODEM transfer protocol:

Download speed is 115200 bps. Change the terminal's speed to 115200 bps, and select XMODEM protocol. Press ENTER key when ready.

According to the above prompt, change the baud rate setting at the terminal to the number equal to the baud rate of the software selected to download. After having set the baud rate of the terminal, disconnect and then reconnect the terminal, then press *Enter* to begin downloading.



After having set the terminal baud rate, make sure to disconnect and then reconnect the terminal emulator. Otherwise, the new baud rate will not be effective.

- 6 The router outputs the following information to indicate waiting for download:

Now Downloading Program File.

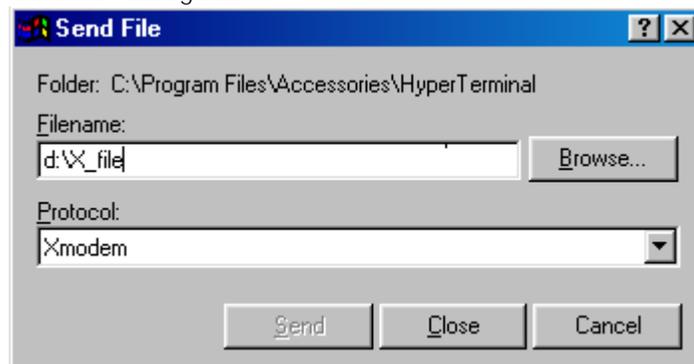
Please Start Transfer Program File Use Xmodem Protocol.

If You Want To Exit Press <Ctrl+X>.

Downloading...CCCCCCCC

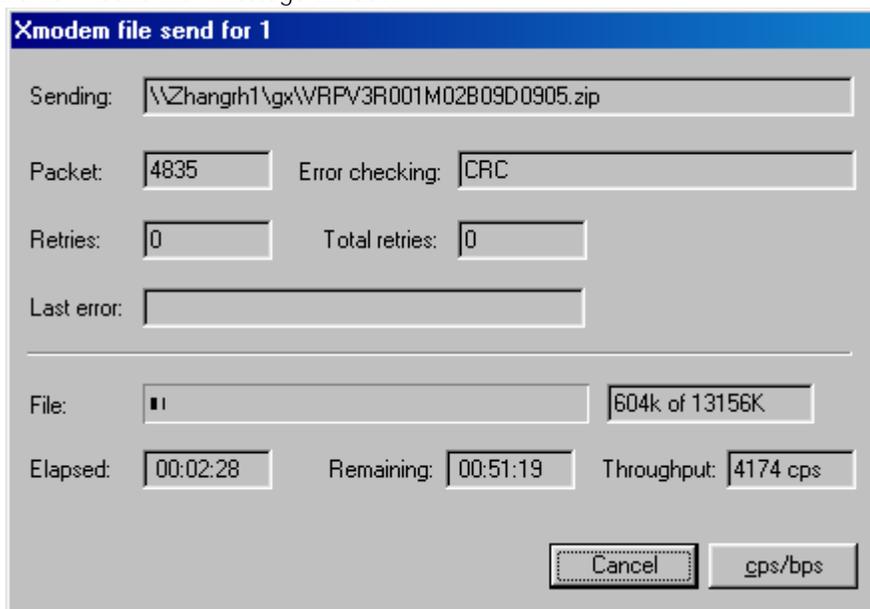
Select *Transfer/Send File* from the terminal emulator menu to select the file to be downloaded, the following dialog box displays:

Figure 15 "Send file" dialog box



- 7 Click *Browse* and select software to be downloaded. Change the downloading protocol to XMODEM, then click *Send*. The following message window displays:

Figure 16 "Send file" message window



- 8 After downloading, the router will save the file into Flash or NVRAM, display the following information, and prompt restoring of the baud-rate setting of the terminal emulator.

```
Download completed.
Writing to flash memory...
Please waiting, it needs a long time #####
Write Bootrom Success.
```

Please return to 9600 bps. Press ENTER key to reboot the system.

The above information indicates that the information is downloaded. Boldface characters prompt the user to restore the baud rate setting of the terminal emulator. Click **[Disconnect]** in the terminal menu, and then click **[Connect]** once again. If the download fails, the system displays the following information, and reboot the router:

```
Download failed.

3Com Router start booting
.....
```

If this message is displayed, you should find out the cause prior to upgrading.

- 9 Restore baud rate of the terminal emulator. Press *Enter* and the Boot ROM software of the router will be directly decompressed and loaded into the memory for execution.

Upgrade the 3Com Router Main Program Software



This section contains information to assist you with upgrading the 3Com Router Main Program software.

CAUTION: You are recommended to upgrade the software only when necessary and under the guidance of technical support personnel. The router software package includes the Boot ROM software and the 3Com Router main program software. When upgrading the software, remember to match the version of the Boot ROM software with that of the main software.

You can load the 3Com Router main software with XModem or TFTP (Trivial File Transfer Protocol) approach when powering on the router. Alternatively, you can load the software with the FTP (File Transfer Protocol) approach after the router is booted.

XModem Approach

- 1 Power on the router. The router performs a Power-On Self-Test (POST), and the following information displays:

```
3Com Router start booting
*****
*                               *
*   3Com Router Series Boot rom, V4.32   *
*                               *
*****
3Com Corporation Copyright(C) Reserved.
Compiled at 17:47:11 , Mar 21 2003.
Now testing memory...OK!
256M   bytes  SDRAM
8192k  bytes  flash memory
Press Ctrl-B to enter Boot Menu
```

Press *Ctrl+B*, and the system enters the menu for upgrading the 3Com Router main software.



The system will enter the menu for upgrading the 3Com Router main software unless you press Ctrl+B within three seconds of displaying "Press Ctrl-B to enter Boot Menu..." on the screen. Otherwise, the system will start decompressing the program. Reboot the router if you want to enter the 3Com Router main software upgrade menu after program decompression is started.

- 2 The system prompts the following information after you press *Ctrl+B*:

```
Please input Bootrom password:
```

Enter the Boot ROM password behind the prompt. If no default ex-factory Boot ROM password was set on the router, directly press *Enter*. If the user has modified the password, make sure to enter the correct one. If attempts for password authentication failed three times, the system will terminate the upgrading process.

- 3 After the correct Boot ROM password is entered, the following information displays:

```
Boot Menu:
1: Download application program with XMODEM
2: Download application program with TFTP
3: Clear application password
4: Clear configuration
5: Exit and reboot
Enter your choice(1-5):
```

Choose an option as required. Notice that option 3 is used for entering the system view from the user password.

- 4 Select 1, and the system prompts you to choose a baud rate for software loading:

```
Please choose your download speed:
1: 9600 bps
2: 19200 bps
```

```

3: 38400 bps
4: 57600 bps
5: 115200 bps
6: Exit and Reboot
Enter your choice(1-6) :
Make your selection as needed.

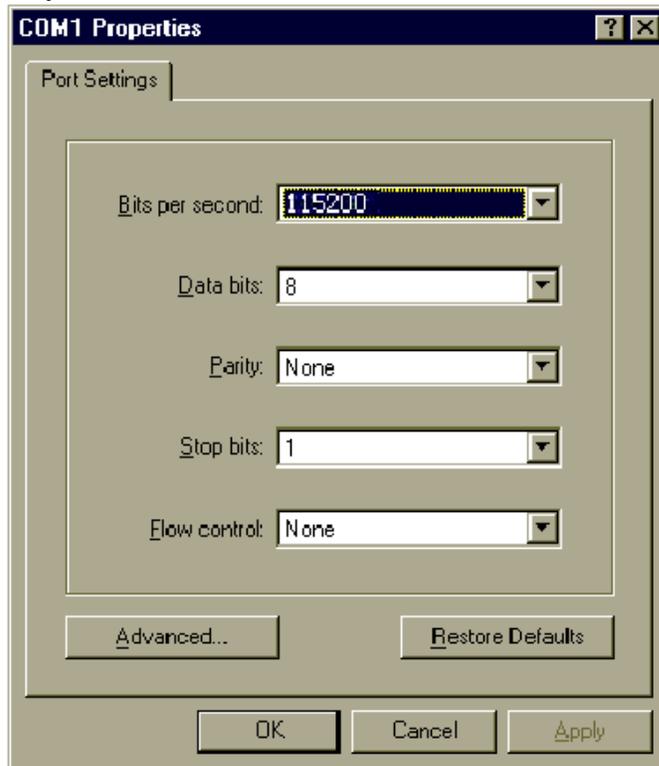
```

- 5 After a baud rate (115200 bps for example) is selected, the system displays the following information to prompt you to modify the baud rate and select the XModem protocol:

Download speed is 115200 bps. Change the terminal's speed to 115200 bps, and select XMODEM protocol. Press ENTER key when ready.

Perform the operation as prompted to change the baud rate set on the terminal into the baud rate selected for software downloading.

Figure 17 Modify the terminal baud rate



Click *OK* after setting the new terminal baud rate. Click *Disconnect* and then *Connect* in the terminal interface to proceed to the next step.



You must disconnect and connect the terminal emulation program after modifying the baud rate of the terminal. Otherwise, the new baud rate cannot take effect.

- 6 The router displays the following, indicating that the system is waiting for loading:

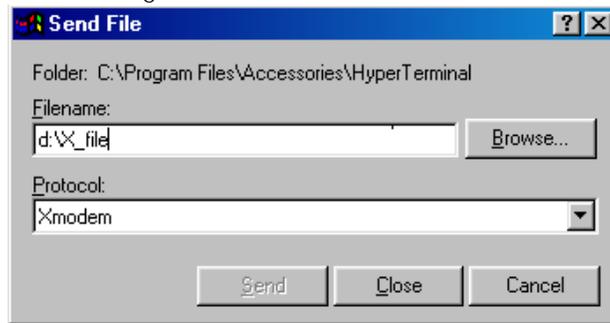
```

Now Downloading Program File.
Please Start Transfer Program File Use Xmodem Protocol.
If You Want To Exit Press <Ctrl+X>.
Downloading...CCCCCCCCCC

```

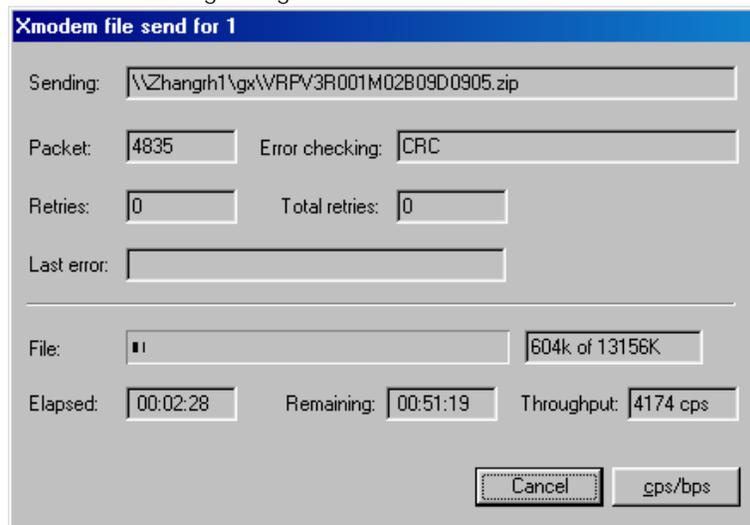
Select [Transfer File] in the terminal emulation program menu and the following dialog box displays:

Figure 18 Transfer File dialog box



- 7 Click *Browse* to open the folder containing the Boot ROM software, select the file, change the download protocol to XModem, click *Send*, and the system will start downloading and the following dialog box displays:

Figure 19 The Downloading dialog box



- 8 Upon the completion of the loading operation, the router writes the Boot ROM into the Flash or NVRAM, and the following prompts display:

```
Download completed.
Writing into flash memory...
Please wait,it needs a long time (about 1 min)
Writing into Flash Succeeds.
```

Please use 9600 bps.Press <Enter> key to reboot the system.

Perform the operation as prompted, click *Disconnect* and then *Connect* in the terminal interface.

If the downloading operation fails, the system displays the following and the router will be rebooted:

```
Download failed.
3Com Router start booting
.....
```

In this case, you should find out the failure causes and upgrade Boot ROM once again.

- 9 Restore the baud rate of the terminal emulation program to 9600 bps and press *Enter* for rebooting the router so that the new 3Com Router main program software can be run.

TFTP Approach

TFTP is a protocol used for transferring trivial files between clients and servers in the TCP/IP suite. It provides low-cost and simple file transfer service. Carried in UDP, TFTP provides only the unreliable traffic transmission service without any access authorization and authentication mechanism. It ensures data will reach destinations with the approach of timeout retransmission. Compared with FTP, the TFTP software is much smaller. At present, TFTP Version 2 (RFC 1350) is the most popular version.

The 3Com Router can provide you with TFTP client service. That is, the router works as a TFTP client, and the file server as the TFTP server. You can enter the corresponding commands on the router to upload its configuration files to the file server or download the configuration files from the file server into the Flash or NVRAM of the local router.

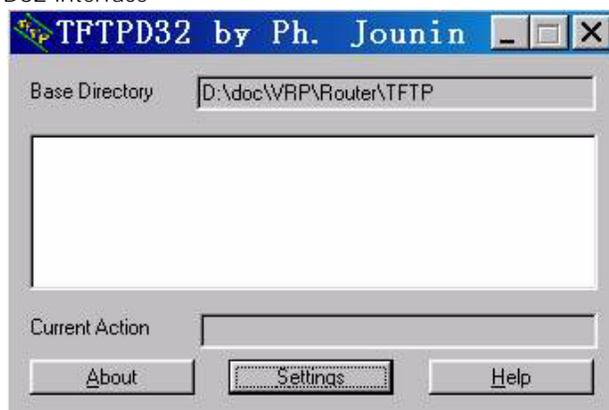
Before using TFTP, you should purchase and install a TFTP server application as the 3Com Router does not come with a TFTP server application.

The TFTP server application can run on Windows 95/98/NT.

Preparation for using the TFTP server

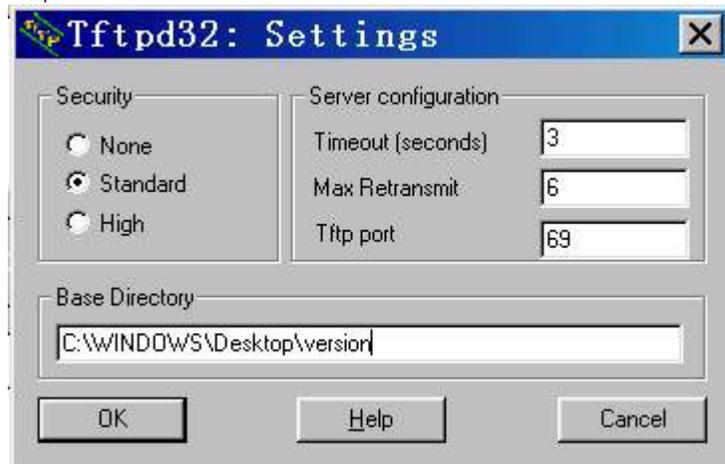
- 1 Enable the TFTP server program
 - a Enable the TFTP server program. Select a PC installed with the Windows 95/98/NT operating system and an Ethernet card and start the TFTP server program on the PC. (Alternatively, a PC running HyperTerminal can also be used.) TFTP32 in a Windows 98 environment will be taken as an example for describing the procedure. The following figure shows a TFTP32 interface.

Figure 20 TFTP32 interface



- b Set the directory for the TFTP server files. After enabling the TFTP server, redefine a TFTP file directory and copy the desired 3Com Router main program software into this directory. Alternatively, you can set the directory containing the 3Com Router main program files as the directory for TFTP server files. Specifically, click *Settings* in the TFTP32 interface, and the Tftpd32: Settings for the interface as shown in Figure 21 are displayed.

Figure 21 Tftpd32: Set interface



Enter the file directory in the field of *Base Directory*, and click *OK* for confirmation.



The setting interface may vary with different TFTP server program software.

2 Connect the router

a Select an Ethernet interface for downloading on the router.

3Com Router series support application loading on a particular Ethernet interface.

- Select Ethernet0 for 5231 Routers.
- On an Router 5640, check the slots for a 1-port 10/100Base-TX Fast Ethernet interface module (1FE) card in the order of 0, 2, 1, and 3. The Ethernet interface thus found will be used as the downloading network interface. If the router is not available with a 1FE card, check the slots for the available 2FE card in the same order, and the Ethernet interface 0 of the 2FE module found first will be used as the downloading network interface.
- On an Router 5680, check the slots for a 1FE card in the order of 0, 2, 4, 6, 1, 3, 5 and 7. The Ethernet interface thus found will be used as the downloading network interface. If the router is not available with a 1FE card, check the slots for the available 2FE cards in the same order, and the Ethernet interface 0 of the 2FE card found first will be used as the downloading network interface.

b After the Ethernet port for downloading is determined, connect the port to the PC running the TFTP server program through an Ethernet cable. Assume that the IP address of the PC is 10.110.10.13.

Upgrade the 3Com Router Main Software with TFTP when Powering on the Router

1 Run the terminal emulation program on the PC connected to the console port, start the router, quickly press *N* upon the display of 3Com Router start booting on the screen and the following prompt will be displayed:

```
(M)odify any of the 3Com router configuration or (C)ontinue? [M]
```

Press *Enter* and the following prompts will be displayed:

For each of the following questions, you can press <Return> to select the value shown in braces, or you can enter a new value.

```

NETWORK INTERFACE PARAMETERS:
Do you want a LAN interface? [N] y
This board's LAN IP address? [169.254.1.1] 10.110.10.1
Subnet mask for LAN (0 for none)? [255.255.0.0]
TFTP SERVER PARAMETERS:
IP address of the TFTP server? [169.254.75.166] 10.110.10.13
What is the name of the file to be loaded and started? [m8240ram.arj]
How long (in seconds) should CPU delay before starting up? [5]

The IP address of the TFTP server? [169.254.75.166] must be set to the IP
address of the PC connected to the Ethernet port of the router. After the last
parameter is set the following prompts will appear to ask for confirmation:

```

```

-----
NETWORK INTERFACE PARAMETERS:
  IP address on LAN is 10.110.10.1
  LAN interface's subnet mask is 0xffff0000
HARDWARE PARAMETERS:
  Processor type is MPC8240
  Internal Clock Rate 250 Mhz
  External Clock Rate 100 Mhz
  LAN Controller is DEC 21143
  Serial channels will use a baud rate of 9600
TFTP SERVER PARAMETERS:
  IP address of the TFTP host is 10.110.10.13
  The file to download and start is m8240ram.arj
  After board is reset, start-up code will wait 5 seconds

```

```

-----
(M)odify any of the 3Com router configuration or (C)ontinue? [M]

```

- 2 Enter *C* to confirm the selection and the router performs POST again, and the Boot ROM starts normally.
- 3 The router performs POST, and the following displays:

```

3Com Router start booting
*****
*                                     *
* 3Com Router Series Boot rom, V4.32 *
*                                     *
*****
3Com Corporation Copyright(C) Reserved.
Compiled at 17:47:11 , Mar 21 2002.
  Now testing memory...OK!
  256M   bytes  SDRAM
  8192k  bytes  flash memory
  Press Ctrl-B to enter Boot Menu

```

Press *Ctrl+B* as prompted and the system enters the 3Com Router main software upgrade menu.



The system enters the 3Com Router main software upgrade menu unless you press Ctrl+B within three seconds of displaying "Press Ctrl-B to enter Boot Menu..." on the screen. Otherwise, the system will start decompressing the program. Reboot the router if you want to enter the 3Com Router main software upgrade menu after program decompression is started.

- 4 Enter *Ctrl+B* and the system prompts:


```

Please input Bootrom password:

```

Input the Boot ROM password at the prompt. (By default, no ex-factory Boot ROM password is set on the router. Simply press *Enter* in this case.) If the Boot ROM password has been modified, enter the correct password. The system terminates the process if the password authentication attempts fails three times.

- 5 The system displays the following prompts upon input of the correct Boot ROM password:

```

Boot Menu:
1: Download application program with XMODEM
2: Download application program with TFTP
3: Clear application password
4: Clear configuration
5: Exit and reboot
Enter your choice(1-5):

```

Make the selection as desired. Notice that option 3 is used for entering the system view from the user password.

- 6 Select 2 for loading the 3Com Router main program with TFTP, and the following prompt displays:

```
Please start TFTP server then press ENTER key to get start
```

- 7 Press *Enter* for loading.

```

Starting the TFTP download...
.....
TFTP download completed...
read len=[03713478]
Writing program code to FLASH...
Please waiting,it needs a long time (about 1 min)
WriteFlash Success.
Press ENTER key to reboot the system.

```

- 8 Press *Enter* upon the completion of the loading and the router reboots and the 3Com Router main program directly decompresses and loads into the memory for execution.

Upgrade the 3Com Router Main Software with TFTP after Booting the Router

This approach implements upgrading by executing the `get` command to load the 3Com Router main software from the TFTP server after the router is booted.

Start the TFTP server and connect it with the router before using this method to upgrade the 3Com Router main software. Then, execute the following command in system view.

Table 15 Download configuration files from a TFTP server

Operation	Command
Downloads the 3Com Router main software from a TFTP server	<code>get ip-addr file-name system</code>

FTP Approach

An application layer protocol in the TCP/IP suite, File Transfer Protocol (FTP), is mainly used for file transfer between remote hosts. Carried on TCP, FTP can provide reliable and connection-oriented data traffic transmission without access authorization and authentication mechanisms.

After a client originates a control connection to a server by using the `port` command and uses a randomly assigned FTP port to establish the control link with port 21 on the server, the link will be in place until there is no data waiting for transmission. The server uses port 20 to establish data link with the client for data transmission.

The 3Com Router can provide you with the FTP server service. That is, the router works as a TFTP server, and a subscriber can run the FTP client application to log in the router for accessing the files on the router.

Before using FTP, you should purchase and install a FTP client application, as the 3Com Router is not supplied with this software.

Prepare for using the FTP server

1 Set an authentication method on the FTP server

This step can be omitted. AAA defaults to local authentication without accounting.

The authorization of the FTP server is provided for the top level working directory of FTP subscribers. Only the subscribers that have passed authentication and authorization can obtain the service provided by the FTP server. The 3Com Router authenticates and authorizes FTP subscribers through an AAA server. If no AAA is configured, the local user authentication is adopted by default.

When using AAA, the router cannot perform local accounting. Therefore, when using local authentication, you need to open the accounting option switch to disable the accounting function.

Perform the following configuration in system view.

Table 16 Set an authentication mode for an FTP server

Operation	Command
Enable AAA	<code>aaa-enable</code>
Enable accounting switch	<code>aaa accounting-scheme optional</code>
Adopt local authentication on PPP connections	<code>aaa authentication-scheme login default local</code>

2 Add an FTP-authorized user name and the password

Perform the following configuration in system view.

Table 17 Add an FTP-authorized user name and the password

Operation	Command
Add an FTP-authorized user name and the authentication password	<code>Local-user username password { 0 7 } password service-type ftp password {simple cipher } password</code>
Delete the FTP user	<code>undo user username</code>

For the details of the command, refer to the AAA and RADIUS Configuration contained in the Security section of this manual.

3 Enable the FTP service

The FTP service can be enabled after configuring the authentication and authorization on the FTP server. The FTP server supports multi-user access. A

remote FTP user sends a request to the FTP server, and the server will perform actions accordingly and return the execution result to the subscriber.

Perform the following configuration in system view.

Table 18 Enable FTP server

Operation	Command
Enables the FTP server	ftp-server enable
Disables the FTP server	undo ftp-server enable

Upgrade the 3Com Router Main Software with FTP

- 1 Assign an IP address to the interface on the router for connecting the router to the host running the FTP client program.
- 2 Using the Windows98 FTP client program as an example — place the file to be uploaded on a specified directory, C:\temp for example, on the FTP client.
- 3 Open the DOS window, enter **FTP x.x.x.x** (where **x.x.x.x** represents the IP address of the router), and enter the user name and password as prompted:

```
C:\WINDOWS>ftp 10.110.27.1
Connected to 10.110.27.1.
220 FTP service ready on the 3Com Router at
User (10.110.27.1:(none)): cjj
331 Password required for cjj.
Password:
230 User cjj logged in .
ftp>
```

- 4 After the authentication is passed, the FTP client displays the prompt **ftp>** enter **binary** after the prompt, and set the upload directory on the FTP client.

```
ftp> binary
200 Type set to I.
ftp> lcd c:\temp
Local directory now C:\temp.
```

- 5 At the prompt **ftp>**, set a directory for the FTP server (the router). By default, the file name of the 3Com Router main program is "system", which is case sensitive. You can modify the file name using the **ftp-server system-name** command on the router. For details, refer to Configure FTP.

```
ftp> dir
200 Port command okay.
150 okay.
config                               1007 Bytes
system                               5802368 Bytes
226 Data transmit over.
ftp: 76 bytes received in 0.00Seconds 76000.00Kbytes/sec.
```

- 6 At the prompt **ftp>**, enter the **put LocalFile [RemoteFile]** command to upload the specified file to the router. **RemoteFile** must be the name of the system file on the router.

```
ftp> put 3Com Router 1.71 system
200 Port command okay.
150 Server okay , now receive file.
226 file transmit success.
ftp: 5802263 bytes sent in 80.74Seconds 71.86Kbytes/sec.
```

- 7 At the prompt `ftp>`, appearing after the file uploading is completed, enter the `dir` command to display the file name and size on the router. If the uploading operation is successful, the program or configuration file on the router and the uploaded file on the host should have the same size.
- 8 At the prompt `ftp>`, enter the `quit` command to exit the FTP client program.
- 9 The router writes the files into the Flash after receiving all of them, and the following information displays on the terminal:

```
Now saving the program file.
Please wait for a while

Receive          5802263 Bytes from client

Writing program code to FLASH...

Please waiting, it may take a long time (about 10 min)
#####
#####
#####

Write success, please reboot router!
```

The upgraded software can only take effect after rebooting the router.

Back up the 3Com Router Main Program Software

TFTP Approach

With this approach, you can use the `copy` command to copy the 3Com Router main software to the TFTP server for redundancy, after booting the router.

Start the TFTP server and connect it with the router before using this method to back up the 3Com Router main software. Then, execute the following command in system view.

Table 19 Download configuration files from a TFTP server

Operation	Command
Copies the 3Com Router main software to a TFTP server for redundancy	<code>copy ip-addr file-name system</code>

FTP Approach

The procedure of backing up the 3Com Router main program software with FTP is the same as loading the software with FTP, except for step 6. See “FTP Approach” on page 41 for reference. When backing up the software with FTP, however, the step 6 described in “FTP Approach” on page 41 should be modified as follows:

At the prompt `ftp>`, use the `get RemoteFile [LocalFile]` command to upload the specified file to the router. *RemoteFile* should use the name of the system file on the router, and the name is case sensitive. You can use the `ftp-server config-name` command to modify the file name on the router. For details, refer to “FTP Approach” on page 44.

```
ftp> get config config.bak
200 Port command okay.
150 Server okay , now transmit file .
226 file transmit success.
ftp: 5802263 bytes received in 80.74Seconds 71.86Kbytes/sec.
```

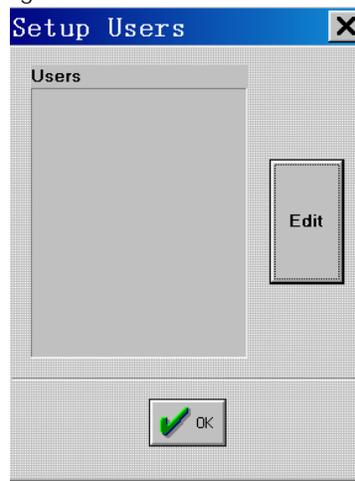
Configure On-Line Upgrading of the Card

The 3Com Router 1.x supports on-line upgrading of such cards as 2SA/4SA, E1VI and 6AM/12AM. While upgrading, the host acts as FTP Server and the router to be upgraded as the FTP Client. The host and the router coordinate to download the card upgrading files.

When you complete the installation of the FTP application, you can execute Serv-u.exe and configure the serv-u FTP according to the following steps:

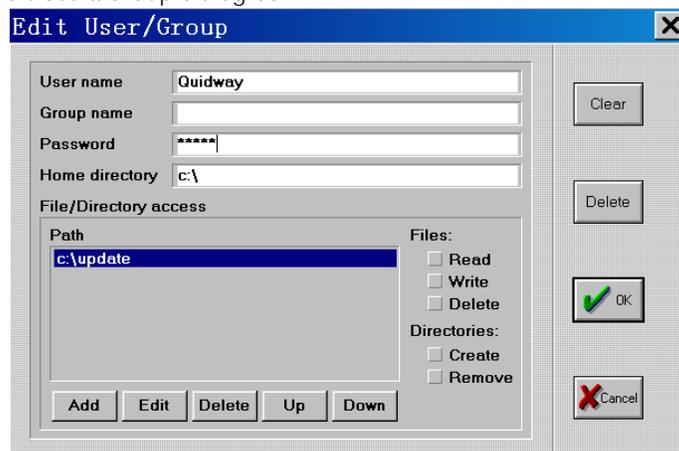
- 1 Click *Setup/Users* and the Setup Users dialog box displays as shown below:

Figure 22 Setup Users Dialog Box



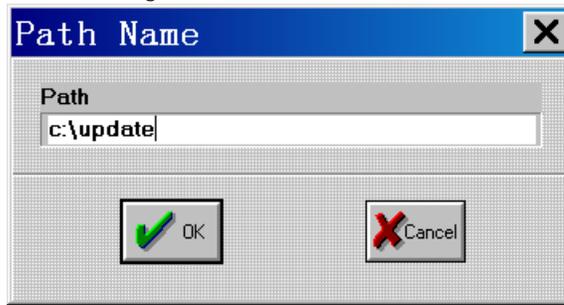
- 2 Click *Edit* to pop up the Edit Users/Group dialog box. Enter user name and password in the first two boxes respectively, and the path of the serv-u FTP in the Home Directory box.

Figure 23 Edit Users/Group dialog box



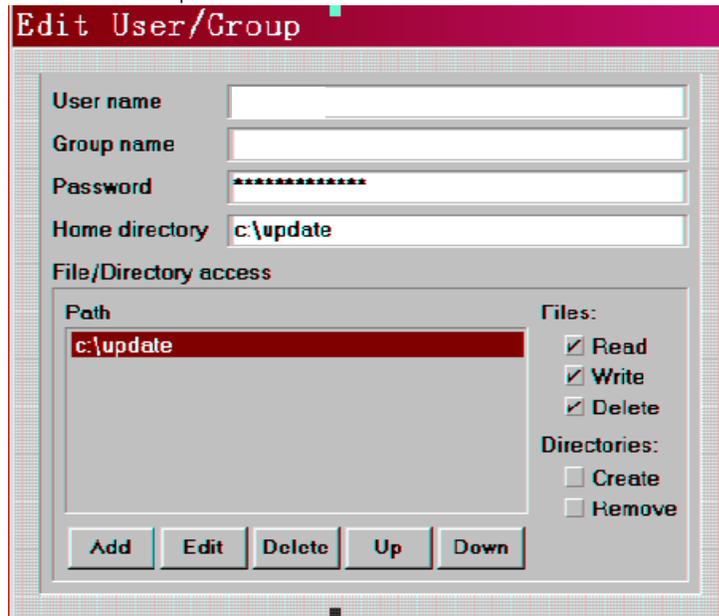
- 3 Click *Add* to pop up the Path Name dialog box. Enter the path of the serv-u FTP and click *OK* to return.

Figure 24 Path Name dialog box



Select the check boxes Read, Write and Delete in FILES and click *OK* to return.

Figure 25 Edit Users/Group check box



- 4 The cards can be upgraded on-line after the on-line upgrading files are copied to the path of the serv-u FTP.

Perform the following configuration in the system view.

Table 20 Configure on-line upgrading of the card

Operation	Command
Configure on-line upgrading of the card software	<code>update slot slot-number ftpserver { host-name ip-address } filename file-name [port port-number user user-name password password]</code>

- 5 The system will display the following information according to different situations:

If the on-line upgrading succeeds, the Console displays the following prompt information:

```
End of programming successful! Total 131072 bytes written.
```

If the on-line upgrading fails, the Console periodically displays the following prompt information:

```
Please enter the update request command for slot number
```

After the **display version** command is used, the information on the slot displays:

```
card name Driver need to be updated
```

On-line upgrading uses the upgrading program of other cards and this card will not be upgraded on-line. The Console displays the following prompt information:

```
%Error: File ID error!
```

If the on-line upgrading file is damaged, the card cannot be upgraded on-line. The Console displays the following prompt information:

```
%Error: File CRC error!
```

If another user on the same card is using the on-line upgrading command input, this user cannot execute the command. The Console displays the following prompt information:

```
The indicated board is at updating status
```

Configuration File Management

This section contains information on configuration file management.

Content and Format of the Configuration File

The configuration file is a text file, with the following format:

- Saved in command format.
- To save space, only the parameters are saved but the defaults are not saved (Please refer to the following chapters for the default values of configuration parameters.).
- Commands are organized by views. Commands in the same view are organized together, forming a section, and sections are separated with a blank line or a comment line (beginning with "!").
- Sections are usually arranged in the following order: global configuration, physical interface configuration, logical interface configuration, route protocol configuration, etc.
- Ended with "return" .

Download Configuration File

You can edit the configuration files offline following the specified format and then load them onto the router. Three methods are available for loading configuration files, which are:

- XModem approach
- TFTP approach
- FTP approach

XModem Approach

With this approach, configuration files can be loaded using the **download config** command in the terminal emulation program after booting the router. This command can only be executed in the terminal emulation program. If executing the command in Telnet, the following prompt will be displayed:

```
Download can only be executed by the serial terminal client.
```

Perform the following command in system view.

Table 21 Load configuration files

Operation	Command
Loads configuration files	download config

Follow these steps in the terminal emulation program:

- 1 Enter the command and make the confirmation.

```
[Router] download config
Do you want really download the config.ini?(Y/N)y
```
- 2 Set the binary transmission protocol to XModem/CRC.

```
Change Protocol to Xmodem, then Send the Selected File...
```
- 3 Transmit the configuration files to the router in the binary format.

```
Downloading...CCC
```
- 4 Save the loaded files into the Flash, if the loading operation is successful.

```
Download completed.
Writing to flash memory...
```
- 5 Reboot the router as prompted to validate the configuration files.

```
Write completed, please reboot the router.
```



When performing offline editing and loading of configuration files, you are recommended to do it under the guidance of technical support personnel. If a wrong configuration file is loaded, restore the default configuration by erasing the configuration file in the Flash or NVRAM (depending on the equipment).

TFTP Approach

With this approach, you can use the **get** command to download the configuration files from the TFTP server after booting the router.

Like the preparation done before loading the 3Com Router main program with TFTP, the TFTP server application should be enabled on the PC, and the transferring path for downloading the configuration files, IP address of the server host, and the number of the port to be used should be set. After all these preparation tasks have been completed, you can perform the following configuration on the router. For the procedure, refer to Upgrading with TFTP.

Perform the following command in system view.

Table 22 Download configuration files from a TFTP server

Operation	Command
Loads configuration files from a TFTP server	get tftp-server-ip-addr file-name config

FTP Approach

The procedure of loading configuration files with FTP is the same as loading the main 3Com Router program software with FTP, except for the files to be loaded. When loading configuration files with FTP, however, the step 6 described in "FTP Approach" on page 41 should be modified as follows:

At the prompt of "ftp>", use the **put LocalFile [RemoteFile]** command to upload the specified file to the router. *RemoteFile* should use the name of the config file on the router, and the name is case sensitive. You can use the **ftp-server config-name** command to modify the file name on the router. For details, refer to Configure FTP.

Back up Configuration Files

You can back up configuration files in the following ways:

- The **display current-configuration** command output backup approach
- The TFTP approach
- The FTP approach

The display current-configuration command output backup approach

Executing the **display current-configuration** command displays all the configurations (except for the default configuration) of the router. In Hyper terminal, simply copying all the displayed configuration information to a text file will fulfill the purpose of backup.

You can back up the configuration file by copying and saving the contents displayed below "Current configuration" into a text file.

TFTP approach

First of all, start the TFTP server application program on a PC (the router should be connected to the PC directly or indirectly, and ping operation can be performed between them), then set a path and use the **copy** command in the system view, thus, you can upload the configuration files to the TFTP server from the router. The method is often used in remote maintenance.

Perform the following command in system view.

Table 23 Upload configuration files to a TFTP server

Operation	Command
Upload configuration files to the TFTP server with a specified address and specify the name for the uploaded file	copy tftp-server-ip-addr file-name config

FTP approach

The procedure of loading configuration files with FTP is the same as loading the main 3Com Router program software with FTP, except for the files to be loaded. See "FTP Approach" on page 41 for reference. When loading configuration files with FTP, however, the Step 6 described in "FTP Approach" on page 41 should be modified as follows:

At the prompt of ftp>, use the **get RemoteFile [LocalFile]** command to upload the specified file to the router. *RemoteFile* should use the same name of the config file on the router, and the name is case sensitive. You can use the **ftp-server config-name** command to modify the file name on the router. For details, refer to Configure FTPConfigure FTP.

```
ftp> get config config.bak
200 Port command okay.
150 Server okay , now transmit file .
```

```
226 file transmit success.
ftp: 735 bytes received in 0.06Seconds 12.25Kbytes/sec.
```

View Current and Saved Configuration of the Router

During the power-on of the router, read the configuration files from Flash (or NVRAM) to initialize the router. Therefore, the configuration file in Flash (or NVRAM) is called initial configuration. If there is no configuration file in Flash (or NVRAM), the router will use default parameters for initialization. Corresponding to initial configuration, the configuration immediately effective during the running process of the router is called current configuration.

In general, the initial configuration and current configuration should be the same. In the case of upgrading (such as upgrading the host software version or board), the initial configuration might be different from the current configuration. Then you should save the initial configuration in time to avoid the loss of some configuration commands.

The following commands can be used in all views.

Table 24 View router configuration

Operation	Command
View the initial configuration of the router	display saved-configuration
View the current configuration of the router	display current-configuration
View the current system configuration of the router	display current-configuration global
View all the current interface configuration of the router	display current-configuration interface type [number]
View the current IP routing and routing policy configuration of the router	display current-configuration ip { route route-policy }
View all the routing protocol configuration of the router	display current-configuration protocol protocol
View the current IKE proposal configuration of the router	display current-configuration ike-proposal
View the current IPSec policy configuration of the router	display current-configuration ipsec-policy
View the current IPSec proposal configuration of the router	display current-configuration ipsec-proposal
View the current fr-class configuration of the router	display current-configuration fr-class
View the current voice configuration of the router	display current-configuration voice { aaa access-number acct-method cdr }

View and Select the Storage Media of Configuration File

The the 3Com Router series has two kinds of media, i.e. Flash and NVRAM, to store configuration files. Either can be selected with the **configfile** command to serve as the storage media of configuration file. The current media can be viewed by the **display current-configuration** command.

Please use the following commands in corresponding views.

Table 25 Select and view the storage media of configuration file

Operation	Command
Select the storage media of configuration file (in system view)	configfile { flash nvr am }
View the storage media type of current configuration file (in all view)	display configfile

If there is only one type of storage media available, the **configfile** command will not be effective.

Modify and Save Current Configuration

Users can modify the current configuration of the router via the command line interface. To save the current configuration as initial configuration for the next power-on, use the **save** command to save the current configuration in Flash or NVRAM, which will be decided by the **configfile** command.

Please use the following command in system view.

Table 26 Save current configuration

Operation	Command
Save current configuration	save

Erase Configuration File in Storage Media

The **delete** command can be used to delete the configuration file in Flash or NVRAM of the router. After deleting the configuration files, the router will use the default configuration parameters for initialization during the next power-on. The configuration file in Flash or NVRAM can be deleted in the following cases:

- After upgrading, if the router software does not match with the configuration file.
- If the configuration file in Flash or NVRAM is damaged, for example, the wrong configuration file is loaded.

Please use the following command in system view.

Table 27 Erase the configuration file in storage media.

Operation	Command
Erase the configuration file in storage media	delete

Set the Flag Bit to Enter the Initial Setup Mode

first-config set is used to set the flag bit of the initial setup. After the flag bit is set, the router will delete the config files in Flash or NVRAM before the system enters setup mode, in case of powering off, and reset. The operation is similar to the **delete** command.

first-config reset is used to cancel the setting of the flag bit.

Do not use this command before the **save** command, which also cancels the setting of the flag bit.

Use these commands in system view.

Table 28 Set/clear the flag bit to enter the initial setup

Operation	Command
Set the flag bit to enter initial setup mode	first-config set
Clear the flag bit of initial setup mode	first-config reset

By default, no flag bit for entering the initial setup mode is set.

Configure FTP

FTP (File Transfer Protocol), which belongs to the application layer protocol in the TCP/IP protocol suite, mainly provides file transfer between remote hosts. Borne on TCP, FTP provides reliable and connection-oriented data transfer service but does not provide access authorization and authentication mechanism.

When the client originates control connection to a server (with port command) and establishes control connection with the server port numbered 21 via an arbitrarily allocated local protocol port number, this connection will be reserved until data transfer is complete. The server establishes data connection with the client via port 20 and transfer data.

The 3Com Router 1.x provides FTP service, that is, the router serves as the FTP server. Users can run the FTP client application and logon to the router to access files on the router.

Before using FTP, users need to install the FTP Client application. You need to purchase the FTP Client application as this is not supplied as part of the 3Com Router series.

Configure FTP Server

FTP server configuration includes:

- Configure authentication and authorization of the FTP server
- Start FTP server
- Upload the configuration file/program file
- Download the configuration file/program file
- Configure the running parameters of FTP server

Configure authentication and authorization of FTP server

1 Set the authentication mode of the FTP server

The authorization information of the FTP server is the top-level working directory of FTP users. Only authenticated and authorized users can enjoy the service of the FTP server. The 3Com Router 1.x configures authentication and authorization of the FTP user using AAA. If no AAA is configured, the local user authentication is adopted by default.

When using AAA, the router cannot perform local accounting. Therefore, when using local authentication, you need to open the accounting option switch to disable the accounting function.

Please configure with the following commands in system view.

Table 29 Set the authentication mode of FTP server

Operation	Command
Start AAA server	aaa-enable
Disable AAA server	undo aaa-enable
Turn on the accounting selection switch	aaa accounting-scheme optional
Turn off the accounting selection switch	undo aaa accounting-scheme optional
Set local authentication for PPP connection	aaa authentication-scheme login default local

2 Add FTP authorized user name and password

Input the following command in system view.

Table 30 Add FTP authorized user name and password

Operation	Command
Add FTP authorized user name and password	local-user username service-type ftp password {simple cipher } password
Delete FTP user	undo user username

For a detailed introduction to the above command, please refer to the chapter "AAA and RADIUS Configuration" in the Security section of this manual.

Start FTP Server

The FTP server can be started after configuring the authentication and authorization of the FTP server. The FTP server supports multi-user access simultaneously. The remote FTP user sends a request to the FTP server, which will execute a corresponding action and return the execution result to the user.

Enter the following commands in system view.

Table 31 Start FTP server

Operation	Command
Start FTP server	ftp-server enable
Disable FTP server	undo ftp-server

Configure Parameters of FTP Service

Configure FTP service parameters according to system running status, so as to make proper use of system resources.

1 Set the file name on FTP server

Before the file is uploaded or downloaded, the name of the program/configuration file should be set on the router.

Please enter the following commands in system view.

Table 32 Set the file name on FTP server

Operation	Command
Set the program file name on FTP server	ftp-server system-name file-name
Set the configuration file name on FTP server	ftp-server config-name file-name

The names of the program/configuration file are “system” and “config” respectively by default. In the command, *file-name* is a character string with the length of 1 to 30.

2 Set FTP update mode

When logging onto the FTP Server from a PC, you can use the **put** command to upload the file. The FTP Server adopts two update modes: fast update mode and normal update mode.

- Fast update mode: In this mode, after the FTP Server has received the files uploaded by the user, it will write the files into Flash. Even when the power is disconnected during the period of transmitting the files, the existing files in the router will not be destroyed.
- Normal update mode: In this mode, the FTP Server writes the files uploaded by the user into Flash as it receives the files. The existing files in the router may be destroyed due to power disconnection. Compared with fast update mode, the system demands less empty memory in the router when working in normal update mode.

Please perform the following configuration in system view.

Table 33 Set FTP update mode

Operation	Command
Set FTP update mode	ftp-server update { fast normal }

By default, the FTP server adopts fast update mode.

3 Set the connection time limit of FTP service.

To prevent illegal access by unauthorized users, if no service request from the FTP client is received within a certain period, connection with this FTP client will be disconnected.

Please enter the following command in system view.

Table 34 Set the connection time limit of FTP service

Operation	Command
Set the connection time limit of FTP service	ftp-server timeout seconds

The connection time limit of FTP server is 600 seconds by default.

Force to shut down FTP process

In some cases (such as use of FTP by a malicious user), the administrator user logging from the Console port can use **kill ftp** command to disconnect the link from the FTP user to the router. Use caution when executing this command.

Please perform the following configuration in system view.

Table 35 Force to shut down FTP process

Operation	Command
Force a shut down of the FTP process	kill ftp

Display FTP Server Table 36 Display FTP server

Operation	Command
Display the configuration status of current FTP server	display ftp-server
Display detailed information of the FTP user	display local-user

4

TERMINAL SERVICE

This chapter includes information on the following topics:

- Terminal Service Overview
- Terminal Message Service
- Dumb Terminal Service
- Terminal Service of Telnet Connection
- Rlogin Terminal Service
- X.25 PAD Remote Access Service

Terminal Service Overview

The terminal services provided by the 3Com Router to access the command line interface are as follows:

- Perform terminal configuration via Console port
- Perform terminal configuration via asynchronous serial port
- Perform terminal configuration via Telnet connection
- Perform terminal configuration via RLogin connection
- Perform remote login via X.25 PAD
- Perform terminal message service

Features of Terminal Service at Console Port

The Local configuration environment can be established via the console port. Please refer to Chapter 2 "3Com Router User Interface" for specific method.

The features of the terminal service at the console port are shown in the following table. Parameters of the terminal program running on the computer should be set according to this table.

Table 37 Features of terminal service at console port

Service type	Features
Echo mode	No local echo
Terminal emulation type	VT100
Baud rate	9600 bps
Data bit	8 bits
Parity check	None
Stop bit	1 bit
Flow control	None
Binary transmission protocol	Xmodem

Features of Terminal Service at Async Serial Port

The 3Com Router supports remote configuration on the router via asynchronous serial port (including synchronous/asynchronous serial port, 8/16 asynchronous serial port, and AUX port). Please refer to Chapter 2 “3Com Router User Interface” of this manual for the specific method to establish the configuration environment.

The remote terminal service features of the asynchronous serial port are shown in the following table. Parameters of the terminal program running on the computer should be set according to this table, and parameters such as baud rate, data bit, parity check and flow control should be consistent with those of corresponding router interfaces.

Table 38 Remote terminal service features of the asynchronous serial port

Service	Features
Echo mode	No local echo
Terminal emulation type	VT100
Baud rate	Consistent with interface configuration, 9600 bps by default
Data bit	Consistent with interface configuration, 8 bits by default
Parity check	Consistent with interface configuration, no parity by default
Stop bit	Consistent with interface configuration, 1 bit by default
Flow control	Consistent with interface configuration, no flow control by default

Set the Attributes of Terminal Service

Usually, the terminal user connected via the console port can last for 3 minutes. The time for the dumb terminal user can last for 10 minutes. For the user who uses the dummy terminal in dial-up mode, the disconnection timeout is 6 minutes but the user can disable this function by using the `undo idle-timeout` command so that all the terminal users will never be disconnected.

Perform the following configuration in system view.

Table 39 Set the attributes of terminal service

Service	Attribute
Enable the function of timeout disconnection from the terminal user	<code>idle-timeout</code>
Disable the function of timeout disconnection from the terminal user	<code>undo idle-timeout</code>

By default, the system will enable the timeout disconnection of the terminal user.

Terminal Message Service

Whenever the terminal users that log into the same router want to communicate with each other, they can use the terminal message service to send messages. The remote users can telnet onto the local router to transmit information such as simple configuration files and description characters that are not easily expressed through telephones among terminal users, using the `send` command. It is much more convenient than email. Ensuring information security and reliability, the terminal message service fulfills information interaction among multiple terminals on one router.

For example, user A and user B respectively log into Router A and Router B. If user A wants to communicate some information (such as configuration information)

with user B, user A should telnet onto Router B and execute the **send** command to send the related information in all views. Then user B can receive the “message” sent from user A. If user B does not want to receive additional similar messages, they can use the **send switch** command to disable the function of receiving messages.

Configure Terminal Message Service

Terminal message service configuration includes:

- Send message to terminals
- Enable/disable receiving messages from other terminals

1 Configure to send a message to terminals

Perform the following configuration in all view.

Table 40 Send a message to terminals

Operation	Command
Send a message to all the terminals	send

Press *Ctrl+W* to terminate inputting the message, and the system will ask the user whether to send the message to all the terminal users:

```
Send message? [confirm]
```

Press *Enter*, *Ctrl+W*, *y*, or *Y* to confirm the sending. Press *Ctrl+C* or other characters to give up the sending.

The terminal message service supports the following features:

- Supports the users that login through Telnet or console port to use the message services.
- Supports the input of multiple lines of messages.
- Supports the screen paste on HyperTerminal.
- Supports using the backspace button to modify the message input in a line.
- Does not support the control keys such as *Insert*, *Delete*, \uparrow , \downarrow , \leftarrow , \rightarrow *Home*, *End*, and *Tab*.
- Displays the prompt information when users input *?*, *h* or *H*.

2 Enable/disable receiving messages from other terminals

In the terminal message service, receipt of messages from other terminals is determined by the **send switch** command. If the terminal message service is currently enabled, it will be disabled after a second input of this command.

Perform the following configuration in all views.

Table 41 Enable/disable receiving messages from other terminals

Operation	Command
Enable/disable receiving messages from other terminals	send switch

By default, the terminal message service is enabled to receive messages from other terminals

Display Terminal Message Service

Perform the following configuration in all views.

Table 42 Display the terminal message service

Operation	Command
-----------	---------

Display the current status of terminal message service	<code>send status</code>
--	--------------------------

Typical Example of Terminal Message Service Configuration

```
# Input the send command in system view.
[Router] send
Enter message, end with CTRL/Z; abort with CTRL/C:
# Input the contents of the message that the terminal will send.
hello world # (Enter <Ctrl+W> to terminate the message input )
end message? [confirm]
```

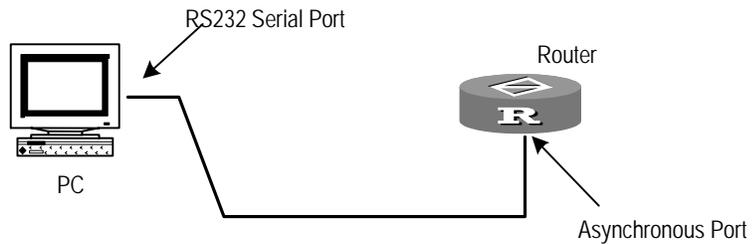
Press *Enter*, *Ctrl+W*, *y*, or *Y* to confirm the sending. Press *Ctrl+C* or other characters to give up the sending.

Dumb Terminal Service

When the asynchronous serial port (such as synchronous/synchronous serial port, AUX port) of the router operates in flow mode, the command line interface (CLI) of the router can be used to carry out configuration of the router. This is achieved by directly connecting the RS-232 serial port with the asynchronous serial port of the router. This is called the dumb terminal operation mode.

As shown in the diagram below, the user can connect with any asynchronous serial port and log in to the router by running the hyper terminal on PC to carry out the configuration management of the router.

Figure 26 Configuration management through dumb terminal



The typical method of terminal access is:

- The asynchronous port working under the flow mode is connected to the RS-232 serial port via dedicated line to enter the router command line interface thereby providing another mode of configuring routers besides the mode of console port and Telnet mode.
- Based on the dumb terminal, other applications can be built, for instance, logging on to other equipment by executing the Telnet command.

Configure Dumb Terminal Service

Follow these steps to configure a dumb terminal service.

1 Configure dumb terminal service

For the synchronous/asynchronous serial port, `physical-mode async`, `async mode flow`, and `undo modem` should be set first.

Perform the following configuration in the interface view.

Table 43 Configure dumb terminal service

Operation	Command
-----------	---------

Configure the synchronous/asynchronous serial work in asynchronous mode	physical-mode async
Configure the serial interface of the router to be in flow mode	async mode flow
Forbid modem to dial in or dial out	undo modem

By default, no dumb terminal service is configured.

2 Configure **auto-execute command** command

If the **auto-execute command** command is configured on the asynchronous serial interface, when you press *Enter* twice on the external terminal connected to the interface or log onto the router in modem dial-up mode and press *Enter* twice, the router will automatically execute the operation preset by the **auto-execute command** command.

If the router is configured with the **auto-execute command** command, you will not be allowed to log into the configuration interface of the router. If the command cannot be executed, you will return to the interface with the prompt *Press ENTER to get started*, and after you press *Enter*, the command will be executed.

Please perform the following configurations in asynchronous serial interface view.

Table 44 Configure **auto-execute command** command

Operation	Command
Configure the auto-execute command command on the asynchronous serial interface	auto-execute command command
Remove this command	undo auto-execute command command

By default, the **auto-execute command** command is not configured.

Configuration Examples of Dumb Terminal Service

Configure Dumb Terminal

- The configuration procedure of the dumb terminal on sync/async serial 0 ports is as follows:

```
[Router-Serial0] physical-mode async
[Router-Serial0] undo modem
[Router-Serial0] async mode flow
```

- The configuration procedure of the dumb terminal on 8/16 async serial 0 port is as follows:

```
[Router-Async0] undo modem
[Router-Async0] async mode flow
```

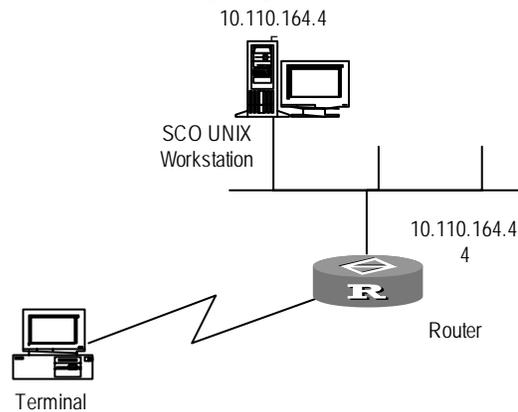
- The configuration procedure of the dumb terminal on AUX port is as follows:

```
[Router-Aux0] undo modem
```

After the above operation, *Press ENTER to get started* displays on the terminal connected to this async interface, press *Enter* twice to enter the router configuration interface. During the configuration, you can click *logout* to exit the command line interface and can also click *Enter* twice to return.

Configure Auto-execute command

The user can use the Telnet command specified by the **auto-execute** command to log on the remote SCO UNIX workstation after establishing the connection with the Router via the dumb terminal.

Figure 27 Dumb terminal networking diagram

- 1 Configure the interface to dumb terminal mode.

```
[Router-Serial1] physical-mode async
[Router-Serial1] undo modem
[Router-Serial1] async mode flow
```

- 2 Configure the **auto-execute command** command.

```
[Router-Serial1] auto-execute command telnet 10.110.164.45
```

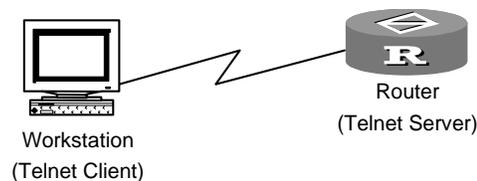
After the configuration, press *Enter* twice on the terminal connected to this async interface to log on the SCO UNIX host 1.110.164.45. During the configuration, you can click *exit* to exit the command line interface and can also click *Enter* twice to return.

Terminal Service of Telnet Connection

Telnet Overview

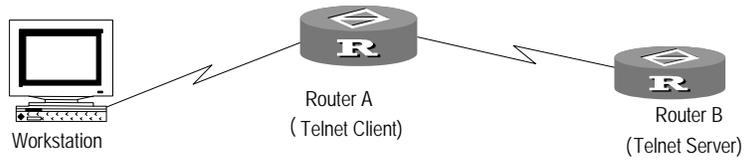
Telnet protocol, which belongs to the application layer protocol in the TCP/IP protocol suite, describes how to provide telnet and virtual terminal functions via the network. Telnet connection services provided by the 3Com Router 1.x include:

- Telnet Server service: provides services for local and remote users to logon to the router, maintains the router and accesses network resources. As shown in the following figure, users can logon to the router by running the Telnet client program on the computer and perform the configuration management for the router.

Figure 28 Telnet server service

- Telnet Client service: provides service for local or remote users who have logged on to the local router to access other remote system resources by using the Telnet Client program of the local router. As shown in the following figure, users can re-logon to router B using the Telnet command and perform configuration management after establishing a connection with router A via the terminal emulator or Telnet program on the computer.

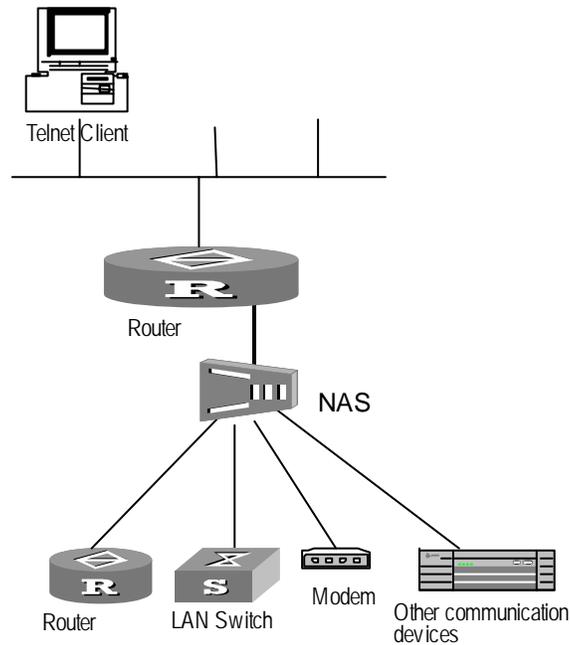
Figure 29 Telnet client service



Reverse Telnet Overview

Reverse Telnet service: the user logs on the router with a specified port number by running the Telnet client program on the PC. Then the connection to the serial port device connected with the async port of the router is established. One example: the 3Com Router performs remote configuration and maintenance of the external devices connected with its 8/16 asynchronous port with Reverse Telnet service.

Figure 30 Reverse Telnet service



Connection Configuration of Telnet and Reverse Telnet

Terminal Service Features of Telnet Connection

The terminal service features of Telnet connection are shown in the following table, and the parameters of the Telnet Client program running on the computer should be set according to the table.

Table 45 Terminal service features of telnet connection

Service	Value
Input mode	Character mode
Echo mode	No local echo
Terminal type	VT100

Establish Telnet Connection

Please use the following commands on the Telnet Client program of the host and in r system view.

Table 46 Establish Telnet Server or Telnet Client connection

Operation	Command
Enable the Telnet Client connection service	<code>telnet host-ip-address [service-port]</code>

By default, Telnet Server starts automatically. The default value of *service-port* is 23.

To terminate Telnet service, enter *Ctrl+] at Telnet Client side.*

Setup Reverse Telnet Connection

Please use `async mode flow` and `undo modem` commands in asynchronous interface view, use `telnet` and `terminal telnet refuse-negotiation` commands in system view, use `reverse-telnet disconnect`, `reverse-telnet timeout`, `reverse-telnet listenport` and `reverse-telnet return-deal` commands in interface view.

Table 47 Enable Reverse Telnet connection

Operation	Command
Forbid the modem to dial in or dial out	<code>undo modem</code>
Set the router to flow mode	<code>async mode flow</code>
Log onto the router at specified port and connect to corresponding async port	<code>telnet host-ip-address service-port</code>
Disable/Enable the option negotiation towards the Telnet client	<code>terminal telnet refuse-negotiation</code>
Configure the timeout of Reverse Telnet	<code>terminal telnet timeout</code>
Configure the Reverse Telnet timeout of the interface	<code>reverse-telnet timeout time</code>
Disconnect the Reverse Telnet of the interface	<code>reverse-telnet disconnect</code>
Do not send the carriage return received from the telnet end to the terminal	<code>reverse-telnet return-deal from-telnet</code>
Do not send the carriage return received from the terminal to the telnet end	<code>reverse-telnet return-deal from-dumb</code>

By default, the option for negotiation towards the Telnet client is enabled, and Reverse Telnet will expire in 600 seconds. Reverse Telnet transparently transmits all data. The interface use the default listen port number.

Reverse Telnet timeout ensures that if no data is transmitted during a specified time, the established Reverse Telnet will disconnect automatically. By default, no timeout is configured for the Reverse Telnet, that is, as long as the Reverse Telnet is connected, even if there is no data being transmitted, the Reverse Telnet will not be disconnected.

The Reverse Telnet can be disconnected in interface view.



The `undo modem` command must be used to disable modem calling-in and calling-out before the Reverse Telnet timeout of the configuration interface is configured.



On the 3Com Router series, the maximum number of Reverse Telnet connections is related to the interface card and the maximum number of tasks supported by the router.



The interface listen port number is within the range of 1025 to 65535. Please note that the listen port number cannot be the same as that of the widely used ports. By default, the port number and asynchronous interface have the following relations:

- The async serial interface number starts from 2001. For instance, the first async serial interface number is 2001, the second is 2002, and so on.
- The AUX interface number is 3000.
- The sync serial interface number starts from 3001. For instance, the first sync serial interface number is 3001, the second is 3002, and so on.

Force shut down Telnet Process

In some cases (such as usage of Telnet by a malicious user), the administrator user logging from the Console port can use the **kill telnet** command to disconnect the link from the Telnet user to the router or disconnect the link according to the process number found through the **display client** command. Use caution when executing this command.

Please perform the following configuration in system view.

Table 48 Force to shut down Telnet process

Operation	Command
Force to shut down Telnet process	kill telnet { all userID userid }

Display and Debug Reverse Telnet Connection

Perform the following configuration in all views.

Table 49 Establish Telnet Server or Telnet Client connection

Operation	Command
Display information of Telnet clients	display client
Display information of Telnet connection	display tcp status

display client can only be used to display the interface through which the Telnet client connected to the router passes. If you want to view the IP address of the Telnet server connected to the router, you should execute the **display tcp status** command. The TCP connection whose local port number is 23 is the Telnet connection, including the Telnet client connection and Telnet server connection.

Typical Configuration Example of Telnet and Reverse Telnet

Example of Telnet

In the networking diagram shown in Figure 28 "Telnet server service", the host establishes connection with router A (IP address 10.110.0.1), then logs on and configures router B (IP address 129.102.0.1).

- 1 Execute the following commands on the user host and Telnet to Router A.

```
C:\WINDOWS>Telnet 10.110.0.1
```

- 2 Execute the following commands in the popup Telnet window, and log onto Router B.

```
[RouterA] telnet 129.102.0.1
Trying 129.102.0.1 ... (use CTRL + C to break)
Connected to 129.102.0.1
Service port is 23 .
Username: guest
```

```
Password:
User guest logged in .
```

- 3 The message showing successful Telnet to Router B should pop up and display the host name of RouterB.

```
[RouterB]
```

Example of Reverse Telnet

The host is connected to the router, then communicates with the device connected to the seventh asynchronous serial interface of the router. The IP address of the router is 10.110.164.44.

```
[Router] telnet 10.110.164.44 2007
Trying 10.110.164.44...
Service port is 2007 (tty)
Connected to 10.110.164.44
```

After successful Reverse Telnet, host name of RouterB will be displayed.

```
[RouterB]
```

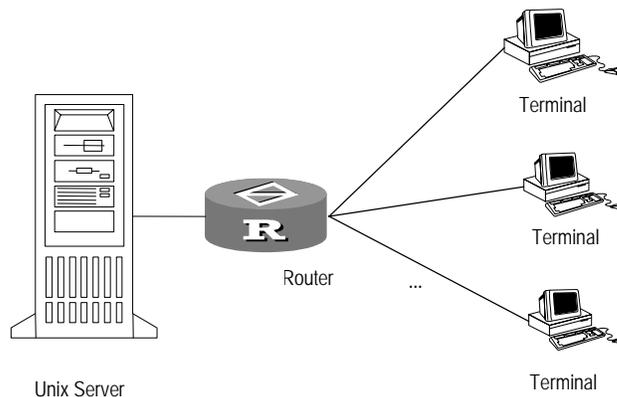
The host can send commands to communicate with the device connected to the asynchronous serial interface. If a modem is connected to the interface, you can detect the modem status or configure the modem by using the AT command.

Rlogin Terminal Service

Rlogin (Remote Login) is one of the most common Internet applications developed by the BSD UNIX system, in which a client is connected with the server by TCP connection. It provides the function of several remote terminals accessing the UNIX host. Rlogin originated from Berkeley UNIX and is used for telnet service between UNIX systems. Compared with Telnet protocol, it is easier to implement and use Rlogin protocol.

The 3Com Router implemented by Rlogin is Client-based. Rlogin Client enables 3Com Router series to have functions similar to that of a multi-serial port card, i.e., digital or analog terminals that log onto routers through the terminal access functionality and can use Rlogin protocol to log onto a remote UNIX host.

Figure 31 Connect Unix Server and Terminal through the 3Com Router



The Rlogin client provided by the 3Com Router series has the following features:

- Only supports IP address configuration. DNS is not supported.
- The supported terminal type is VT100.
- The supported baud rate is 9600 bps.
- Supports remote access of user terminals connected with the asynchronous serial port under the flow mode by asynchronous private line or modem dial-up and supports the maintenance of terminals connected with Console port. Remote access of the terminals connected with routers in other means (such as through telnet) is not supported.
- The function of activating multiple Rlogin sessions at the same user terminal is not provided.

Configure Rlogin Please implement the following configuration in system view.

Table 50 Establish a Rlogin connection

Operation	Command
Establish a Rlogin connection	<code>rlogin ip-address [username]</code>
Shut down a Rlogin connection	<code>exit</code>

Typical Rlogin Configuration Examples

Use local user name abc to log on

```
[Router] rlogin 10.110.96.53 root
Trying 10.110.96.53 ...
Password:
Last successful login for root: Thu Jan 30 20:29:45 2003 on tty2
Last unsuccessful login for root: Sun Jan 26 11:21:53 2003
```

SCO OpenServer(TM) Release 5

(C) 1976-1998 The Santa Cruz Operation, Inc.

(C) 1980-1994 Microsoft Corporation

All rights reserved.

For complete copyright credits,
enter "copyrights" at the command prompt.

```
you have mail
TERM = (vt100)
Terminal type is vt100
# exit
```

rlogin: connection closed.

Use local user name abc and enter the wrong password for the first time

```
[Router] rlogin 1.1.254.78
Trying 1.1.254.78 ...

Password:      ( enter Wrong password)
Login incorrect
Wait for login retry:
login: abc
Password:      (enter correct password)
```

```
Last successful login for root: Thu Sep 06 15:14:15 2001 on tty0
Last unsuccessful login for root: Thu Sep 06 14:22:35 2001 on tty0
```

```
SCO OpenServer(TM) Release 5
(C) 1976-1998 The Santa Cruz Operation, Inc.
(C) 1980-1994 Microsoft Corporation.
All rights reserved.
```

```
For complete copyright credits,
enter "copyrights" at the command prompt.
```

```
you have mail
Terminal type is vt100
#
```

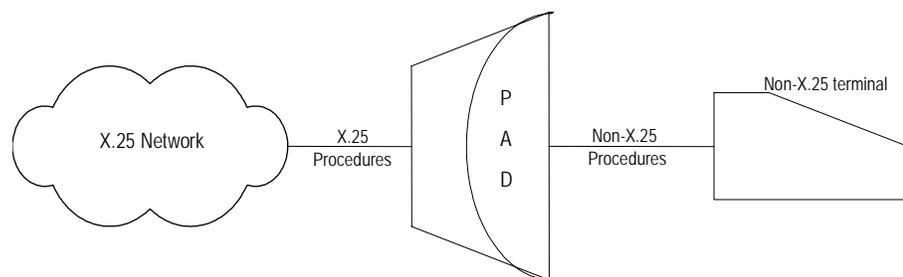
X.25 PAD Remote Access Service

PAD (Packet Assembly/Disassembly facility) is a definition specific to X.25 protocol.

The traditional X.25 network requires that all its terminals are of X.25 type, and relevant hardware and software are needed to support X.25 protocol, which are the so-called packet terminals. Packet terminals must be intelligent ones, but many terminals uses are either non-X.25 or not intelligent (such as keyboard, monitor, printer, etc.) or intelligent but do not support X.25 procedures. In that case it is impossible for non-X.25 terminals to interconnect with each other through the X.25 network, or even access the X.25 network. X.25 PAD technology was developed to address how these devices can be enabled to communicate via X.25 network.

X.25 PAD bridges the X.25 network and non-X.25 terminals — it provides a mechanism through which non-X.25 terminals can access the X.25 network. As shown in the figure below, a PAD is positioned 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.

Figure 32 Access function of PAD



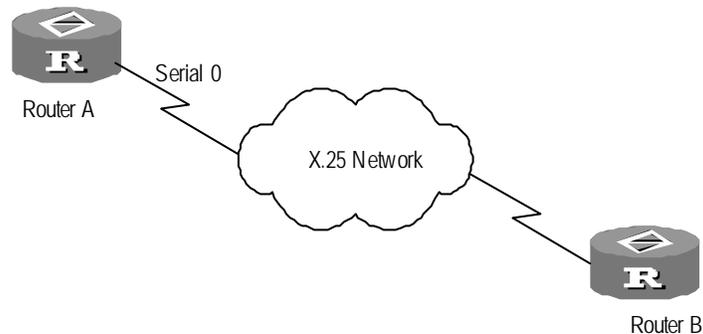
The main functions of the X.25 PAD are to:

- Provide support to X.25 procedures and accordingly to connect and communicate with the X.25 network.
- Provide support to non-X.25 procedures and accordingly to connect non-X.25 terminals.
- Provide non-X.25 terminals with functions of call establishment, data transmission and call clearing through the X.25 network.
- Provide non-X.25 terminals with functions of observing and changing interface parameters so as to adjust to the requirements of varied terminals.

Therefore X.25 PAD devices actually serve as a procedure translator or network server, providing services to different terminals and helping them to access the X.25 network.

The 3Com Router implements X.29 and X.3 protocol in the X.25 PAD as well as in the X.29 protocol-based Telnet application and the users can configure routers without geographical limitation, as shown in the figure below. When the user, for the sake of security, is unable to use IP protocol-based Telnet to configure routers, they can access a remote router through X.25 PAD for the configuration.

Figure 33 Access remote router through an X.25 PAD



Configure X.25 PAD

The X.25 PAD configuration includes:

- Configure X.25 PAD remote users
- Enable AAA authentication of X.25 PAD remote users
- Place the X.25 PAD call and access the remote terminal
- Set the response time for the Invite Clear message

Configure X.25 PAD remote user

Since remote PAD users can place an X.25 PAD call through the X.25 network, access the local router, and configure the router, it may be necessary to authenticate the validity of remote users. You can configure X.25 remote users with access permission on the router for the purpose of authentication on receiving the remote PAD request.

This command is not necessary, but if required, it must be used together with the **login pad** command.

The called end (also called the configured end) is defined as the Server side, and the calling end (also called the configuration end) is defined as the Client side.

Please implement the following configuration under the system view at the Server side.

Table 51 Configure X.25 PAD remote user

Operation	Command
Configure X.25 PAD remote user	local-user user-name service-type type [password { simple cipher } password]
Cancel the completed configuration of X.25 PAD remote user	undo local-user user-name

By default, no X.25 PAD remote user is configured at the Server side.

For details of the Command, refer to the relevant sections on Security Configuration Commands in *Command Reference (V1.6)*.

Start AAA authentication of X.25 remote users

After the configuration of X.25 PAD remote users, AAA authentication is started at the Server side for the purpose of identity authentication on receipt of a remote PAD request.

This command is not mandatory, but if required, it must be used together with the **user** command.

Please implement the following configuration under the system view at the Server side.

Table 52 Enable AAA authentication for X.25 remote PAD users

Operation	Command
Enable AAA authentication of X.25 remote user	login pad
Disable AAA authentication of X.25 remote user	undo login pad
Enable AAA authentication	aaa-enable
Configure user name and password	local-user username password password

By default, there is no AAA authentication for X.25 remote PAD users.

Establish an X.25 PAD call

In the routers interconnected through X.25 network, the following commands are used to place a PAD call to remote terminals. If both terminals support X.25 PAD, the call will be authenticated at the Server side. (If user authentication is not set, this step can be skipped.). If the authentication succeeds, the Client side can access the Server side and configure the Server side. After successful access of the remote terminals, users can log out and disconnect the X.25 PAD connection.

Please implement the following configuration under the system view at the Client side.

Table 53 Establish a X.25 PAD call

Operation	Command
Establish a X.25 PAD call	pad x.121-address
Exit X.25 PAD login	exit

If a call successfully logs on, the user can, at the Client side, access the Server.

pad command can be nested with itself or with the **telnet** command, that is, the user can place an X.25 PAD call on a router and access another router, from which they do the same and access a third router. Or, the user first Telnets to a router from which they can place X.25 calls and access a third router. Or, users can place X.25 calls, access a router and then telnet to another router, and so on. It is recommended to limit the nesting to three times to ensure normal transmission.

Exit command can also be nested with the **Pad** command. That is, users can access a third or even more routers from a router by repeatedly using the **telnet/pad** command or by repeatedly using the **exit** command to exit the routers being accessed in turns until returning to the one from which the first call is placed.

Please implement the following configuration under the system view at the Server side.

Set the Response Time to the Invite Clear Message

If for some unknown reason (for example, the Client side gives an exit request or needs to release link resources) after the Server side of the X.25 PAD sends the link-clearing message Invite Clear to the Client side, the Server side will wait for a response from the Client side. If the Client side fails to respond to the message within the specified time, the Server side will clear the link positively.

Please implement the following configuration under the system view at the Server side.

Table 54 Set the response time to the Invite Clear message

Operation	Command
Set the response time to the Invite Clear message	x29 inviteclear-time <i>time seconds</i>

Display and Debug X.25 PAD

Perform the following configuration in all views.

Table 55 Display and debug X.25 PAD

Operation	Command
Display the relevant information of X.25 PAD	display x25 pad [<i>pad-number</i>] [<i>tty</i>]
Enable the debugging of X.25 PAD on varied levels	debugging pad { <i>packet</i> <i>error</i> <i>all</i> }

Typical X.25 PAD Configuration Example

I. Networking Requirement

As shown in the figure below, with Serial 0 as the interface to the X.25 network, router A is connected with router B through the X.25 network. It is required that router B can access and configure router A after it calls router A.

II. Networking Diagram

As shown in Figure 33 "Access remote router through an X.25 PAD".

III. Configuration Procedure

1 Configure RouterA:

- a Configure X.25 PAD remote users.

```
[RouterA] local-user paduser service-type exec-guest password simple pad
```

- b Enable AAA authentication of X.25 PAD remote users.

```
[RouterA] login pad
```

- c Enter the view of interface Serial 0 and set its link layer protocol as X.25 DTE IETF.

```
[RouterA]interface serial 0
[RouterA-serial0]link-protocol x25 dte ietf
```

- d Set its X.121 address as 123456.

```
[RouterA-serial0]x25 x121-address 123456
```

2 Configure Router B:

- a Enter the view of interface Serial 0 and set its link layer protocol as X.25 DTE IETF.

```
[RouterB]interface serial 0
[RouterB-serial0]link-protocol x25 dte ietf
```

- b Set its X.121 address as 5678.

```
[RouterB-serial0]x25 x121-address 5678
```

- c Return to the system view and place the X.25 PAD call to router A

```
[RouterB] pad 123456
Trying 123456...Open
Username:paduser
Password:
User paduser logged in.
[RouterA]
```

Fault Diagnosis and Troubleshooting of X.25 PAD

Fault one: If after X.25 calls a remote terminal, logon fails. The screen displays Trying xxxxxxxxxxxx...Destination unreachable.

Troubleshooting: Follow the steps below.

- X.25 protocol is encapsulated on the serial port that is used for connection and both ends support X.25 PAD protocol.
- After the above condition is met, make sure that the serial port at the Server side used to receive X.25 calls has set the X.121 address and the address is correctly called at the Client side.
- After the above conditions are satisfied, then you should confirm that the serial interface used to accept the X.25 PAD calls at the Server end has specified the X.121 address, and the Client has correctly called this address.
- If the above condition is also satisfied, please check if the Client side has set switch attributes (i.e., **x25 switching** command is used under system view), but does not set the route to the Server side. If so, the data cannot be transmitted from the Client side to the Server side in the packet mode. It is not mandatory for the Client side to configure the route to access the Server, though. If the Client side does not configure switch attributes, X.25 will choose the default route for the call. Therefore, please confirm that the Client side is not configured with the switch attributes or the Client side is configured with the switch attributes as well as the route to the Server side.

5

CONFIGURING NETWORK MANAGEMENT

This chapter includes information on the following topics:

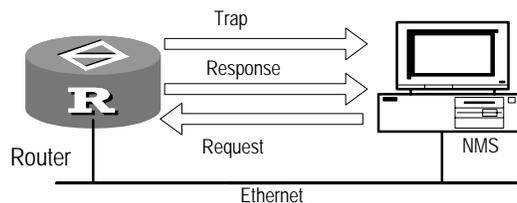
- SNMP Overview
- RMON Overview

SNMP Overview

Simple Network Management Protocol (SNMP), a widely accepted industry standard, is the most dominant network management protocol in computer networks by far. It is developed to ensure transmission of management information between any two nodes, which will facilitate network administrators to search for information at any node on the networks for the purpose of modifying, locating faults, troubleshooting, planning capacity and generating reports. Adopting the polling mechanism, SNMP provides essential functionality, and is suitable for a networking environment requiring small size, high speed and low cost. Since it uses the transport layer protocol UDP (User Datagram Protocol) which requires no acknowledgement, it gains wide support in many products.

SNMP system comprises an NMS (Network Management Station) and an agent. NMS is the workstation running the client application. It sends various request packets to the managed network devices, receives the response and trap packets from the managed devices, and displays status information of the managed devices. The agent is a process running on the managed equipment. It receives and processes the request packets from the NMS, and responds to the NMS by returning the corresponding management variables obtained from the protocol module of the managed equipment. Whenever the agent detects the occurrence of emergency events on the managed device, such as a change in the interface status or a failed call, it will send traps to notify the NMS. The relationship between NMS and agent is shown in the following figure:

Figure 34 Relationship between NMS and agent



SNMP is the most widely applied communication protocol between NMS and Agent in the computer network.

Development of SNMP

There are three versions of SNMP: SNMPv1, SNMPv2c and SNMPv3. SNMPv3 defines a series of access control management functions for network security, in

addition to the functions defined in SNMPv2c and SNMPv1. In other words, SNMPv3 develops SNMPv2c by adding security and management functions.

SNMPv1 and SNMPv2c lack security functions, especially in the aspect of authentication and privacy. SNMPv1 defines only a type of community representing a group of managed devices. Each NMS controls access to the devices via the community name list. However, agents do not verify whether the community names used by the senders are authorized, and they even do not check the IDs of administrators. Additionally, transmission of SNMP messages without encryption, which exposes the community name, brings potential threats to security. Even though some security mechanisms, like digest authentication, timestamp authentication, encryption and authorization, have been considered at the early stage of proposing SNMPv2c, only the "community name" similar to SNMPv1 is used in the final criterion of RFC 1901 through 1908. SNMPv2c is only a transitional version between SNMPv1 and SNMPv3. To avoid the lack of security in SNMPv1 and SNMPv2c, IETF develops the SNMPv3 protocol, which is described in RFC2271 through 2275 and RFC2570 through RFC2575 in details.

RFC2570 through RFC2575 supplements and subdivides SNMPv3 on the basis of RFC2271 through RFC2275, giving a complete and exact description of the processing of abnormal errors and the message processing procedure. The SNMPv3 framework thus defined has become a feasible standard.

Security of SNMPv3 is mostly represented by data security and access control.

- Data security features provided in SNMPv3

Message-level data security provided in SNMPv3 includes the following three aspects:

- Data integrity. It ensures that data will not be tampered with by means of unauthorized modes and the data sequence will only be changed within the permitted range.
- Data origin authentication. It confirms which user the received data is from. Security defined in SNMPv3 is user-based. Hence, it authenticates the users that generate messages instead of the particular applications that are used to generate the messages.
- Data confidentiality. Whenever an NMS or agent receives a message, it will verify when the message is generated. If the difference between the generating time of message and the current system time exceeds the specified time range, the message will be rejected. Thereby, it ensures that the message has not been tampered with in-transit on the network and prevents processing of received malicious messages.

- Access control in SNMPv3

As a security measure, access control defined in SNMPv3 implements a security check on the basis of protocol operations, thereby to controlling access to the managed objects.

MIB accessible to a SNMP entity is defined by the particular context. For security reasons, different groups and corresponding authorities probably need to be defined on one entity. The authorities are specified by the MIB view. A MIB view specifies a collection of managed object types in the context. The MIB view takes the form of a "view sub-tree" to define objects because MIB adopts the tree structure. If the flag of the object to be accessed belongs to the MIB

sub-tree, the network administrator can access the device with read or write authority. Otherwise, the operations will be rejected.

SNMP architecture

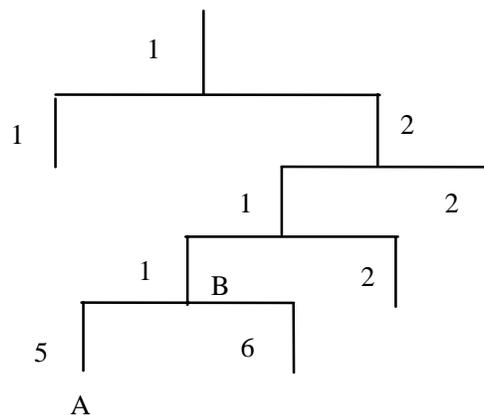
An SNMP entity comprises one SNMP engine and multiple SNMP applications. The SNMP engine is the core of the SNMP entity. It transceives and authenticates SNMP messages, extracts PDU (Protocol Data Unit), reassembles messages, and communicates with the SNMP applications. SNMP applications process PDUs, implement protocol operations, and stores/gets MIB.

The SNMP engine comprises the scheduler, message processing sub-system, security sub-system, and access control sub-system. SNMP applications include the command generator, command responder, indication generator, indication receiver, and proxy transponder. The SNMP entity that owns the command generator or indication receiver is called the SNMP manager, and the SNMP entity that owns the command responder, indication generator or proxy transponder is called the SNMP agent. Nevertheless, an SNMP entity can have functions of both manager and agent.

SNMP-supported MIB

To uniquely identify the equipment management variables in SNMP packets, SNMP identifies the managed objects by using the hierarchical structure to name them. The hierarchical structure is like a tree, in which, the nodes of the tree represent the managed objects. As shown in the following figure, it can use a path starting from the root to identify an object unambiguously.

Figure 35 MIB tree structure



As shown in the above figure, the managed object B can be uniquely specified by a digit string {1.2.1.1}, which is the object identifier of the managed object. Consisting of collections of standard variable definitions of monitored network equipment, MIB describes the hierarchical structure of the tree

SNMP agents in the 3Com Router series support standard network management versions SNMPv1, SNMPv2c, and SNMPv3. MIBs that are compatible with the agents are shown in the following table.

Table 56 3Com Router-supported MIB

MIB attribute	MIB description	Reference
Public MIB	MIB II based on TCP/IP network equipment	RFC1213
	RMON MIB	RFC1757
	RIP-2 MIB	RFC1389
	OSPF MIB	RFC1253
	BGP MIB	RFC1657
	PPP MIB	RFC1471
	X.25 MIB	RFC1382
	LAPB MIB	RFC1381
	PPP	RFC1471, RFC1472, RFC1473, RFC1661, RFC1332, and RFC1334
	FrameRelay MIB	RFC1315 and RFC2115
	SNMP	RFC1907, RFC2271, RFC2272, RFC2273, RFC2273, RFC2274 and RFC2275
Private MIB	IP MIB	
	ICMP MIB	
	QoS MIB	
	NDEC MIB	
	DLSw MIB	
	MIB of terminal access servers	
	MIB of RMON extension alarms	
	3Com Router MIB	
	3Com Module MIB	

Configure SNMP SNMP configuration includes:

- Configure the network management agent on a router
- Configure the information of router administrator
- Configure the SNMP version
- Configure the trap
- Adjust the maximum size of SNMP packets

1 Configure network management agent on a router

Perform the following configurations in system view.

Table 57 Configure network management agent on a router

Operation	Command
Enable SNMP service	snmp - - agent
Disable SNMP service	undo snmp-agent
Set an engine ID for the equipment	snmp-agent local-engineid engineid
Set the engine ID of equipment to the default value	undo snmp-agent local-engineid

By default, the system disables SNMP service.

Engine ID is the unique ID of individual routers on the overall network. It is a string of 5 to 32 bytes in hexadecimal format. By default, the SNMP engine ID is

“ Corporation code of 3Com Corporation. (800007DB) + Equipment information” . Equipment information can be the IP address, MAC address or self-defined hexadecimal digit string.



*You can skip these two operations when you begin to configure SNMP for a router because SNMP service will be enabled once you configure any related SNMP commands (except for the **display** commands). It is equivalent to configuring the **snmp-agent** command. Furthermore, the default engine ID can generally ensure the uniqueness of the router on the network.*

2 Configure SNMP version and related tasks

The 3Com Router series support SNMPv1, SNMPv2c and SNMPv3.

SNMPv1 and SNMPv2c adopt a community name for authentication, and the SNMP packets that are not compliant with the community name authorized by the equipment will be discarded. Different groups can have either the read-only or read-write access authority. A group with the read-only authority can only query equipment information, whereas a group with read-write authority can configure the equipment. The authorities are specified by MIB views.

Security defined in SNMPv3 is user-based hence an SNMP user inherits the authority of the SNMP group to which it belongs. Different NMS have different access authority. An SNMP group can have read-only, read-write or notifying authority. The authorities of the SNMP group are also determined by MIB views.

Perform the following configurations in system view.

Table 58 Configure SNMP version and related tasks

Operation	Command
Select an SNMP version for NMS	<code>snmp-agent sys-info version { v1 v2c v3 all }</code>
Define the SNMP version(s) that NMS are not permitted to use	<code>undo snmp-agent sys-info version { v1 v2c v3 all }</code>
Create or update view information	<code>snmp-agent mib-view { included excluded } viewname subtree subtree</code>
Delete a view	<code>undo snmp-agent mib-view view-name</code>
Set name and access authority for a community	<code>snmp-agent community { read write } community_name [mib-view view-name] [acl number]</code>
Remove the previous community name	<code>undo snmp-agent community community_name</code>
Set an SNMP group	<code>snmp-server group { v1 groupname v2c groupname v3 groupname { authentication noauthentication privacy } } [read-view readview] [write-view writeview] [notify-view notifyview] [acl number]</code>
Delete an SNMP group	<code>undo snmp-agent group { v1 groupname v2c groupname v3 groupname { authentication noauthentication privacy } }</code>
Add a new user to an SNMP group and specify the SNMP version as well as the authentication/encryption mode	<code>snmp-agent usm-user { v1 username groupname v2c username groupname v3 username groupname [authentication-mod { md5 sha } auth-password [privacy-mod des56 priv-password]] } [acl number]</code>

Delete a user from the SNMP group	<code>undo snmp-agent usm-user { v1 username groupname v2c username groupname v3 username groupname }</code>
-----------------------------------	--

By default, SNMPv3 is used. The default view name in the system is ViewDefault, and OID of which is 1.3.6.1. SNMP group has only the read-only authority by default.



If SNMPv1/SNMPv2c is used, the community name or SNMPv1/SNMPv2c groups and users should be configured. If SNMPv3 is used, SNMPv3 groups and users should be configured.



Before configuring an SNMP group, you should first define the view, which will be used for configuring the SNMP group. When configuring the community name, however, specifying a view is optional.

3 Configure information of router administrator

You should correctly configure information describing location and management of the local equipment so that the network administrator can contact the equipment administrator.

Perform the following configurations in system view.

Table 59 Configure information of router administrator

Operation	Command
Set the administrator ID and the contact method	<code>snmp-agent sys-info contact string</code>
Restore the default administrator ID and the contact method	<code>undo snmp-agent sys-info contact</code>
Set router location information	<code>snmp-agent sys-info location string</code>
Restore the default router location	<code>undo snmp-agent sys-info location</code>

4 Configure traps to be sent by the router

Traps are unsolicited messages that a managed device sends to an NMS for reporting some urgent and significant events. When a router works as a managed device, you should configure the destination and source addresses of the trap that it will send. The destination address is the IP address of the NMS receiving the trap packet, and the source address is the address of the local router, that is, the address of an interface on the local router.

Perform the following configurations in system view.

Table 60 Configure the traps to be sent by the router

Operation	Command
Enable the router to send traps	<code>snmp-agent trap enable [trap-type]</code>
Disable the router to send traps	<code>undo snmp-agent trap enable</code>
Specify the interface whose address is bound as the source address in the trap messages	<code>snmp-agent trap source interface-type interface-number</code>
Remove the interface whose address is bound as the source address in the trap messages	<code>undo snmp-agent trap source</code>

Set the address of host receiving the traps	snmp-agent target-host trap address host-addr [port port] [parameters { v1 v2c v3 { authentication noauthentication privacy } }] securityname name
Remove the address of host receiving the traps	undo snmp-agent target-host trap address host-addr [port port] securityname name
Set the message queue length of traps destined to a host	snmp-agent trap queue-size length
Restore the default message queue length	undo snmp-agent trap queue-size
Set the timeout time for traps	snmp-agent trap life timeout
Restore the default timeout time for traps	undo snmp-agent trap life

By default, the router is disabled to send traps.

- Configure the maximum size of SNMP packets that the router can send/receive
Set the Max SNMP messages that can be received/sent by the agent according to the network loading capacity.

Perform the following configurations in system view.

Table 61 Configure the maximum size of SNMP packets that the agent can send/receive

Operation	Command
Set the maximum size of SNMP packets that the agent can receive/send	snmp-agent packet max-size byte-count
Restore the default maximum size of SNMP packets	undo snmp-agent packet max-size

Display and Debug SNMP

Perform the following commands in all views.

Table 62 Display and debug SNMP

Operation	Command
Display the statistics of SNMP packets	display snmp-agent statistics
Display the current equipment engine ID	display snmp-agent local-engineid
Display information of system location	display snmp-agent sys-info location
Display system contact information	display snmp-agent sys-info contact
Display information of snmp groups on the router	display snmp-agent group
Display information of all SNMP users in the group user name list	display snmp-agent usm-user
Display the group names that have been configured	display snmp-agent community
Display information of the MIB views that have been configured	display snmp-agent mib-view
Enable SNMP debugging	debugging snmp-agent { headers packets process trap all }

Typical Configuration Examples

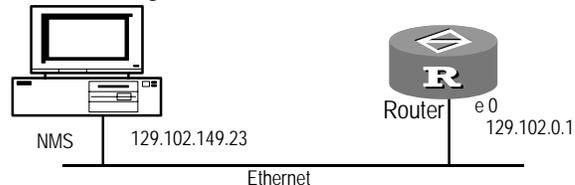
Example 1: Configure Network Management of SNMPv1

I. Networking Requirements

In the following diagram the NMS and a router are connected via the Ethernet. The IP addresses of NMS and the Ethernet interface on the router are respectively 129.102.149.23 and 129.102.0.1.

II. Networking Diagram

Figure 3-3 Configure SNMP



III. Configuration Procedure

- 1 Enable the router to support SNMP and select an SNMP version.

```
[Router] snmp-agent
[Router] snmp-agent sys-info version v1
```

- 2 Set the community name and access authority.

```
[Router] snmp-agent community public read
[Router] snmp-agent community private write
```

- 3 Set the ID of administrator, contact method and physical location of the router.

```
[Router] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Router] snmp-agent sys-info location telephone-closet,3rd-floor
```

- 4 Enable the router to send traps to NMS (129.102.149.23) and use the community name "public", and set the source address in the traps to be the IP address of the interface ethernet 0.

```
[Router] snmp-agent trap enable
[Router] snmp-agent target-host trap address 129.102.149.23
securityname public
[Router] snmp-agent trap source ethernet 0
```

- 5 Configure an IP address for the Ethernet interface ethernet 0.

```
[Router] interface ethernet 0
[Router-Ethernet0] ip address 129.102.0.1 255.255.0.0
```

Example 2: Configure Network Management of SNMPv3

I. Networking Requirements

- According to the networking of Example 1, NMS is connected to the router via the Ethernet, and their IP addresses are respectively 129.102.149.23 and 129.102.0.1.
- SNMPv3 is required. Three SNMP groups will be configured and respectively authorized with read-only, writing, and notifying rights. Three SNMP users belong to the three groups respectively, and three MIB views are used as read, write and notify views respectively.
- Information of the network administrator is required to be configured.

- Required if traps are to be sent — the IP address of the interface ethernet 0 is the source address of the traps, and the address of the NMS is the destination address.

II. Networking Diagram

Refer to the networking diagram of Example 1.

III. Configuration Procedure

- 1 Enable the router to support SNMP and select an SNMP version.

```
[Router] snmp-agent
```

- 2 Set SNMP groups, users and views.

```
[Router] snmp-agent mib-view included read_view subtree 1.3.6.1
[Router] snmp-agent mib-view included write_view subtree 1.3.6.1.5
[Router] snmp-agent mib-view excluded notify_view subtree 1.3.6.2
[Router] snmp-agent group v3 group_read noauthentication read -view
read_view
[Router] snmp-agent group v3 group_write privacy write-view
write_view
[Router] snmp-agent group v3 group_notify authentication read-view
notify_view
[Router] snmp-agent usm-user v3 user_read group_read
[Router] snmp-agent usm-user v3 user_write group_write
authentication md5 123 privacy-mod des56 asdf
[Router] snmp-agent usm-user v3 user_notify group_notify
authentication md5 qwer
```

- 3 Configure information of equipment administrator

```
[Router] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Router] snmp-agent sys-info location telephone-closet,3rd-floor
```

- 4 Configure the router to send Traps to the host whose IP address is 129.102.149.23.

```
[Router] snmp-agent trap enable
[Router] snmp-agent target-host trap address 129.102.149.23
securityname user_notify parameters v3 auth
[Router] snmp-agent trap source ethernet 0
```

- 5 Configure an IP address for the Ethernet interface ethernet 0

```
[Router] interface ethernet 0
[Router-Ethernet0] ip address 129.102.0.1 255.255.0.0
```

RMON Overview

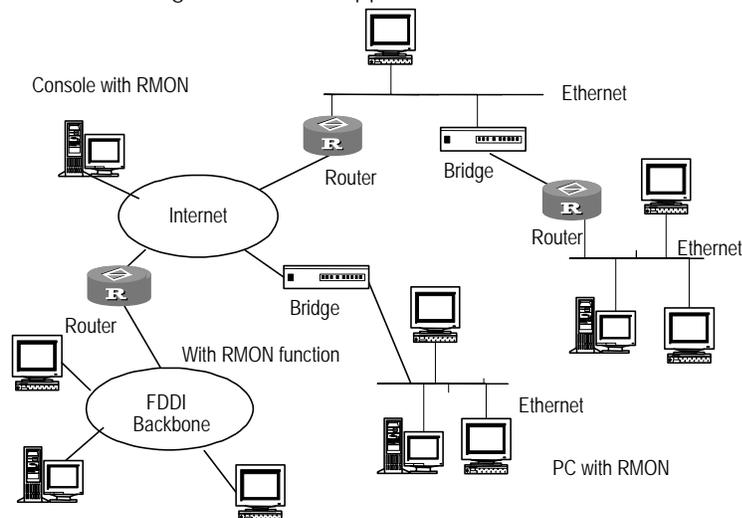
RMON (Remote Monitor) is a MIB defined by IETF and is the most important enhancement for the MIB II standard. It mainly monitors the data flow in a network segment or on the entire network. It is implemented on the basis of the SNMP architecture (one of its strengths), including NMS and Agent running on network equipment.

RMON Agent performs statistics of diversified flow information on the network segments connected to the ports, such as the total messages on a network segment within a certain period or the total of correct messages sent to a host. It enables SNMP to monitor remote network devices more efficiently and more actively and provides an efficient method to monitor sub-network running. This method can help reduce communication flows between the NMS and the Agent,

thus managing large-scale interconnection networks easily and effectively. RMON also allows several monitors and can collect data in two ways: one is to collect with the RMON probe — NMS directly obtains management data from an RMON probe and controls network resources. In this way, all RMON MIB data can be obtained. The other way is by the RMON Agent directly implanted in network equipment (router, switch and HUB) which will become network facilities with RMON probe function. NMS exchanges data information with them and collects network management information through SNMP basic commands. However, limited by equipment resources, not all RMON MIB data can be obtained this way. In most cases, only four groups of information can be collected. Currently, the 3Com Router 1.x implements RMON in the second way.

RMON-MIB is composed of a group of statistics data, analysis data and diagnosis data. Standard MIB not only provides a lot of the original port data of the managed object, but it provides statistics data and calculation results of a network segment. By running SNMP Agent supporting RMON on the network monitor, NMS can obtain the overall flow, error statistics, and performance statistics of the network segment, that connects the interfaces of managed network equipment so as to fulfill network management. An RMON application example is shown below:

Figure 36 Schematic diagram of RMON application



The value includes three managed objects. With enhanced RMON alarm group function, if a sample is found to cross the threshold, which has been configured, RMON Agent will report to NMS so as to avoid a lot of query messages of the NMS.

Configure RMON on the Router

To configure RMON after SNMP, first configure RMON command lines on the 3Com Router series. Then enable RMON statistics before NMS can be used to monitor network traffic and perform network management.

RMON configuration includes:

- Enable RMON statistics of Ethernet interface

1 Enable RMON statistics of Ethernet interface

After enabling RMON statistics of an Ethernet interface, the router will perform the statistics of the packet incoming and outgoing through this interface. After disabling it, the router will not perform the statistics of the packet incoming and outgoing through this interface.

Perform the following task in Ethernet interface view.

Table 63 Enable RMON statistics of an Ethernet interface

Operation	Command
Enable RMON statistics of an Ethernet interface	rmon promiscuous
Disable RMON statistics of an Ethernet interface	undo rmon promiscuous

RMON statistics is disabled by default.

This command cannot be used in Sub-interface view.

RMON Configuration Examples

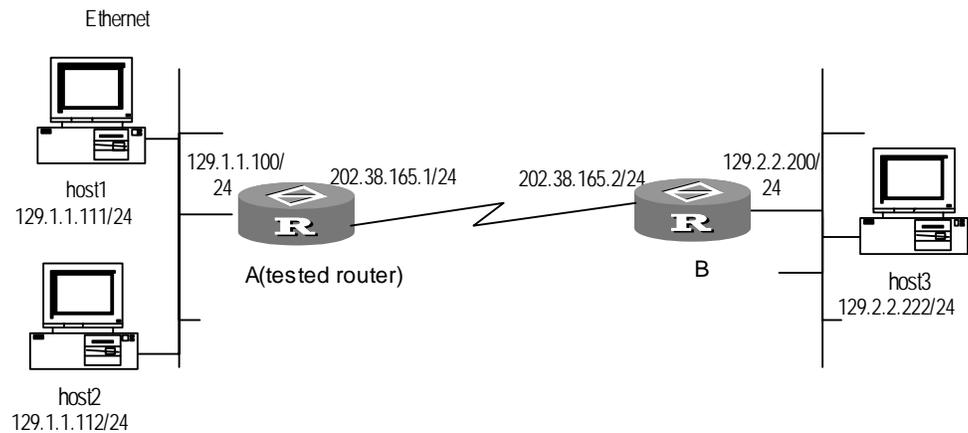
Enable RMON statistics

I. Networking Requirement

To ensure that the router can detect the packet whose destination is another router from the Ethernet interface, the interface should be added in the DLSw bridge set. Otherwise, the router only performs statistics for frames with this router as the destination.

II. Networking Diagram:

Figure 37 Enable RMON statistics



III. Configuration Procedure

Configure the 3Com Router

- 1 Configure address and route of host1, host2, host3, routerA and routerB. Make sure they can ping through each other. Specific operation is omitted here.

- 2 Add Ethernet interface Ethernet 0 to DLSw bridge set.

```
[RouterA] interface ethernet 0
[RouterA-Ethernet0] bridge-set 1
```

- 3 Enable RMON statistics of Ethernet 0

```
[RouterA] interface ethernet 0  
[RouterA-Ethernet0] rmon promiscuous
```

6

DISPLAY AND DEBUGGING TOOLS

This chapter includes information on the following topics:

- Display Command Set
- Debugging Command Set
- Test Tool of Network Connection
- Log Function

Display Command Set

With **display** commands, the system status and system information can be viewed. **display** commands can be divided as follows according to the functionality:

- The command to display system configuration information
- The command to display system running status
- The command to display system statistic information

The following commands can be used to display related information of the whole system in all views. Please see related chapters in this manual for specific **display** commands.

Table 64 Commands to display information of the whole system

Operation	Command
Display current terminal user.	display client
Display the system clock	display clock
Display the current memory type	display configfile
Display states of various debugging switches	display debugging
Display the history record of input command	display history-command
Display the router name	display sysname
Display current configuration information of the system	display current-configuration
Display initial configuration information of the system stored in router Flash	display saved-configuration
Display primary system configuration information	display tech-support [page]
Display registered terminal user	display user
Display version information of system	display version

Debugging Command Set

The command line interface of the 3Com Router 1.x provides abundant **debugging** commands, almost corresponding to all the protocols supported by the router, helping the user to diagnose and eliminate network faults.

Two switches control the output of the debugging information:

- Debugging switch, which controls whether to test a certain function/module/protocol.
- Syslog output direction switch, which controls outputting the debugging information to the control console, Telnet terminal or internal buffer or log host.

The following is part of the common **debugging** commands. For more specific **debugging** commands related to various protocols, please see related chapters in this manual and the *3Com Router Command Reference Guide*.

The 3Com Router provides a shortcut *Ctrl+D* to close the huge amount of debugging information output by the terminal, which functions the same as the command **undo debugging all**.

Examples are omitted here. Please see relevant chapters in the *3Com Router Command Reference Guide*.

In addition, when any terminal user enables or disables the debugging, the debugging information output on other user terminals will be affected.

As for all link layer protocols, the debugging can be controlled according to interfaces, so that the interference of a huge amount of redundant information can be avoided effectively and it makes troubleshooting more convenient.

On the 3Com Router, Syslog (log system) manages the output of debugging information and other prompt information. Before obtaining the debugging information, you need to open the related Syslog switch. Firstly, you must use the **info-center enable** command to enable Syslog function, then you can use the **info-center console** or **info-center monitor** command to enable debugging according to the different type of terminal, or use the **info-center console debugging** command on the Console terminal, or use **info-center monitor debugging** on the telnet terminal or dumb terminal. Refer to subsequent sections for introduction and detailed descriptions and commands of Syslog.



*Since the output of the debugging information will affect the running efficiency of the router, please do not turn on any debugging switches unless necessary, especially the **debugging all** command. After completing debugging, please turn off all debugging switches.*

Test Tool of Network Connection

Ping Command

The **ping** command is mainly used to check the connection of the network, i.e. whether the host is accessible. Ping sends Internet Control Message Packets (ICMP) echo packets to another computer connected on the network to see whether it echoes back. Ping is a useful command to test the connectivity of the network and details about the journey.

Table 65 ping command

Operation	Command
-----------	---------

ping supporting IP protocol	ping [ip] [-Rdnqrv] [-c count] [-p pattern] [-s packetsize] [-t timeout] { host ip-address }
ping supporting IPX protocol	ping [ipx] [-n] [-v] N.H.H.H [count [,timeout [,packetsize]]]

Please see relevant chapters in the *3Com Router Command Reference Guide* for detailed meanings of various options and parameters.

Ping supporting IP protocol

- For each ping message sent, if the response message has not been received when the waiting time crosses the threshold, then Request time out is output.
- Otherwise, the data byte number, message sequence number, TTL, and response time in the response message will be displayed.
- Finally, the statistic information will be output, including the sent message number, received response message number, percentage of messages unresponded, and the minimum, maximum, and average values of the response time.

Examples:

```
[Router]ping 202.38.160.244
```

The system displays:

```
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
```

Ping supporting IPX protocol

- For each Ping message sent, the response information is output. "!" indicates the response message is received, while "." indicates not received.
- Finally, the statistic information is output, including sent message number, received response message number, percentage of messages unresponded, and the minimum, maximum, and average values of the response time.

Examples:

```
[Router]ping ipx 2.0.0c91.f61f
```

The system displays:

```
Press CTRL_C to break
Sending 5, 100-byte IPX Echoes to 2.0.0c91.f61f, timeout is 2
seconds
```

```

!!!!
--2.0.0c91.f61f IPX ping statistics--
 5 packets transmitted
 5 packets received
 0% packet loss
 round-trip min/avg/max = 1/2/3 ms
    
```

tracert command (Trace Route Command)

The trace route command helps to trace the current network path to a destination. With **tracert** command, all gateways by which the test packet passes from the source address to the destination address can be displayed. It can be used to check network connection and locate fault.

The **tracert** command is executed as follows: first, send a packet with TTL 1, and the first hop returns an ICMP error message, indicating that this packet cannot be sent (for TTL timeout). Then, this packet is re-sent with TTL added by 1 (namely 2). Similarly, the next hop returns TTL timeout. In this way, the procedure continues till the destination is reached. The purpose of these procedures is to record the source address of each ICMP TTL timeout message, so as to provide the path by which an IP packet has to pass to reach the destination address.

The following command can be executed in any command modes:

Table 66 tracert command

Operation	Command
Display the path from the source address to the destination address	tracert [-a ip-address] [-f first_TTL] [-m max_TTL] [-p port] [-q nqueries] [-w timeout] host

Please see relevant chapters in the *3Com Router Command Reference Guide* for detailed meanings of various options and parameters.

Described below are two examples to analyze the network connection with **tracert** command. In the former example, network connection is correct, while in the latter, network connection is faulty.

```

[Router] tracert 35.1.1.48
Trace route 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 above results indicate which gateways (1~9) are passed from the source address to the destination address. That is very useful to network analysis.

```

[Router] 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 above results indicate which gateways (1~17) are passed from the source host to the destination host, and which gateways are faulty (12, 14, 15, 16 and 17).

Log Function

This section describes the various attributes that form the log function and how to configure on the router.

Syslog Overview

The 3Com Router 1.x is configured with Syslog (log system). As an indispensable part of the 3Com Router 1.x, Syslog serves as the information junction of the 3Com Router 1.x system software module. The log system is responsible for most of the information output and can perform detailed classification so as to filter information effectively. In combination with the **debugging** command, the system provides powerful support for the network administrator and development staff to monitor the network running state and diagnose the network faults.

The Syslog of the 3Com Router 1.x features the following:

- Support log output in four directions, i.e. to the control console (Console), to the telnet terminal and the dumb terminal (Monitor), to the internal buffer (Buffer), and to the log host (Loghost).
- Log information is divided into eight levels according to the importance and filter based on the levels.
- Information is classified according to the source modules and filter based on the modules.
- Information can be output in Chinese or English.

Configure Syslog

The configuration tasks of Syslog include:

- Set the direction of Syslog outputting log information
- Set the Severity of log information
- Set the Filter of log information
- Turn on/off Syslog

Set the direction of syslog outputting log information

As described before, Syslog of the 3Com Router 1.x can output various log information in four directions:

- Output log information to local control console via Console port
- Output log information to remote Telnet terminal or dumb terminal. This function is helpful to remote maintenance.
- Allocate proper router buffer to record log information.
- By configuring the log host, log information is directly sent by Syslog to the log host and then saved as file for later view.

Please enter the following commands in system view.

Figure 38 Set the direction of syslog output log information

Operation	Command
Enable to output log information to local control console	<code>info-center console</code>
Disable to output log information to local control console	<code>undo info-center console</code>
Enable to output log information to the terminal	<code>info-center monitor</code>
Disable to output log information to the terminal	<code>undo info-center monitor</code>
Enable to output log information to internal buffer	<code>info-center logbuffer</code>
Disable to output log information to internal buffer	<code>undo info-center logbuffer</code>
Define the size of internal buffer of output log information	<code>info-center logbuffer size</code>
Enable to output log information to the log host	<code>info-center loghost</code>
Disable to output log information to the log host	<code>undo info-center loghost</code>
Change the language mode (Chinese English) of output log information	<code>info-center { console monitor logbuffer loghost } { chinese english }</code>

Here, Console and Monitor stand for default output directions.



The setting of output direction of the log information will be effective only if Syslog is turned on.



The settings of the output log information in four directions are independent. The shutdown of an output in any direction will not affect the output in other directions.



When there are multiple telnet users or dumb terminal users simultaneously, various users share the same configuration parameters, which include the filtering setting based on the module, Chinese/English selection and severity threshold. When a user changes the values of these parameters, other user terminals will also be affected. At this time, the `undo info-center monitor` command can only turn off the log information output on the respective terminal. Therefore, to turn off the log information outputs of all telnet terminals and dumb terminals, please use the `undo info-center monitor all` command.

Set Severity of Log Information

Syslog is divided into 8 levels according to the Severity (or priority) of the information. The rule to filter the log information according to the level is: the more urgent the log information is, the less severe it will be. The log information with severity higher than the set threshold is forbidden to be output. Only the log information with severity no higher than this threshold can be output.

Perform the following task in system view.

Table 67 Enable to output log information with priority

Operation	Command
Enable to output log information with priority to local control console	<code>info-center console {emergencies alerts critical errors warnings notifications informational debugging}</code>
Enable to output log information with priority to the terminal	<code>info-center monitor {emergencies alerts critical errors warnings notifications informational debugging}</code>
Enable to output log information with priority to internal buffer	<code>info-center logbuffer {emergencies alerts critical errors warnings notifications informational debugging}</code>
Enable to output log information with priority to the log host	<code>info-center loghost <0-9> {local<0-7>/ip-address} {emergencies alerts critical errors warnings notifications informational debugging}</code>
Disable to output log information with priority to the log host.	<code>undo info-center { console monitor logbuffer loghost}</code>

Syslog-defined severity is as follows:

Table 68 Syslog-defined severity

Severity	Descriptions
Emergencies (0)	Most severe/emergent fault
Alerts (1)	Fault needs to be corrected immediately
Critical (2)	Major fault
Errors (3)	Noticeable but not major fault
Warnings (4)	Cautions, it is possible there may be a fault
Notifications (5)	Information needs to pay attention to
Informational (6)	Ordinary prompt information:
Debugging (7)	Debugging information

Set Filter of Log Information

In different output modes, the Filter can be set according to the source of log information. Only the log information complying with the Filter definition can be output.

Please enter the following commands in system view.

Table 69 Set filter of the log information

Operation	Command
Set Filter of the control console	<code>info-center console filter module</code>
Delete Filter of the control console	<code>undo info-center console filter</code>

Set terminal Filter	<code>info-center monitor filter module</code>
Delete terminal Filter	<code>undo info-center monitor filter</code>
Set Filter of internal buffer	<code>info-center logbuffer filter module</code>
Delete Filter of terminal buffer	<code>undo info-center logbuffer filter</code>
Set Filter of log host	<code>info-center loghost <0-9> { local<0-7> ip-address } filter module</code>
Delete Filter of log host	<code>undo info-center loghost <0-9> { local<0-7> ip-address } filter</code>

Here, module stands for the module name. Only the log information related to a specified module can be filtered and output.

Turn on/turn off syslog

Please enter the following commands in system view.

Table 70 Turn on/turn off syslog

Operation	Command
Turn on Syslog	<code>info-center enable</code>
Turn off Syslog	<code>undo info-center enable</code>



When Syslog is turned on, the performance of the system will be affected due to the information classification and output - especially when processing a large amount of information.

Display and Debug Syslog

Perform the following configuration in all views.

Table 71 Display and debug syslog

Operation	Command
Display basic configuration information of Syslog	<code>display info-center</code>
Display internal buffer information of Syslog	<code>display info-center logbuffer</code>

Typical Syslog Configuration Example

Configuration of Log Host

The configuration, implemented on SunOS 4.0, is almost the same as that performed on the Unix operating system of other manufacturers.

- 1 Execute following commands as root (supervisor)

```
#mkdir          /var/log/Router
#touch          /var/log/Router/config
#touch          /var/log/Router/security
```

- 2 Edit the file `/etc/syslog.conf` as the root and add the following selector/action pairs.

```
#Router configuration messages
Local4.crit    /var/log/Router/config
```



When editing `/etc/syslog.conf`, note the following:

- *The comments can only be in separate lines, beginning with character #.*
- *The selector/action pairs must be separated with one Tab instead of a space.*
- *There must not be redundant spaces behind the file name.*

- 3 When log files like config and security are created and /etc/syslog.conf file is modified, an HUP will be sent to the system daemon, Syslogd, by executing the following commands to make Syslogd re-read its configuration file

```
/etc/syslog.conf.
```

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

After the above operations, the router can record information in relevant log files.



Configure Facility (facility name), Severity (severity threshold), Filter, and syslog.conf file to make a detailed classification of information, so as to filter the information.

Syslog Configuration Example

- Configure log information output of the control console.

- 1 Turn on the log system

```
[Router] info-center enable
```

- 2 Configure the log information output of the control console, severity ranging between emergencies ~ debugging, and do not filter the log information output of PPP module.

```
[Router] info-center console
[Router] info-center console debugging
```

- 3 Turn on debugging switch of PPP module.

```
[Router] debug ppp all
```

- Configure the log host

The router-side configuration is as follows:

- 1 Turn on the log system

```
[Router] info-center enable
```

- 2 Use the host with IP address of 10.110.12.119 as the log host, set the severity threshold to informational, and choose English as the output language.

```
[Router] info-center loghost 10.110.12.119 language english
```

Please see "Configuration of log host" for the host-side configuration.

7

POS TERMINAL ACCESS SERVICE

This chapter contains information on the following topics:

- POS Access Service Overview
- POS Access Service Configuration
- Display and Debug POS Access
- Typical Configuration Example of POS Access Service

POS Access Service Overview

Point of Sale (POS) service is a type of smart card service widely used in shopping malls, gas stations, and so on. It links the POS terminal device at the commercial client (located in shopping mall or gas station) to the bank card accounting system to provide service.

The POS terminal device is widely used in the fields of commerce, finance, taxation, and so on. The earlier POS terminal devices worked independently in different banks, and they could not communicate with each other. The technology based on a shared POS access service has solved this problem and makes it possible to use different bank cards on the same POS.

The POS terminal is connected to the transaction center in two ways, namely, through dial-up POS access and POS network access.

Dial-up POS Access

In the dial-up POS access mode, after responding to the smart card, the POS terminal device will synchronously or asynchronously dial up with the built-in modem. Thus the POS terminal device at the commercial client accesses the bank card accounting system. In this case, the 3Com Router series providing POS access service can be placed at the commercial client side. The routers can be connected to the front end processor via the WAN. They can also be connected to the front end processor of the bank via the asynchronous interface or Ethernet port.

The following figure shows the networking diagram of the typical dial-up POS access.

Figure 39 Dial-up access when the POS access router is located at the FEP side

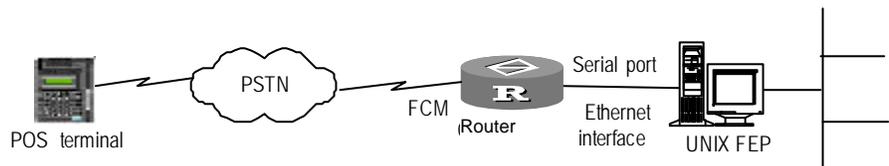
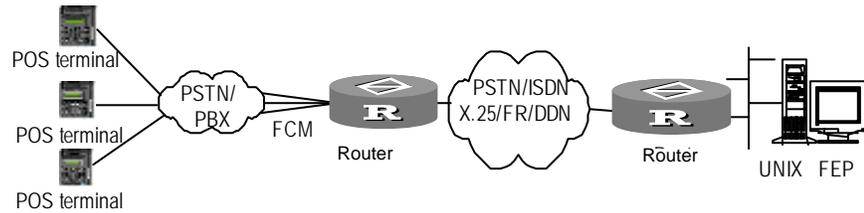


Figure 40 Dial-up access when the POS access router is located at the commercial client side



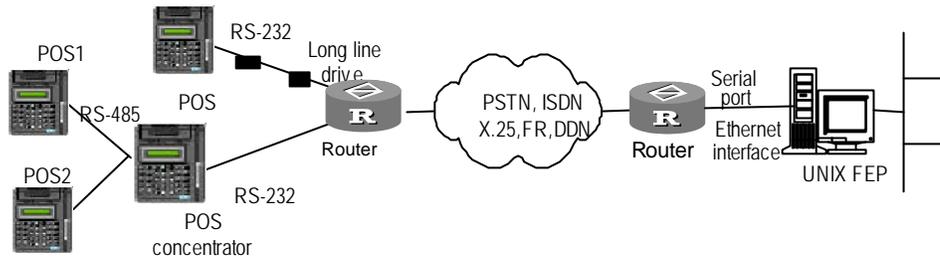
Due to the way POS access service usually operates, that is, low speed, high frequency and small traffic, it is rather sensitive to the dial-up connection time and requires the interface board for fast dial-up function. However, the present common PC modem cannot meet the response time requirements of 10 to 20 seconds. At present, most POS equipment manufacturers use the special modem chip that supports fast connection to implement the function. The FCM card of the 3Com Router series is a fast handshaking modem specially designed for POS dial-up access service.

POS Network Access

In the POS network access mode, the router providing POS access service is located at the commercial client end and helps all the POS terminals access the 3Com Router series. The router located at the FEP side can be any router and communicates with the 3Com Router series through X.25, FR, DDN, ISDN or modem.

The following figure shows the networking of typical POS network access.

Figure 41 Access mode when the POS access router located at the commercial client end



In the POS network access mode, 3Com Router series can be connected to the POS terminal in the following two ways:

- Directly connect the POS RS-232 connector with the asynchronous interface (including the asynchronous mode of the synchronous/asynchronous interface) of the 3Com Router series. If the distance between them exceeds 15 meters, it will be necessary to install a long-line-driver at each end of the connection line. The valid connection distance of a pair of passive long-line-drivers is about 1200 meters.
- Set up an RS-485 network with the POS terminal device and POS concentrator, then connect the RS-232 connector of the POS concentrator with the asynchronous interface of the 3Com Router series. The 3Com Router series communicate on the egress port in the same way as the first connection method. Access in this way can save the router interface source greatly.

The advantages of POS network access are as follows:

- Avoiding the dial-up time problem and fast connecting to the transaction processing center.
- Reducing the number of occupied communication links, hence saving the communications cost greatly.
- Avoiding the problem of service queuing as it is as though each POS terminal device enjoys a dedicated line (except the networking is comprised of the POS terminal and the POS concentrator).
- The POS access feature can be combined with other services of the router, i.e., dumb terminal, SNA, and VoIP, which brings a wide market and provides users with integrated solutions.

POS Access Service Configuration

POS access service configuration includes:

- Enable POS access server
- Configure POS access port
- Configure POS application interface
- Configure POS application
- Configure POS multi-application map
- Bind the source address of TCP connection

1 Enable POS Access Server

To implement the POS access service, the POS access server must first be started. Please perform the following configuration in system view.

Table 72 Start POS server

Operation	Command
Enable POS access server	<code>pos-server enable</code>
Disable POS access server	<code>undo pos-server enable</code>

By default, the system disables the POS access server.

2 Configure POS Access Port

Only configured as a POS access port can the interface provide POS access service.

At present, the interfaces of the 3Com Router series, which can be used for POS access service, include the asynchronous interface, AUX port, the synchronous/asynchronous interface, and the FCM interface.

Please perform the following configuration in asynchronous interface view or FCM interface view.

Table 73 Configure POS access port

Operation	Command
Configure the POS access interface	<code>async mode pos pos-id</code>

By default, the asynchronous interface and FCM interface operate in protocol mode, that is, no POS access port is configured.



Only when the active interface operates in protocol mode can the command be configured.



If the FCM interface is used as POS access interface `undo modem` cannot be configured. If another interface is used as the POS access interface `undo modem` must be configured.



Since POS access does not support flow control, the interface should be configured with the `flow-control none` command.



If the POS access port is connected to the POS terminal in asynchronous mode, and the POS asynchronous port does not send a DSR-DTR signal, it is necessary to configure the command `undo detect dsr-dtr` on the interface. If the POS access port is connected to the FCM interface via dial-up, it is unnecessary to configure the `undo detect dsr-dtr` command.

3 Configure POS Application

The POS access router connects to the UNIX FEP in the following two ways: asynchronous connection and TCP/IP connection. The commands used for configuring the POS application are different in the two modes. Connecting to the UNIX FEP through the Ethernet is called a TCP/IP connection, while connecting through the asynchronous serial port is called asynchronous connection. No matter how the connected is made, it is necessary to configure the POS application to UNIX FEP for the terminal.

Please perform the following configuration in system view.

Table 74 Configure a POS application

Operation	Command
Configure a POS application in asynchronous connection	<code>pos-server app flow app-number interface-type interface-number</code>
Delete a POS application in asynchronous connection	<code>undo pos-server app flow app-number</code>
Configure a POS application in TCP/IP connection	<code>pos-server app tcp app-number ip-address port-number</code>
Delete a POS application in TCP/IP connection	<code>undo pos-server app tcp app-number</code>

By default, no POS application is configured by the system.

4 Configure POS Application Interface

POS application interface should operate in `posapp` mode.

Please perform the following configuration in asynchronous interface view.

Table 75 Configure the asynchronous connection interface to operate in POS application mode

Operation	Command
Configure the operation mode of POS application interface	<code>async mode posapp</code>



When the POS access router is connected to the UNIX FEP in asynchronous mode, the interface should operate in `posapp` mode.



This command can be configured only when the active interface is configured with the command `async mode protocol`



Only after the command `undo modem` is configured, can data be transceived normally.



POS access does not support flow control, therefore, the interface should be configured with the **flow-control none** command.

5 Configure POS Multi-Application Map

POS multi-application is a kind of POS access function, which sends the packets from a POS terminal device to different POS applications according to the packet destination addresses. For TCP/IP connection, an application is marked by two parts, IP address and port number, that is, the different applications may have different IP addresses or share the same IP address but have different port numbers. The packets can be sent to different applications according to the destination address number. When the destination address number has a corresponding entry in the mapping table, the packet will be sent to the application corresponding to the entry. If there is no entry matching the destination address, the packet will be sent to the default application.

Please perform the following configuration in system view.

Table 76 Configure POS multi-application mapping table

Operation	Command
Configure the POS multi-application mapping table	pos-server map { des-code default } app-number
Delete the POS multi-application mapping table	undo pos-server map { des-code default }

By default, no POS multi-application mapping table is configured.

At present, the 3Com Router series support up to 32 applications.

6 Bind the Source Address of TCP Connection

When several POS terminal devices multiplex one TCP connection to set up relations with the application of the host, for the sake of security, it is necessary to hide the true IP address of the up TCP connection in the access service, and set another IP address for the source address instead. At the same time, to perform the backup of the link, the terminal access server provides the function of binding the source address of the TCP connection.

The principle of binding the source address of the TCP connection is to configure an IP address on the other interface that is not used on the router (Dial-up interface is recommended), the unnumbered IP address is the address of the up TCP connection on the terminal access server. Using the **undo pos-server source-ip** command, you can remove the binding of TCP source address and the IP address of the TCP connection will be restored to the real IP address of the original physical interface.

Please perform the following configurations in system view.

Table 77 Bind the source address of TCP connection

Operation	Command
Bind the source address of TCP connection	pos-server source-ip app-number ip-address
Remove the binding of the source address of the TCP connection	undo pos-server source-ip app-number

By default, the source address of the TCP connection is not bound.



Please note that this command can be applied only in the application in the TCP connection, and the application state is that the TCP connection has not been

implemented otherwise, the system will prompt as follows to indicate that the configuration has failed: App-state is wrong.

7 Set the parameters of FCM used during Modem negotiation

In the POS access application, the Modem on the FCM card usually acts as the called party, and the Modem embedded in the POS terminal acts as the calling party. In the Modem communication, the POS terminal originates a call after the called party detects the calling signal, it will answer and send an answer tone to the POS terminal. After the POS terminal receives answer tone, both sides begin the Modem negotiation (V.22). For a system with poor network quality, the short answer tone may cause Modem negotiation failure. On the router, in the case that you can see a constant UP and DOWN on the Modem port, without data being transmitted or received, just enlarge the value of ANSWERTIME.

After the negotiation reached, communication begins. The POS terminal adopts SDLC protocol, and the retransmission mechanism is used between the monitoring frame and the data frame to deal with abnormal occasions. The parameter PACKET INTERVAL is used to set the timeout value. For big packets (greater than 512 bytes), the system should enlarge the timeout value.

To improve the utilization of the POS access port, and to avoid a POS terminal being occupied for a long time, it is necessary to manage individual transaction times through configuring the parameter TRADETIME. If the maximum transaction time is exceeded after the POS terminal is dialed, the router will disconnect to unblock the resource.

In general, the default values of the parameters can satisfy the demands of application, but in abnormal occasions you need to modify some parameters.

Please perform the following configurations in system view.

Table 78 Set the parameters of FCM used during Modem negotiation

Operation	Command
Set the parameters of FCM used during Modem negotiation	<code>pos-server fcm [answertime time] [tradetime time] [packetinterval time]</code>
Restore the parameters of FCM used during Modem negotiation	<code>nundo pos-server fcm [answertime time] [tradetime time] [packetinterval time]</code>

Display and Debug POS Access

Perform the following configuration in all views.

Table 79 Display and debug POS access

Operation	Command
Clear the counter of the displayed information.	<code>reset pos</code>
Clear the number of times that negotiation fails or the number of times of disconnection due to transaction timeout to zero	<code>reset fcm</code>
Display the brief information of POS application.	<code>display pos-app</code>
Display the brief information of POS interface	<code>display pos-interface</code>
Display the number of times that negotiation fails or the number of times of disconnection due to transaction times out	<code>display fcm</code>
Enable the debugging of POS application	<code>debugging pos-app [app-number]</code>

Enable the debugging of POS access interface	<code>debugging pos-interface [pos-id]</code>
--	---

Typical Configuration Example of POS Access Service

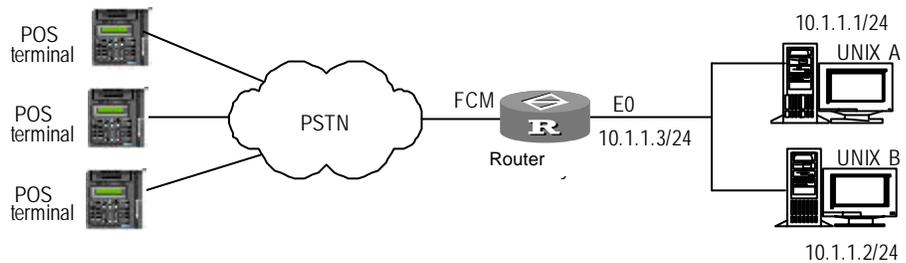
Configuration Example when the Router is Located at the FEP Side in TCP/IP Mode

I. Networking Requirements

Three POS terminals access the Router A located at the FEP side through the FCM card and connect to UNIX A (10.1.1.1) and UNIX B (10.1.1.2) in TCP/IP mode.

II. Networking Diagram

Figure 42 Networking diagram when the router is located at the FEP side in TCP/IP mode



III. Configuration Procedures

- 1 Enable POS access server

```
[Router] pos-server enable
```

- 2 Configure the POS application to UNIX A in TCP/IP connection mode, the application is 0.

```
[Router] pos-server app tcp 0 10.1.1.1 9010
```

- 3 Configure the POS application to UNIX B in TCP/IP connection mode, the application is 1.

```
[Router] pos-server app tcp 1 10.1.1.2 9020
```

- 4 Configure the POS multi-application mapping table (to map the packet whose destination address is 01f1 to application 0).

```
[Router] pos-server map 01f1 0
```

- 5 Configure the POS multi-application mapping table (to map the packet whose destination address is 01f2 to application 1).

```
[Router] pos-server map 01f2 1
```

- 6 Configure the Ethernet interface Ethernet 0.

```
[Router] interface ethernet 0
[Router-Ethernet0] ip address 10.1.1.3 255.255.255.0
```

- 7 Configure the POS access interface FCM0

```
[Router] interface fcm0
[Router-FCM0] async mode pos 1
```

- 8 Configure POS access interface FCM1

```
[Router] interface fcm1
[Router-FCM1] async mode pos 2
```

9 Configure POS access interface FCM2

```
[Router] interface fcm2
[Router-FCM2] async mode pos 3
```

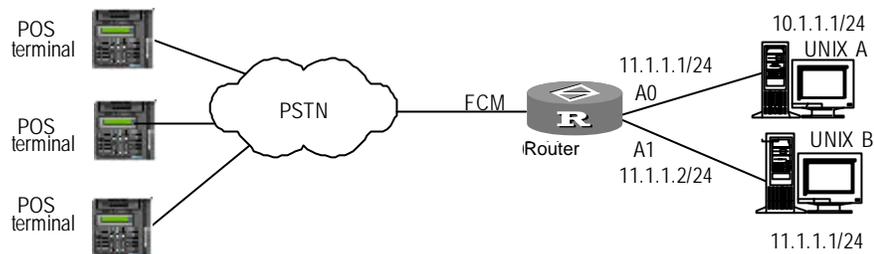
Configuration Example when the Router is Located at the FEP Side in Asynchronous Connection Mode

I. Networking Requirements

Three POS terminals access the Router A located at the FEP side through the FCM and connect to UNIX A (10.1.1.1) and UNIX B (11.1.1.1) in asynchronous connection mode.

II. Networking Diagram

Figure 43 Networking diagram when the router is located at the FEP side in asynchronous connection mode



III. Configuration Procedure

1 Start the POS access server.

```
[Router] pos-server enable
```

2 Configure the POS application to UNIX A in asynchronous connection mode, the connected interface is async 0, the application sequence number is 0.

```
[Router] pos-server app flow 0 async 0
```

3 Configure the POS application to UNIX B in asynchronous connection mode, the connected interface is async 1, the application sequence number is 1.

```
[Router] pos-server app flow 1 async 1
```

4 Configure the POS multi-application mapping table (to map the packet whose destination address is 01f1 to application 0).

```
[Router] pos-server map 01f1 0
```

5 Configure the POS multi-application mapping table (to map the packet whose destination address is 01f2 to application 1).

```
[Router] pos-server map 01f2 1
```

6 Configure POS access interface FCM0.

```
[Router] interface fcm0
[Router-FCM0] async mode pos 1
```

7 Configure POS access interface FCM1.

```
[Router] interface fcm1
[Router-FCM1] async mode pos 2
```

8 Configure POS access interface FCM2.

```
[Router] interface fcm2
```

```
[Router-FCM2] async mode pos 3
```

- 9 Configure Async 0 to operate in POS application mode.

```
[Router] interface async 0
[Router-Async0] undo modem
[Router-Async0] flow-control none
[Router-Async0] async mode posapp
```

- 10 Configure Async 1 to operate in POS application mode.

```
[Router] interface async 1
[Router-Async1] undo modem
[Router-Async1] flow-control none
[Router-Async1] async mode posapp
```

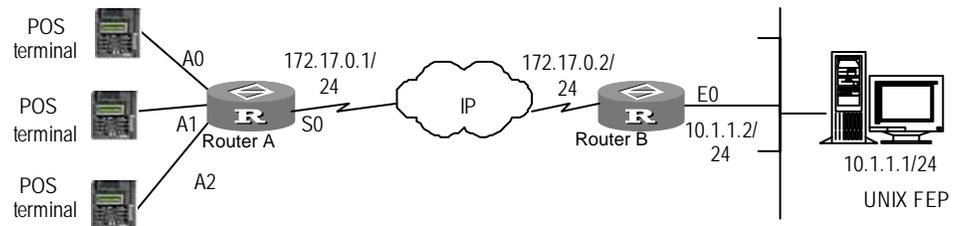
Configuration Example when the Router is Located at the Commercial Client Side in TCP/IP Connection Mode

I. Networking Requirements

Three POS terminals access the 3Com Router series located at the commercial client through the asynchronous serial port and connect to UNIX host (10.1.1.1) in TCP/IP connection mode.

II. Networking Diagram

Figure 44 Networking diagram when the router is located at commercial client in TCP/IP connection mode.



III. Configuration Procedures

- 1 Configure Router A

- a Start the POS access server.

```
[RouterA] pos-server enable
```

- b Configure the POS application to destination UNIX host in TCP/IP connection mode.

```
[RouterA] pos-server app tcp 0 10.1.1.1 9010
```

- c Configure POS default multi-application mapping table (to map the packet which cannot be matched with any application to the application).

```
[RouterA] pos-server map default 0
```

- d Configure POS access interface 0.

```
[RouterA] interface async 0
[RouterA-Async0] undo modem
[RouterA-Async0] flow-control none
[RouterA-Async0] undo detect dsr-dtr
[RouterA-Async0] async mode pos 1
```

- e Configure POS access interface 1.

```
[RouterA] interface async 1
[RouterA-Async1] undo modem
[RouterA-Async0] flow-control none
[RouterA-Async0] undo detect dsr-dtr
[RouterA-Async1] async mode pos 2
```

f Configure POS access interface 2.

```
[RouterA] interface async 2
[RouterA-Async2] undo modem
[RouterA-Async0] flow-control none
[RouterA-Async0] undo detect dsr-dtr
[RouterA-Async2] async mode pos 3
```

g Configure the route to Router B (take the static route as example).

```
[RouterA-Async2] quit
[RouterA] ip route-static 10.1.1.2 255.255.255.0 serial 0
```

2 Configure Router B

a Configure the Ethernet interface Ethernet 0.

```
[RouterB] interface ethernet 0
[RouterB-Ethernet0] ip address 10.1.1.2 255.255.255.0
```



INTERFACE

- Chapter 8 Interface Configuration Overview
- Chapter 9 Configuring LAN Interface
- Chapter 10 Configuring WAN Interface
- Chapter 11 Configuring Logical Interface

8

INTERFACE CONFIGURATION OVERVIEW

This chapter contains information on the following topics:

- Interface Configuration Overview
- Configure Interface
- Display and Debug Interface

Interface Configuration Overview

The router interface refers to the part through which the router exchanges data and interacts with other devices in the network. It functions to implement data exchange between the router and other network devices.

The 3Com Router supports physical interface and logical interface on the router.

Physical interface is an interface physically exists and can be supported by corresponding devices, such as the Ethernet interface and synchronous/asynchronous serial interface. There are two types of physical interfaces. One is the LAN interface, which mainly refers to the Ethernet interface through which the router can exchange data with the network devices in LAN. Second one is the WAN interface which includes interfaces like the synchronous/asynchronous serial interface, asynchronous serial interface, AUX interface, CE1/PRI, ISDN BRI interface. Through the WAN interface, the router can exchange data with the network devices in the external network.

Logical interface is an interface that does not physically exist and needs to be established through configuration, which can also exchange the data. Logical interface includes the Dialer interface, sub-interface, standby center logic channel and virtual-template.

Configure Interface

Interface View To facilitate configuration and maintenance of the interface, the interface view has to be set in the 3Com Router software. Interface commands will be effective only when used in the view of relevant interfaces.

Enter the Interface View

With **interface** command in all views, you can enter the specified view of the interface.

Table 80 Enter view of specified interface

Operation	Command
Enter view of specified interface	interface type number



In the 3Com Router, the command to enter E1/T1 interface view is `controller { e1 | t1 }`, which is different from the command of other interfaces.

Exit the Interface View.

In the interface view, input `quit` to return to the system view.

Set Interface Description

The 3Com Router has a configuration item of interface description for router's physical interface. Interface description is mainly used to help identifying the usage of interface. Please use this command in interface view.

Table 81 Set interface description

Operation	Command
Set interface description	<code>description</code> <code>interface-description</code>
Recover default interface description.	<code>undo description</code>

Set Time Interval for Flow Control Statistics

The 3Com Router system counts interface flow at every time interval and calculates the unit flow as the reference for standby center. Other flow control methods (including the `dialer threshold` command) need this parameter.

Perform the following configuration in system view.

Table 82 Set time interval for flow control statistics

Operation	Command
Set interval time for flow control on the interface	<code>flow-interval minutes</code>

The parameter *minutes* is 5 minutes by default.

Interface Configuration Method

Before configuring an interface, it is necessary to have a clear idea about the networking requirement and network diagram. The following operations must be implemented at least for the interface configuration.

- If the interface is a physical interface, be clear about the connection state, working mode of the physical interface to be selected and related working parameters.
- If the interface is a WAN interface, assign the encapsulated link layer protocol and working parameters that should be abided by for the opposite port connected with this interface.
- Configure network protocol (such as IP) address of this interface.
- Configure the static route that can reach the destination network via this interface, or configure working parameters of the dynamic route protocol on this interface.
- If the interface supports dial-up, please configure working parameters and management to Modem.
- If the interface acts as the main interface or standby interface at the standby center application, please configure related working parameters of the standby center.

- If a firewall is to be established on this interface, please configure parameters about related message filtering or address conversion.

There are lots of parameters to be configured in the interface view. So, this part will mainly introduce configurations of some parameters specific to the physical interface, and briefly introduce the logical interface definition. Configurations about the link layer protocol, network layer protocol, parameter and some special functions (such as dial, standby center, and firewall) will be introduced specifically in other parts of this manual and no further details are provided here.

Display and Debug Interface

Please use the following commands in all views.

Table 83 Display and debug interface

Operation	Command
Display current running state and statistic information of the interface (in all views)	display interfaces [type number] display interfaces brief
Clear interface statistic information (in system view)	reset counters interface [type number]
Shut down interface (in interface view)	shutdown
Restart interface (in interface view)	undo shutdown

When the physical or protocol state of the interface changes, the system will automatically output related prompt information of the interface (e.g., Serial0) as shown in following table.

Table 84 Interface state information

Interface state information	Meaning
% Interface Serial0 is down	The interface is shut down by the user.
% Interface Serial0 is reset	The interface is restarted by the user.
%01:10:34: Interface Serial0 changed state to DOWN	The physical state of the interface is changed to DOWN
%01:11:03: Interface Serial0 changed state to UP	The physical state of the interface is changed to UP
%01:12:02: Line protocol ip on interface Serial0, changed state to DOWN	The protocol state of the interface is changed to DOWN
%01:11:34: Line protocol ip on interface Serial0, changed state to UP	The protocol state of the interface is changed to UP



*If a physical interface on the router is idle and not connected with cable, use the **shutdown** command to disable the interface in case that the interface goes abnormal due to some interference.*

9

CONFIGURING LAN INTERFACE

This chapter contains information on the following topics:

- Ethernet Interface Overview
- Configure Ethernet Interface
- Display and Debug Ethernet Interface
- Typical Ethernet Interface Configuration Example
- Troubleshooting

Ethernet Interface Overview

Ethernet interface of the 3Com Router series comprises fast Ethernet interface.

The conventional Ethernet interface complies with 10BASE-T physical layer specifications, working at 10 Mbps and in two modes: full duplex and half duplex.

The fast Ethernet interface complies with 100BASE-T and also 10BASE-T physical layer specifications, working at 10 Mbps or 100 Mbps, and in two modes: half duplex and full duplex. With the auto-negotiation capability, it can consult other network devices to determine and automatically select the optimum working mode and rate, thus greatly simplifying the configuration and management of the system.

Configure Ethernet Interface

Ethernet interface configuration includes:

- Enter view of specified Ethernet interface
- Set network protocol address
- Set frame format of sending message
- Set MTU
- Select working rate of fast Ethernet interface
- Select working mode of Ethernet interface
- Enable or disable internal loopback and external loopback.

The specified Ethernet interface cannot be configured unless you enter its view. It is necessary to configure IP address. Since there are default values for other parameters that can enable the system to work normally in most cases, it is recommended not to perform other configuration on Ethernet interface.

- 1 Enter view of specified Ethernet interface

Please use the following command in the all views.

Table 85 Enter view of specified Ethernet interface

Operation	Command
Enter view of specified Ethernet interface	interface ethernet number

2 Set network protocol address

The 3Com Router supports IP and IPX at Ethernet interface. Therefore, it is necessary to configure IP or IPX network address.

Please use the following commands in Ethernet interface view.

Table 86 Set IP address

Operation	Command
Set IP address	ip address ip-address ip-mask [sub]
Cancel IP address	undo ip address ip-address ip-mask [sub]

When an Ethernet interface is configured with two or more IP addresses, use keyword "**sub**" to identify them.

Please use the **ipx enable** command in system view, and use the **ipx network** in Ethernet interface view.

Table 87 Set IPX address

Operation	Command
Specify IPX network node value	ipx enable [node node]
Delete IPX network node value.	undo ipx enable
Specify IPX network number	ipx network network-number
Delete IPX network number	undo ipx network

3 Set frame format of sending message

Both Ethernet_II and Ethernet_SNAP can support IP and IPX. The Ethernet interface can identify these two formats out of received frame, but can only choose one frame format for the sent frame.

Please use the following commands in Ethernet interface view.

Table 88 Set frame format of sending message

Operation	Command
Set frame format of sending message	send-frame-type { ethernet_ii ethernet_snap }
Recover default frame format of sending message	undo send-frame-type

The frame format of sending message is Ethernet_II by default.

4 Set MTU

Maximum transmission unit (MTU) will influence the fragmentation and reassembling of network message.

Please use the following commands in Ethernet interface view.

Table 89 Set MTU

Operation	Command
Set MTU	mtu size

Recover MTU default value	undo mtu
---------------------------	-----------------

Value ranges and default values of MTUs with different link layer protocol are different. When Ethernet_II frame format is adopted, MTU value range will be 46-1500 bytes with the default value as 1500 bytes, and when Ethernet_SNAP frame format is adopted, MTU value range will be 46-1492 bytes with default value 1492 bytes.

5 Select work rate of fast Ethernet interface

As described before, the fast Ethernet interface can work at rates of 10Mbps and 100Mbps. Therefore, it is possible to select interface working rate with following command in Ethernet interface view.

Table 90 Select working rate of fast Ethernet interface

Operation	Command
Select working rate of fast Ethernet interface	speed { 100 10 negotiation }

The default is "**negotiation**", i.e. the system automatically chooses an optimum working rate. The user can also specify the interface working rate. But the rate specified must be the same as that of the actually connected network.

6 Select work mode of Ethernet interface

's Ethernet interface should work in half duplex mode when connected with HUB and in full duplex mode when connected with LAN Switch. Therefore, it is possible to select working mode with the following command in Ethernet interface view.

Table 91 Select working mode of Ethernet interface

Operation	Command
Select working mode of Ethernet interface	duplex { negotiation full half }

The default is "**negotiation**", i.e. the system automatically chooses an optimum working mode.

7 Enable or disable internal loopback and external loopback

When performing special functionality test on Ethernet interface, it needs to be set as internal loopback and external loopback sometimes. Therefore, it is possible to enable internal loopback and external loopback with the following commands in Ethernet interface view.

Table 92 Enable or disable internal loopback and external loopback

Operation	Command
Enable internal loopback and external loopback	loopback
Disable internal loopback and external loopback	undo loopback

The default is to disable both internal loopback and external loopback.

Display and Debug Ethernet Interface

The following command can be used to view the state of Ethernet interface in all views, so that the specified Ethernet interface can be displayed and debugged.

Table 93 Display the state of specified Ethernet interface

Operation	Command
Display the state of specified Ethernet interface	display interfaces ethernet number

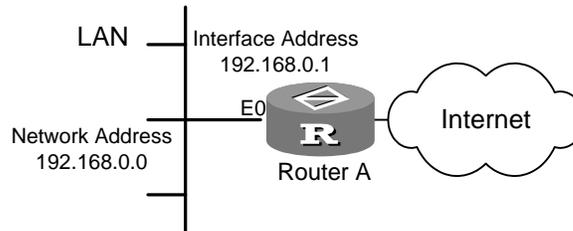
Typical Ethernet Interface Configuration Example

I. Networking Requirement

As shown below, the Ethernet interfaces of Router A is connected to IP networks 192.168.0.0. The computer in LAN connects to the Internet through Router A. Set the MTU of Ethernet interface to 1492 bytes, and set the frame format to Ethernet_II.

II. Network Diagram

Figure 45 Networking diagram of Ethernet configuration example



III. Configuration Procedure

- 1 Specify the IP address as 192.168.0.1 and the mask as 255.255.255.0.

```
[Router] interface ethernet 0
[Router-Ethernet0] ip address 192.168.0.1 255.255.255.0
```

- 2 Set MTU of the interface to 1492 bytes and frame format to Ethernet_II.

```
[Router-Ethernet0] mtu 1492
[Router-Ethernet0] send-frame-type ethernet_ii
```

Troubleshooting

The following test methods can be used to check faulty Ethernet interface is faulty:

- Ping the Ethernet interface from the host located in the same LAN as the router to observe whether the returned messages are correct.
- View the statistic information of two ends of the connection (such as the router and switch) to observe whether the statistic number of the received error frames increases quickly.

If either test fails to pass, it indicates that the Ethernet interface of the router or the connected Ethernet is abnormal.

After confirming the fault, proceed as follows:

- 1 View whether the LAN connection between the host and router is correct.

If the Ethernet is connected with HUB or LAN Switch, please check the status of relevant link indicators on HUB or LAN Switch. If the indicators are on, it means that the Ethernet interfaces of the host and router and the network cable are physically correct. Otherwise, please replace such faulty physical equipment as the network adapter, network cable, router or relevant interface module.

When the Ethernet is connected with unshielded twisted pair and at least one of the connected parties supports 100BASE-TX, rate matching must be taken into consideration. If the working rates of two parties do not match, i.e. one works in 100 Mbps mode while the other works in 10 Mbps mode, then the fault is that

the party with 100 Mbps configuration shows no connection, while the party with 10 Mbps connection shows the connection has been established. Furthermore, the activity indicator of the physical layer blink quickly and messages can not be received or transmitted normally.

On checking the connection of fast Ethernet interface of the 3Com Router series, the following prompt information is very helpful. Both these two pieces of information are output on the control console when the user is executing the rate selection command or connecting the network cable.

```
Ethernet 0: Warning--the link partner do not support 100M mode
Ethernet 0: Warning--the link partner may not support 10M mode
```

Here, the first piece of prompt information indicates that the opposite end, which is detected by the Ethernet interface of the 3Com Router series, does not support 100 Mbps working rate, while the local end is working at 100 Mbps rate by force. At this time, the user should ensure that the opposite side has been configured correspondingly and is working at the rate of 100 Mbps. The second prompt information indicates that the opposite end, detected by the Ethernet interface of the 3Com Router series, may not support 10 Mbps working rate, while the local end is forced to work in 10 Mbps rate. Now, the user should ensure the opposite end to work at the rate of 10 Mbps. However, when the Ethernet interface of the 3Com Router series is connecting 10/100 Mbps adaptive port of HUB, this information does not mean the setting is incorrect.

- 2 View whether IP addresses of the Ethernet interfaces of the host and router are within the same sub-net. That is the network addresses must be the same, only the host addresses are different. If they are not in the same sub-net, please re-set the IP address.

- 3 Check whether the link layer protocols match one another.

Take for example two link layer protocol standards supporting IP protocol, Ethernet_II and Ethernet_SNAP: These two link layer protocols have different encapsulation formats and MTU. MTU of the former has 1500 bytes and MTU of the latter has 1492 bytes. Two Ethernet devices can not communicate reliably unless they are connected with the same link layer protocol. The Ethernet interface of the 3Com Router series can simultaneously receive data frames with Ethernet_II and Ethernet_SNAP formats. However, the format of sending data frame must be in accordance with either Ethernet_II or Ethernet_SNAP as specified by the user. Therefore, please confirm whether the data frame sending format of the router is the same as that of other hosts. When the protocols do not match although the cables and interfaces are physically normal, they can not be pinged through.

- 4 View whether the working mode of the Ethernet interface is correct.

When connecting the Ethernet with unshielded twisted pair or fiber, there are two working modes: full duplex and half duplex, specified in 10BASE-T/100BASE-TX/100BASE-FX standard. When using HUB, the half-duplex working mode should be selected. When using LAN Switch, if LAN Switch works in half duplex mode, the Ethernet interface of the router also works in half duplex mode. If LAN Switch works in full duplex mode, the Ethernet interface of the router works in full duplex mode too. If the working mode is incorrect, i.e. one party of the connection works in full duplex mode while the other party in half duplex mode, fault will occur. That is, when network flow increases, the party working in half duplex mode shows frequent network collisions (for example, if

HUB is connected, all the other devices on the whole network segment will show serious network collisions), while the party working in full duplex mode shows large amount of error messages received, accompanied with serious message losses at both parties. In this case, use **display interfaces ethernet** command to view the error ratio of transceiving messages of the Ethernet interface. Usually, the collision can be observed through the status indicator of the network interface.

10

CONFIGURING WAN INTERFACE

This chapter contains information on the following topics:

- WAN Interface Introduction
- Asynchronous Serial Interface
- AUX Interface
- Synchronous Serial Interface
- ISDN BRI Interface
- CE1/PRI Interface
- CT1/PRI Interface
- E1-F Interface
- T1-F Interface
- CE3 Interface
- CT3 Interface

WAN Interface Introduction

The wide area network (WAN) can be divided into X.25 network, frame relay network, ATM network and ISDN network according to the line type. Accordingly, the router has synchronous/asynchronous serial interface, ATM interface, ISDN BRI and CE1/PRI.

Presently, the 3Com Router-supported WAN interfaces include asynchronous serial interface, AUX interface, synchronous serial interface, ISDN BRI interface CE1/PRI interfaces, CT3, CT1/PRI interface, E1-F interface, T1-F interface, CE3 interface.

Asynchronous Serial Interface

There are two asynchronous serial interfaces in the 3Com Router. One is Serial, which sets the synchronous/asynchronous serial interface to work in asynchronous mode. The other is Async, a special asynchronous serial interface.

You can set asynchronous serial interface to dedicated line mode or dialup mode. When the asynchronous serial interface is connected with Modem or ISDN terminal adapter (TA) externally, it can serve as a dialup interface, encapsulating link layer protocol SLIP or PPP, and supporting IP and IPX.

Configure Asynchronous Serial Interface

Asynchronous serial interface configuration includes:

- Set the synchronous/asynchronous serial interface to work in asynchronous mode
- Enter the view of specified asynchronous serial interface

- Set the asynchronous serial interface to work in dialup or dedicated line mode
- Set link layer protocol
- Set baud rate
- Set link establishment mode
- Set the check mode in flow mode
- Set stop bit in flow mode
- Set data bit in flow mode
- Set flow control mode
- Enable or disable level detection
- Enable or disable internal loopback and external loopback
- Set MTU
- Setting the coding format of Modem

The asynchronous serial interface may also need to be configured with SLIP parameter, PPP parameter, BDR parameter, IP address, firewall and standby center parameter as required.

1 Set the synchronous/asynchronous serial interface to work in asynchronous mode

If the physical interface to be configured is synchronous/asynchronous serial interface, it must be set to work in asynchronous mode by executing the following commands.

Please use the following command in the view of synchronous / asynchronous serial interface

Table 94 Set the synchronous/asynchronous serial interface to work in asynchronous mode

Operation	Command
Set the synchronous/asynchronous serial interface to work in asynchronous mode.	physical-mode async

The synchronous/asynchronous serial interface works in synchronous mode by default.

2 Enter the view of specified asynchronous serial interface

Please use the following commands to enter the view of the specified serial interface in all views.

Table 95 Enter view of specified asynchronous interface

Operation	Command
Enter the view of specified asynchronous serial interface	interface async number
Enter the view of the specified synchronous/asynchronous serial interface (which has been set to work in asynchronous mode)	interface serial number

3 Set the asynchronous serial interface to work in dialup or dedicated line mode.

For special asynchronous serial interface or the asynchronous serial interface set from synchronous/asynchronous serial interface, it is possible to dialup with **modem** command. Please see *Operation Manual - Dial-up* for other settings and detailed

instructions in dialup mode. In dedicated line mode, ensure that **modem** command is not configured, i.e. disable dial with **undo modem** command.

Please use the following commands in the view of asynchronous serial interface.

Table 96 Set the work mode of asynchronous serial interface

Operation	Command
Set the asynchronous serial interface to work in dial mode.	modem { in out }
Set the asynchronous serial interface to work in dedicated line mode.	undo modem

The asynchronous serial interface works in dial mode by default, i.e. **modem** command is configured by default. Both calling in and calling out are allowed with **modem in** and **modem out** command. The async/sync serial interface working in asynchronous mode works in dedicated line mode by default.

4 Set link layer protocol

The link layer protocol of asynchronous serial interface can be set as SLIP and PPP.

Please use the following command in the view of the asynchronous serial interface.

Table 97 Set the link layer protocol of asynchronous serial interface

Operation	Command
Set the link layer protocol of the asynchronous serial interface	link-protocol { slip ppp }

The default link layer protocol is PPP.

5 Set baud rate

Please use following command in the view of the asynchronous serial interface.

Table 98 Set the baud rate of asynchronous serial interface

Operation	Command
Set baud rate of the asynchronous serial interface	baudrate baudrate

Default value for baud rate is 9600bps.

When the asynchronous serial interface is used in dialup mode, the baud rate only refers to the communication rate between the asynchronous serial interface of the router and Modem. And the rate between two Modems must be determined according to the line quality after mutual consultation. Therefore, baud rate settings of asynchronous serial interfaces of two routers at two ends of the line can be inconsistent.

When the asynchronous serial interface is used in dedicated line mode, the baud rate setting must be consistent with the opposite equipment.



After the synchronous/asynchronous serial interface is set to work in asynchronous mode, the router will automatically change the baud rate to 9600bps.

6 Set link establishment mode

There are three link establishment modes for the asynchronous serial interface:

- Protocol: After the setup of a physical connection, the local end directly uses the set link layer protocol parameter to establish link with the opposite end.

Dedicated mode is usually used when asynchronous serial interfaces are directly connected.

- **Flow:** Also called the Interactive mode, which means two ends of the link interact with each other after the setup of a physical connection. The calling end sends configuration command to the receiving end (with the same effect as the user inputs configuration command remotely), sets working parameters of the link layer protocol at the receiving end and then establishes the link. This mode is usually used for such man-machine interactions as dumb terminal and dialing, etc.
- **Dumb terminal access (TTY) mode:** It is one type of flow mode. When the asynchronous serial interface of the router is used for dumb terminal access service, this key word and other related parameters could be used to set the number of physical terminal and virtual terminal (VTY) to be accessed. For detailed configuration, see Terminal Service User Manual.

Please use the following commands in the view of the asynchronous serial interface.

Table 99 Set the link establishment mode of asynchronous serial interface

Operation	Command
Set the asynchronous serial interface to establish the link in protocol mode	async mode protocol
Set the asynchronous serial interface to establish the link in flow mode	async mode flow

Establish the link in dedicated mode by default.

7 Set flow control mode

There are two types of data flow control methods, hardware flow control and software flow control, when an asynchronous serial interface adopts the flow mode to establish links. If hardware flow control is adopted, the data transmission on the asynchronous serial interface will be controlled by the hardware signal on the interface. When transmitting data, the interface will automatically detect the CTS signal. If there are CTS signals, it will transmit data. If no signals are detected, it will terminate the data transmission. If software flow control is adopted, the data transmission on the asynchronous serial interface will be controlled by the software flow control characters. When transmitting data, the interface will transmit data if receiving the flow control characters XON (0x11). It will terminate the transmitting, if receiving the flow control characters XOFF (0x13).

Please perform the following configuration in asynchronous serial interface view.

Table 100 Set the method of data flow control on an asynchronous serial interface

Operation	Command
Set the method of data flow control on an asynchronous serial interface	flow-control { none software hardware } [inbound outbound]

By default, the function of hardware flow control is enabled in the **inbound** direction, and the function of flow control is disabled in the **outbound** direction.



Hardware and software flow controls cannot be simultaneously used in the same direction. If configuring the software flow control in a direction already configured with the hardware flow control, the hardware control will be removed, and vice versa.

8 Set the check mode in flow mode

When the link establishment mode of async serial interface is flow or TTY, the two ends of the link will interact with each other after the setup of a physical connection. The calling end will send configuration command to the receiving end and set the interactive parameters of link layer protocol on the receiving end before the establishment of the link. In practical application (such as terminal server), the router will send configuration command to the terminal and transmit interactive operating parameters of the link layer that are set at local end to the opposite end.

This command is used to set the interactive operating parameter of the link layer protocol ---check mode.

Please perform the following configuration in asynchronous serial interface view.

Table 101 Set the check mode when the async serial interface works in flow mode

Operation	Command
Set the check mode when the async serial interface works in flow mode	parity { even mark none odd space }

By default, **none** is adopted for non-parity check.

9 Set stop bit in flow mode

This command is used to set another interactive operating parameter of the link layer protocol---the stop bit.

Please perform the following configuration in asynchronous serial interface view.

Table 102 Set the stop bit when the asynchronous serial interface works in flow mode

Operation	Command
Set the stop bit when the asynchronous serial interface works in flow mode	stopbits { 1 1.5 2 }

By default, there is only 1 stop bit.

10 Set data bit in flow mode

This command is used to set another interactive operating parameter of the link layer protocol--- the data bit.

Please perform the following configuration in asynchronous serial interface view.

Table 103 Set the data bit when the asynchronous serial interface works in flow mode

Operation	Command
Set the data bit when the asynchronous serial interface works in flow mode	databits { 5 6 7 8 }

5, **6**, **7** and **8** stand for 5, 6, 7 and 8 data bits respectively. By default, there are 8 data bits.

11 Enable or disable level detection

If the level detection is disabled for the asynchronous serial interface, the system will only detect whether the asynchronous serial interface connects cables externally and automatically report its state (UP or DOWN) to the user. If the level detection is enabled, the system will detect DSR signal in addition to the above-mentioned detection. Only when this signal is effective will the system regard the asynchronous serial interface as UP. Otherwise, it is regarded as DOWN.

Please use the following commands in the view of the asynchronous serial interface.

Table 104 Enable or disable the level detection for the asynchronous serial interface

Operation	Command
Enable the level detection for the asynchronous serial interface.	detect dsr-dtr
Disable the level detection for the asynchronous serial interface.	undo detect dsr-dtr

By default the level detection is enabled for the asynchronous serial interface.

12 Enable or disable internal loopback and external loopback

On performing special function test, the internal loopback and external loopback is enabled for the asynchronous serial interface.

Please use following commands in the view of the asynchronous serial interface.

Table 105 Enable or disable internal loopback and external loopback for the asynchronous serial interface

Operation	Command
Enable internal loopback and external loopback for the asynchronous serial interface.	loopback
Disable internal loopback and external loopback for the asynchronous serial interface.	undo loopback

The internal loopback and external loopback are disabled by default.

13 Set MTU

MTU of asynchronous serial interface influences the fragmentation and reassembling of IP network protocol message on this interface.

Please use the following commands in the view of the asynchronous serial interface.

Table 106 Set MTU of asynchronous serial interface

Operation	Command
Set MTU of asynchronous serial interface	mtu size
Recover MTU default	undo mtu

The unit of mtu is byte, ranging from 128 to 1500, with 1500 as default.

14 Set the coding format of Modem

Please perform the following configurations in asynchronous serial interface mode.

Table 107 Set the coding format of Modem

Operation	Command
Set the coding format of Modem	country-code area-name

AUX Interface

AUX interface is a fixed port provided by the 3Com Router. It can be used as a common asynchronous serial interface with the highest rate of 115200bps. It can also implement functions such as remote configuration of the router and line backup.

Configure AUX interface

1 Enter AUX interface view

Perform the following configuration in the all views.

Table 108 Enter AUX interface view

Operation	Command
Enter AUX interface view	interface aux 0

2 Configure AUX interface

The configuration of AUX interface is basically the same with that of common asynchronous serial interfaces. The following items should be noted:

- a The operating mode of AUX interface is Flow mode by default, and AUX interface work in dial mode by default.
- b When the data bit is configured on AUX interface, the parameter of the databits command cannot be 5. That is, AUX interface does not support the data bit 5.
- c When the stop bit is configured on AUX interface, the parameter of the stopbits command cannot be 1.5. That is, AUX interface does not support the stop bit 1.5.

In addition to the above points, AUX interface is configured in the same way as that of the asynchronous serial interface.

Synchronous Serial Interface

Features of synchronous serial interface:

- It can work in two modes: DTE and DCE. Usually, the synchronous serial interface serves as DTE and receives DCE-provided clock.
- The synchronous serial interface can connect multiple cables externally, such as V.24 and V.35. The 3Com Router can automatically detect types of cables connected externally and select electrical characters. There is no need to configure manually.
- The link layer protocols supported by synchronous serial interface include PPP, frame relay, LAPB and X.25.
- It supports IP and IPX network layer protocol.
- Type of external cable and the working mode (DTE/DCE) of the synchronous serial interface can be viewed with **display interfaces serial** command.

Configure Synchronous Serial Interface

Synchronous serial interface configuration includes:

- Set the synchronous/asynchronous serial interface to work in synchronous mode.
- Enter the view of specified synchronous serial interface.
- Set link layer protocol
- Set the digital signal encoding format
- Set baud rate.
- Select working clock
- Set clock inversion

- Enable or disable level detection
- Enable or disable data carrier detection
- Setting the synchronous serial interface to work in full duplex or half duplex mode
- Enable or disable internal loopback/external loopback
- Set MTU
- Set the time interval for sending keepalive packets
- Set the idle coding of synchronous serial interface

PPP/X.25/FR parameters, BDR parameters, IP address, firewall parameters and standby center parameters should be configured on the synchronous serial interface if needed. Refer to the relevant chapters in this manual for details.

1 Set the synchronous/asynchronous serial interface to work in synchronous mode.

Before further configuration, please set the synchronous/asynchronous serial interface to work in synchronous mode with the following command in the view of synchronous/asynchronous serial interface.

Table 109 Set the synchronous/asynchronous serial interface to work in synchronous mode

Operation	Command
Set the synchronous/asynchronous serial interface in synchronous mode.	<code>physical-mode sync</code>

The synchronous/asynchronous serial interface works in synchronous mode by default.

2 Enter the view of the specified synchronous serial interface

In all views, enter the view of the specified synchronous serial interface with the following command.

Table 110 Enter view of specified synchronous interface

Operation	Command
Enter the view of the specified synchronous/asynchronous serial interface (which has been set to work in synchronous mode)	<code>interface serial number</code>

3 Set link layer protocol

The link layer protocol of synchronous serial interface can be set to PPP, LAPB, X.25, Frame Relay, HDLC or SDLC.

Please use the following command in the view of the synchronous serial interface.

Table 111 Set the link layer protocol of synchronous serial interface

Operation	Command
Set link layer protocol	<code>link-protocol { fr hdlc lapb ppp sdlc x25 }</code>

Select PPP link layer protocol by default.

4 Set the digital signal encoding format

The synchronous serial interface support two digital signal encoding formats: NRZ (nonreturn to zero) and NRZI (nonreturn to zero, inverted).

Perform following commands in synchronous serial interface view.

Table 112 Set the digital signal encoding format of synchronous serial interface

Operation	Command
Using NRZI encoding format	code nrzi
Using NRZ encoding format	undo code

By default, the digital signal encoding format of synchronous serial interface is NRZ.

5 Set baud rate

Please use the following command in the view of the synchronous serial interface.

Table 113 Set the baud rate of synchronous serial interface

Operation	Command
Set baud rate of the synchronous serial interface	baudrate baudrate

When two synchronous serial interfaces are connected, the baud rate on line is determined at DCE-side. Therefore, when the synchronous serial interfaces are working in DCE mode, the baud rate is to be set. However, if the interfaces act as DTE, then the baud rate need not be configured. Default baud rate of synchronous serial interface is 64000 bps.



After the synchronous/asynchronous serial interface is set to synchronous mode from asynchronous mode, the system will automatically change the default baud rate to 64000 bps.

6 Select work clock

The synchronous serial interface works in two modes: DTE and DCE. Different working modes have different working clocks.

- If the synchronous serial interface is used as DCE, it is necessary to provide clock to the opposite DTE by choosing DCEclk.
- If the synchronous serial interface is used as DTE, the clock provided by the opposite DCE needs to be accepted. As the receiving clock and transmitting clock of the synchronous equipment are independent, the receiving clock of DTE can be the transmitting clock or receiving clock of DCE or the sending clock of DTE can be the transmitting clock or receiving clock of DCE. Thus, there will be four combinations, i.e. four kinds of clock selections are available at DTE side.

Figure 46 Schematic diagram of synchronous serial interface clock selection

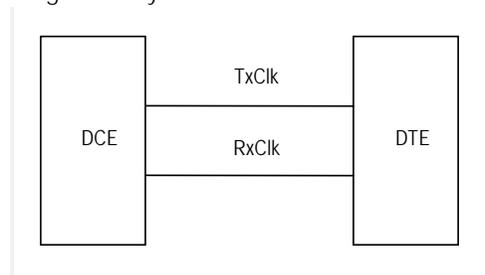


Table 114 Selection method with synchronous serial interface serving as DTE-side clock

Selection method	Meaning
------------------	---------

DTE1	TxCIk = TxCIk, RxCIk = RxCIk
DTE2	TxCIk = TxCIk, RxCIk = TxCIk
DTE3	TxCIk = RxCIk, RxCIk = TxCIk
DTE4	TxCIk = RxCIk, RxCIk = RxCIk



TxCIk stands for transmitting clock, RxCIk for receiving clock, the clock before “=” is DTE-side clock, and that behind “=” is DCE-side clock.

Please use the following commands in the view of the synchronous serial interface.

Table 115 Select work clock

Operation	Command
Select DCE-side synchronous serial interface clock	clock dceclk
Select DTE-side synchronous serial interface clock.	clock { dteclk1 dteclk2 dteclk3 dteclk4 }

The clock of DCE-side synchronous serial interface is **dceclk** by default, and that of DTE side is **dteclk3** by default.

7 Set clock inversion

In some special cases, the clock will generate half-period delay on the line, which may cause failed interconnection of equipment at two ends or large amount of messages discarded. In this case, the transmit clock signal of DTE-side synchronous serial interface can be inverted to eliminate the influence of delay.

Please use the following commands in the view of the synchronous serial interface.

Table 116 Set clock inversion

Operation	Command
Enable the inversion of transmit clock signal of DTE-side synchronous serial interface	invert transmit-clock
Disable the inversion of transmit clock signal of DTE-side synchronous serial interface	undo invert transmit-clock

The inversion is disabled by default.



This command is only effective to certain clock signals provided by some DCEs. Usually, clock inversion should not be set.

8 Enable or disable level detection

By default, when the system decides whether the synchronous serial interface is in UP status or DOWN status, it detects the DSR signal, DCD signal and whether the interface connects a cable at the same time. Only when the three signals are effective, will the system regard the interface is in UP status, otherwise, in DOWN status. If level detection is disabled for the synchronous serial interface, the system will not detect the DSR signal.

Please use the following commands in the view of the synchronous serial interface.

Table 117 Enable or disable level detection for the synchronous serial interface

Operation	Command
-----------	---------

Enable level detection for the synchronous serial interface.	detect dsr-dtr
Disable level detection for the synchronous serial interface.	undo detect dsr-dtr

Level detection is enabled for the synchronous serial interface by default.

9 Enable or disable data carrier detection

By default, when the system decides whether the synchronous serial interface is in UP status or DOWN status, it detects the DSR signal, DCD signal and whether the interface connects a cable at the same time. Only when the three signals are effective, will the system regard the interface is in UP status, otherwise, in DOWN status. If data carrier detection is disabled for the synchronous serial interface, the system will not detect the DCD signal.

Please use the following commands in the view of the synchronous serial interface.

Table 118 Enable or disable data carrier detection for the synchronous serial interface

Operation	Command
Enable data carrier detection for the synchronous serial interface.	detect dcd
Disable data carrier detection for the synchronous serial interface.	undo detect dcd

Data carrier detection is enabled for the synchronous serial interface by default.

10 Set the synchronous serial interface to work in full duplex or half duplex mode

To operate with some devices working in half-duplex mode, the synchronous serial interface can be configured to work in half-duplex mode.

Please make the following configurations in synchronous serial interface mode.

Table 119 Set the synchronous serial interface to work in full duplex or half duplex mode

Operation	Command
Set the synchronous serial interface to work in half duplex mode	reverse-rts
Set the synchronous serial interface to work in full duplex mode	undo reverse-rts

By default, the synchronous serial interface works in full duplex mode.

11 Enable or disable internal loopback/external loopback

To perform special function test, the internal loopback/external loopback are enabled for the synchronous serial interface.

Please use the following commands in the view of the synchronous serial interface.

Table 120 Enable/disable internal loopback/external loopback for the synchronous serial interface

Operation	Command
Enable the internal loopback/external loopback for the synchronous serial interface.	loopback
Disable the internal loopback/external loopback for the synchronous serial interface.	undo loopback

The internal loopback/external loopback are disabled by default.

12 Configure MTU

MTU of synchronous serial interface affects the fragmentation and reassembling of IP network protocol message on this interface.

Please use the following commands in the view of the synchronous serial interface.

Table 121 Set MTU of synchronous serial interface

Operation	Command
Set MTU of synchronous serial interface	mtu size
Recover the default value of MTU	undo mtu

The unit of mtu is byte, ranging between 128-1500, with 1500 as default.

13 Configure the time interval for sending keepalive packets

The serial interface will send keepalive packets to the opposite end at every keepalive interval to check if the link is in normal state or not.

Perform the following configuration in serial interface view.

Table 122 Set the time interval for sending keepalive packets

Operation	Command
Set the time interval for sending keepalive packets	timer hold seconds
Disable keepalive packet sending	undo timer hold

The time interval for sending keepalive packets is 10 seconds by default.



CAUTION: When the serial interface is encapsulated with HDLC protocol, the keepalive interval set on both ends of the link must be the same.

14 Set the idle coding of synchronous serial interface

Perform the following configuration in serial interface view.

Table 123 Set the idle coding of synchronous serial interface

Operation	Command
Set the idle coding of synchronous serial interface to "FF"	idle-mark
Restore the idle coding of synchronous serial interface to "7E"	undo idle-mark

The idle coding of synchronous serial interface is "7E".

ISDN BRI Interface**Technical Background**

Integrated Services Digital Network (ISDN) is a new technology developed from the 1970's. It can provide all-digital services from terminal user to terminal user and fulfill an all-digital transmission mode integrating services such as voice, data, graphics and video.

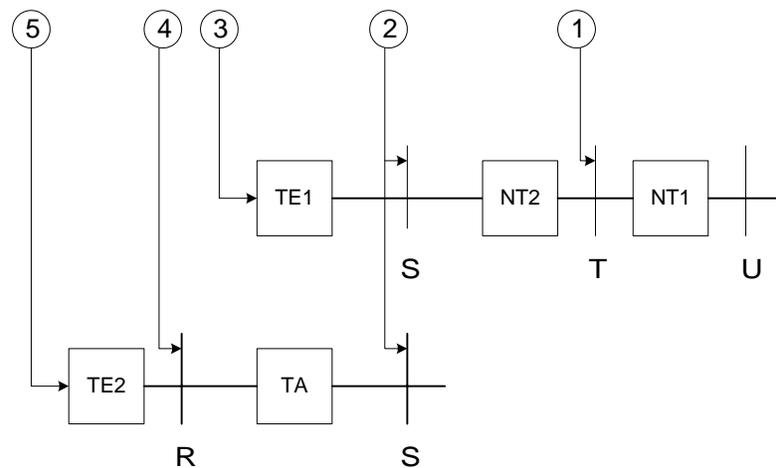
ISDN is different from conventional PSTN. In conventional PSTN, information is sent to the switch via analog user loop, converted to digital signal through A/D conversion and then resumed to analog signal when reaching the destination user. ISDN realizes the digital transmission of user loop to implement digital end-to-end communication. This will enable various digital and analog information to transmit via the standard digital interface. Besides, ITU-T standardizes ISDN services and formulates such recommendations as I.430, Q.921 and Q.931 to make any

equipment complying with relevant ISDN standard of ITU-T able to access ISDN easily.

User-network interface specification of ISDN:

In ITU-T I.411 recommendations, reference configurations for ISDN user-network interfaces are given according to concepts of function group (a group of functions required by users to access ISDN) and reference point (a point used to distinguish function groups), as shown in the following diagram.

Figure 47 Reference configuration of ISDN user-network interface



The function group includes:

- Network terminal 1 (NT1): It mainly fulfills functions of OSI layer 1 including the subscriber line transmission function, loop test and D channel contention.
- Network terminal 2 (NT2): Also called intelligent network terminal, including layer 1-layer 3 of OSI.
- Type-1 terminal equipment (TE1): Also called ISDN standard terminal, which is user equipment conforming to ISDN interface standard (such as digital phone set).
- Type-2 terminal equipment (TE2): Also called non-ISDN standard terminal, which is user equipment not conforming to ISDN interface standard.
- Terminal adapter (TA): It implements adaptation function, making TE2 to access ISDN standard interface.

The reference point includes:

- R reference point: It is between non-ISDN equipment and TA
- S reference point: It is between user terminal and NT2.
- T reference point: It is between NT1 and NT2.
- U reference point: It is between NT1 and line terminal.

Preparations before Configuration

Be clear about the following items before the configuration:

- Whether the interface provided by telecom service provider is ISDN BRI U interface or ISDN BRI S/T interface: In ITU-T I.411 recommendation, the reference model of ISDN user-network interface is given. However, there is a worldwide dispute about the position of division point between the user and network. And U interface or S/T interface is used according to different nations. In this case, before purchasing the router, the user must ensure whether the interface provided by the telecom server is ISDN BRI U interface or ISDN BRI S/T interface.
- Whether digital service is provided: ISDN can provide integrated services like digital service or voice service. Since the router is to perform digital communication, the ISDN line that the user applies for t be realized.
- Whether to select Point-to-Point connection or Point-to-Multipoint connection (optional): ISDN supports semi-permanent connection function. If the user only uses ISDN to connect fixed points, ISDN dedicated line can be used. Otherwise, Point-to-Multipoint connection is required.
- Caller Identification function (optional): On ISDN with CID function, the caller number can be filtered, so that only a group of user lines can dial in this router, enhancing the security of the network.

Configure ISDN BRI Interface

Please enter the view of the specified ISDN BRI interface with the following command in all views.

Table 124 Enter the view of the specified ISDN BRI interface

Operation	Command
Enter the view of the specified ISDN BRI interface	interface bri number

The ISDN BRI interface is used to dial up. Please refer to *Dial-up* for detail.

CE1/PRI Interface

Along with the emergence of Pulse Code Modulation (PCM) technique in the 1960s, Time Division Multiplexing (TDM) technique is eventually achieving broad applications in the digital communication systems. The TDM system is divided into two types: E1 system recommended by ITU-T and T1 system recommended by ANSI. The former one is widely applied in Europe and China, and the latter is mainly applied in North America and Japan (the J1 system adopted in Japan is similar to the T1 system and hence can be taken as T1 system).

CE1/PRI interface has two operating modes: E1 operating mode (also called non-channelized operating mode) and CE1/PRI operating mode (also called channelized operating mode).

When the CE1/PRI interface operates in E1 operating mode, it equals to an interface with the data bandwidth of 2 Mbps, on which no timeslots are divided. Its logic feature is the same as that of a synchronous serial interface. It supports the data link layer protocols such as PPP, Frame Relay, LAPB and X.25, and the network protocols such as IP and IPX.

When the CE1/PRI interface operates in CE1/PRI operating mode, it is physically divided into 32 timeslots numbered from 0 to 31. Timeslot 0 is used to transmit the synchronization information. This interface can be used as either a CE1 interface or a PRI interface.

- When the interface is used as a CE1 interface, all the timeslots except timeslot 0 can be divided into multiple channel sets at will, and each group can be used as an interface upon timeslot binding. Its logic feature is the same as that of a synchronous serial interface. It supports the data link layer protocols, such as PPP, Frame Relay, LAPB and X.25, and the network protocols such as IP and IPX.
- When the interface is used as a PRI interface, timeslot 16 will be used as a D channel to transmit signaling. Therefore, only a group of timeslots except the timeslots 0 and 16 can be chosen as the B channels. These timeslots can be bound together with timeslot 16 to form a pri set to be used as an interface. The logic feature of this interface will be the same as that of an ISDN PRI interface. It will support the data link layer protocol PPP and network protocols, such as IP and IPX, and can be configured with parameters such as BDR (Dial-on-Demand Routing).

Configure CE1/PRI Interface

CE1/PRI interface configuration includes:

- Enter the view for a specified interface
- Set the interface operating mode
- Bind the interface to be channel sets
- Bind the interface to be a pri set
- Set the line code format
- Set line clock
- Set frame format
- Enable/disable internal loopback/external loopback

1 Enter the view for a specified interface

In system view, use the following command to enter the view of a specified CE1/PRI interface.

Table 125 Enter the view of a specified interface

Operation	Command
Enter the view of CE1/PRI interface	controller e1 number

2 Set the interface operating mode

CE1/PRI interface has two operating modes: E1 operating mode and CE1/PRI operating mode

Perform the following configurations in CE1/PRI interface view.

Table 126 Set the operating mode of CE1/PRI interface

Operation	Command
Set the CE1/PRI interface to operate in E1 mode	using e1
Set the CE1/PRI interface to operate in CE1/PRI mode	using ce1

By default, the CE1/PRI interface operates in CE1/PRI operating mode.

After enabling the CE1/PRI interface to operate in E1 mode using the **using e1** command, the system will automatically create a serial interface numbered **serial number:0**. This interface owns the same logic feature as that of a synchronous serial interface, and can be treated as a synchronous serial interface for further configurations.

Perform the following configuration in all views.

Table 127 Enter the synchronous serial interface view

Operation	Command
Enter the synchronous serial interface view	interface serial number:0

The following are to be set:

- Operating parameters of data link layer protocol, such as PPP, Frame Relay, LAPB or X.25.
- IP address
- The operating parameters of the standby center need to be set when the interface serves as the main interface or standby interface of the standby center.
- The rules for address translation or packet filtering need to be set if the firewall is to be set up on the interface.

For more details, refer to the related sections of this manual.

3 Bind the interface to be channel sets

Perform the following configurations in CE1/PRI interface view.

Table 128 Bind the interface to be channel sets

Operation	Command
Bind the timeslots of CE1/PRI interface to a channel set	channel-set set-number timeslot-list range
Remove binding timeslots to form channel sets	undo channel-set set-number

The timeslots can be bind to form up to 31 channel sets on a CE1/PRI interface.



*The CE1/PRI interface can be bound to be channel sets only when it is enabled to operate in CE1/PRI mode through the **using ce1** command.*

Only one timeslot binding mode is supported on one CE1/PRI at one time, that is, the interface can only be bound into either channel sets or a pri set in that period.

After binding the interface to be channel sets, the system will automatically create a Serial interface numbered **serial number:set-number**. This interface has the same logic feature as that of a synchronous serial interface, and can be treated as a synchronous serial interface for further configurations.

Perform the following configuration in all views.

Table 129 Enter the synchronous serial interface view

Operation	Command
Enter the synchronous serial interface view	interface serial number:set-number

The following is to be set:

- Operating parameters of data link layer protocol, such as PPP, Frame Relay, LAPB or X.25.
- IP address
- The operating parameters of the standby center need to be set when the interface serves as the main interface or standby interface of the standby center.

- The rules for address translation or packet filtering need to be set if the firewall is to be set up on the interface.

For more details, refer to the related sections of this manual.

4 Bind an interface to be a pri set

Perform the following configurations in CE1/PRI interface view.

Table 130 Bind the interface to be a pri set

Operation	Command
Bind the timeslots of CE1/PRI interface to be a pri set	pri-set [timeslot-list range]
Remove binding timeslots to be a pri set	undo pri-set

Timeslots on a CE1/PRI interface can be bound to be only one pri set.

When binding an interface to be a pri set, timeslot 16 on a CE1/PRI interface is used as the D channel and the other timeslots are used as B channels. As for the CE1/PRI interface, timeslot 0 will be excluded since it is used to transmit the synchronous information. If no timeslots are specified to be bound, all the timeslots will be bound to form an interface similar to an ISDN PRI interface of 30B+D. If only timeslot 16 is bound, the binding activity will fail.



*The CE1/PRI interface can be bound to be a pri set only when it is enabled to operate in CE1/PRI mode through the **using ce1** command.*

Only one timeslot binding mode is supported on one CE1/PRI interface at one time, that is, the interface can only be bound into either channel sets or a pri set.

After the interface is bound to be a pri set, the system will automatically create a Serial interface numbered **serial number:15**. This interface is logically equivalent to an ISDN PRI interface, and hence you can further configure it.

Perform the following configuration in all views.

Table 131 Enter the ISDN interface view

Operation	Command
Enter the ISDN interface view	interface serial number:15

The following is to be set:

- BDR operating parameters
- Encapsulate the data link layer protocol PPP, its authentication parameters and etc.
- IP address
- The operating parameters of the standby center need to be set when the interface serves as the main interface or standby interface of the standby center.
- Configure the firewall if necessary.

For more details, refer to the related sections of this manual.

5 Set the line code format

A CE1/PRI interface supports two types of line code formats: **ami** format and **hdb3** format.

Perform the following configurations in CE1/PRI interface view.

Table 132 Set the line code format on the CE1/PRI interface

Operation	Command
Set the line code format on the CE1/PRI interface	<code>code { ami hdb3 }</code>
Restore the line code format on the CE1/PRI interface	<code>undo code</code>

By default, the line code format on the CE1/PRI interface is **hdb3**.

6 Set line clock

When the CE1/PRI interface operates as DCE, you should choose the internal clock, that is, **master** clock mode. When it operates as DTE, you should choose the line clock, that is, **slave** clock mode.

When the CE1/PRI interfaces on two routers are directly connected, the two ends will respectively operate in line clock mode (**slave**) and internal clock mode (**master**). When the CE1/PRI interfaces on routers are connected to a switch, the switch will operate as DCE which provides clock signal, the interfaces on the routers will operate in line clock mode (**slave**).

Perform the following configurations in CE1/PRI interface view.

Table 133 Set the line clock of the CE1/PRI interface

Operation	Command
Set the line clock of the CE1/PRI interface	<code>clock { master slave }</code>
Restore the line clock of the CE1/PRI interface to the default value	<code>undo clock</code>

By default, the line clock of CE1/PRI interface is **slave** clock.

7 Set the frame format of interface

When the CE1/PRI interface operates in CE1/PRI mode, it supports two types of frame formats: **crc** and **no-crc4**. The frame format **crc4** supports the 4-bit Cyclic Redundancy Check (CRC) on physical frames, whereas the frame format **no-crc4** does not.

Perform the following configurations in CE1/PRI interface view.

Table 134 Set the frame format of CE1/PRI interface

Operation	Command
Set the frame format of CE1/PRI interface	<code>frame-format { crc4 no-crc4 }</code>
Restore the frame format of CE1/PRI interface	<code>undo frame-format</code>

By default, the frame format of CE1/PRI interface is **no-crc4**.

8 Enable/disable internal loopback/external loopback

The interface needs to be set to internal loopback or external loopback when during the test on some special functions.

Perform the following configurations in CE1/PRI interface view.

Table 135 Enable/disable the internal loopback/external loopback

Operation	Command
Enable the internal loopback/external loopback of the CE1/PRI	<code>loopback</code>
Disable the internal loopback/external loopback of the CE1/PRI	<code>undo loopback</code>

By default, the functions of internal loopback and external loopback are disabled on the CE1/PRI interface.

Display and Debug CE1/PRI Interface

Perform the following configurations in all views to display the status and related information of the CE1/PRI interface, so as to monitor and maintain it.

Table 136 Display and debug CE1/PRI interface

Operation	Command
Display the operating status of the CE1/PRI interface	display controller e1 interface-number
Display the operating status of the channel set or pri set	display interfaces serial interface-number:number

Generally, CE1/PRI interface is applied to the dedicated line and dial-up services. For the typical configuration example and troubleshooting, refer to the configurations of protocols at each layer and dialing configurations in this manual.

CT1/PRI Interface

Along with the emergence of Pulse Code Modulation (PCM) technique in the 1960s, Time Division Multiplexing (TDM) technique is eventually achieving broad applications in the digital communication systems. The TDM system is divided into two types: T1 system recommended by ANSI and E1 system recommended by ITU-T. The former one is mainly applied in North America and Japan (the J1 system adopted in Japan is similar to the T1 system and hence can be taken as T1 system), and the latter is widely applied in Europe and China.

T1 line is comprised of 24 multiplexed channels. In other words, one T1 primary frame DS1 contains 24 DS0 (64kbps) timeslots, each of them has 8 bits, and other 1 bit is taken as the framing bit. As a result, each primary frame has 193 bits. This value can be got as follows: $24 \times 8 + 1 = 193$ bits. Since 8000 frames can be sent per second, the transmission speed of DS1 is $193 \times 8K = 1.544$ Mbps.

The CT1/PRI interface can only operate in channelized operating mode. It is used in the following two ways:

- When the interface is used as a CT1 interface, all the timeslots from 1 to 24 can be divided into multiple groups at will, and each group can be bound to form a channel set. Upon the binding of each group of timeslots, the system automatically generates an interface which logically equals to a synchronous serial interface. It supports the data link layer protocols such as PPP, Frame Relay, LAPB and X.25, and the network protocols such as IP and IPX.
- When the interface is used as a PRI interface, timeslot 24 will be used as a D channel to transmit signaling. Therefore, only a group of timeslots except the timeslot 24 can be chosen as the B channels. These timeslots can be bound together with timeslot 24 to form a pri set which acts as an interface. The logic feature of this interface will be the same as that of an ISDN PRI interface. It will support the PPP data link layer protocol and network protocols, such as IP and IPX, and can be configured with parameters, such as BDR.

Configure CT1/PRI interface

CT1/PRI interface configuration includes:

- Enter the view for a specified interface
- Bind the interface to be channel sets

- Bind the interface to be a pri set
 - Set the length/attenuation of the transmission cable
 - Set the line code format
 - Set line clock
 - Set frame format
 - Enable/disable internal loopback/external loopback
- 1 Enter the view for a specified interface
- In system view, use the following command to enter the view of a specified CT1/PRI interface.

Table 137 Enter the view of a specified interface

Operation	Command
Enter the view of CT1/PRI interface	controller t1 number

- 2 Bind the interface to be channel sets
- Perform the following configurations in CT1/PRI interface view.

Table 138 Bind the interface to be channel sets

Operation	Command
Bind the timeslots of CT1/PRI interface to a channel set	channel-set set-number timeslot-list range [speed { 56 64 }]
Remove binding timeslots to form channel sets	undo channel-set set-number

The timeslots can be bind to form up to 24 on a CT1/PRI interface.



The CE1/PRI interface can be bound to be channel sets only when it is enabled to operate in CE1/PRI mode through the using ce1 command.

Only one timeslot binding mode is supported on one CT1/PRI interface at one time, that is, the interface can only be bound into either channel sets or a pri set in that period.

After binding the interface to be channel sets, the system will automatically create a Serial interface numbered **serial number:set-number**. This interface has the same logic feature as that of a synchronous serial interface, and can be treated as a synchronous serial interface for further configurations.

Perform the following configuration in all views.

Table 139 Enter the synchronous serial interface view

Operation	Command
Enter the synchronous serial interface view	interface serial number:set-number

The following is to be set:

- Operating parameters of data link layer protocol, such as PPP, Frame Relay, LAPB or X.25.
- IP address
- The operating parameters of the standby center need to be set when the interface serves as the main interface or standby interface of the standby center.

- The rules for address translation or packet filtering need to be set if the firewall is to be set up on the interface.

For more details, refer to the related sections of this manual.

3 Bind an interface to be a pri set

Perform the following configurations in CT1/PRI interface view.

Table 140 Bind the interface to be a pri set

Operation	Command
Bind the timeslots of CT1/PRI interface to be a pri set	pri-set [timeslot-list range]
Remove binding timeslots to be a pri set	undo pri-set

Timeslots on a CT1/PRI interface can be bound to be only one pri set.

When binding an interface to be a pri set, timeslot 24 is used as the D channel and the other timeslots are used as B channels. If no timeslots are specified to be bound, all the timeslots will be bound to form an interface similar to an ISDN PRI interface of 23B+D. If only timeslot 24 on the CT1/PRI interface is bound, the binding activity will fail.



Only one timeslot binding mode is supported on one CT1/PRI interface at one time, that is, the interface can only be bound into either channel sets or a pri set.

After the interface is bound to be a pri set, the system will automatically create a Serial interface numbered **serial number:23**. This interface is logically equivalent to an ISDN PRI interface, and hence you can further configure it.

Perform the following configuration in all views.

Table 141 Enter the ISDN interface view

Operation	Command
Enter the ISDN interface view	interface serial number:23

The following is to be set:

- BDR operating parameters
- Encapsulate the data link layer protocol PPP, its authentication parameters and etc.
- IP address
- The operating parameters of the standby center need to be set when the interface serves as the main interface or standby interface of the standby center.
- Configure the firewall if necessary.

For more details, refer to the related sections of this manual.

4 Set the length/attenuation of the transmission cable

When the CT1/PRI interface connects the transmission cables of different lengths, to ensure the quality of the signal to be received by the receiving end, the attenuation and waveform of signal should match the transmission cables.

Perform the following configurations in CT1/PRI interface view.

Table 142 Set the length/attenuation of the transmission cable of CT1/PRI interface

Operation	Command
-----------	---------

Set the CT1/PRI interface to use long-distance transmission cable	<code>cable long { 0db -7.5db -15db -22.5db }</code>
Set the CT1/PRI interface to use short-distance transmission cable	<code>cable short { 133ft 266ft 399ft 533ft 655ft }</code>
Restore the default value of the transmission cable used by the CT1/PRI interface	<code>undo cable</code>

By default, the attenuation of transmission cable that the CT1/PRI interface matches is **long 0db**.

5 Set the line code format

A CT1/PRI interface supports two types of line code formats: **ami** format and **b8zs** format.

Perform the following configurations in CT1/PRI interface view.

Table 143 Set the line code format on the CT1/PRI interface

Operation	Command
Set the line code format on the CT1/PRI interface	<code>code { ami b8zs }</code>
Restore the line code format on the CT1/PRI interface	<code>undo code</code>

By default, the line code format on the CT1/PRI interface is **b8zs**.

6 Set line clock

When the CT1/PRI interface operates as DCE, you should choose the internal clock, that is, **master** clock mode. When it operates as DTE, you should choose the line clock, that is, **slave** clock mode.

When the CT1/PRI interfaces on two routers are directly connected, the two ends will respectively operate in line clock mode (**slave**) and internal clock mode (**master**). When the CT1/PRI interfaces on routers are connected to a switch, the switch will operate as DCE which provides clock signal, the interfaces on the routers will operate in line clock mode (**slave**).

Perform the following configurations in CT1/PRI interface view.

Table 144 Set the line clock of the CT1/PRI interface

Operation	Command
Set the line clock of the CT1/PRI interface	<code>clock { master slave }</code>
Restore the line clock of the CT1/PRI interface to the default value	<code>undo clock</code>

By default, the line clock of CT1/PRI interface is **slave** clock.

7 Set the frame format of interface

A CT1/PRI interface supports two frame formats: Super Frame (SF) and Extended Super Frame (ESF). In SF format, multiple frames can share the same frame-synchronization information and signaling information, so that more significant bits can be used to transmit user data. In practice, a system should be tested often. The application of ESF satisfies the requirement that the services are still in normal operation even at the time of testing.

Perform the following configurations in CT1/PRI interface view.

Table 145 Set the frame format of CT1/PRI interface

Operation	Command
-----------	---------

Set the frame format of CT1/PRI interface	frame-format { sf esf }
Restore the frame format of CT1/PRI interface to the default value	undo frame-format

By default, the frame format of CT1/PRI interface is ESF.

8 Enable/disable internal loopback/external loopback

The interface needs to be set to internal loopback or external loopback when during the test on some special functions.

Perform the following configurations in CT1/PRI interface view.

Table 146 Enable/disable the internal loopback/external loopback of the CT1/PRI

Operation	Command
Enable the internal loopback/external loopback of the CT1/PRI	loopback { remote local }
Disable the internal loopback/external loopback of the CT1/PRI	undo loopback { remote local }

By default, the functions of internal loopback and external loopback are disabled on the CT1/PRI interfaces.

Display and Debug CT1/PRI Interface

Perform the following configurations in all views to display the status and related information of the CT1/PRI interface, so as to monitor and maintain it.

Table 147 Display and debug CT1/PRI interface

Operation	Command
Display the operating status of the CT1/PRI interface	display controller t1 interface-number
Display the operating status of the channel set or pri set	display interfaces serial interface-number :number

Generally, CT1/PRI interfaces are applied to the dedicated line and dial-up services. For the typical configuration example and troubleshooting, refer to the configurations of protocols at each layer and dialing configurations in this manual.

E1-F Interface

E1-F interface is fractional E1 interface, and it is respectively simplified CE1/PRI interface. If there is no need to use multiple channel sets or if ISDN PRI is not necessary in an E1 application, it is too much to use CE1/PRI interface. At this time, E1-F interface is more than enough for meeting the simple E1 access requirements. Compared with CE1/PRI interface, E1-F interface is a nice low-cost choice for E1 access.

Compared with CE1/PRI interfaces, E1-F interface has the following features:

- When working in framed mode, E1-F interface can only bind time slots into one channel set, but CE1/PRI interface can group timeslots randomly and bind them into multiple channel sets.
- E1-F interface does not support PRI operating mode.

E1-F interface can work in both framed and unframed modes.

When it works in unframed mode, it is a timeslot-less interface of 2048kbps data bandwidth. In this case, it is logically equivalent to a synchronous serial interface,

supporting the data link layer protocols PPP, HDLC, Frame Relay, LAPB and X.25, as well as the network protocols IP and IPX.

When it works in framed mode, however, it is physically divided into 32 time slots numbered in the range of 0 to 31. In these time slots, except for time slot 0 used for synchronization information transmission, all the other time slots can be randomly bound into one channel set. E1-F interface has the rate of nx64kbps, owns logical features of synchronous serial interface, and supports the data link layer protocols PPP, Frame Relay, LAPB and X.25 as well as the network protocols IP and IPX.

Configure E1-F Interface

E1-F interface configuration includes:

- Enter the view of a specified interface
- Set interface operating mode
- Set interface rate after binding operation
- Set line code format
- Set line clock
- Set interface frame format
- Enable or disable local/remote loopback

1 Enter the view of a Specified Interface

Unlike CE1/PRI interface, E1-F interface has no Controller view. The system identify an E1-F interface as a synchronous serial interface, so entering the view of E1-F interface is equivalent to entering the view of the corresponding serial interface.

Perform the following configuration in all views.

Table 148 Enter the view of an E1-F interface

Operation	Command
Enter the view of an E1-F interface	interface serial serial-number

E1-F interface is sequenced based on the same numbering and are numbered together with the synchronous serial interfaces. For example, insert one 1E1-F module in slot 0 on a 3Com Router, and one 4SA module in slot 1. Hence, the E1-F interface will be numbered Serial 0, and the 4SA interfaces will be numbered Serial 1 through Serial 4.

2 Set Interface Operating Mode

E1-F interface can work in both unframed and framed modes.

Perform the following configuration in E1-F interface view.

Table 149 Set Operating mode for an E1-F interface

Operation	Command
Set an E1-F interface to work in unframed mode	fel unframed
Set the E1-F interface to work in framed mode	undo fel unframed

By default, E1-F interfaces work in framed mode.

3 Set Interface Rate after Binding Operation

When E1-F interface works in framed mode, time slot binding on the interfaces can be made according to user's demands.

Perform the following configuration in E1-F interface view.

Table 150 Set interface rate after binding operation

Operation	Command
Bind time slots on an E1-F interface	fel timeslot-list { all range }
Restore the default setting for time slot binding on the interface	undo fel timeslots

By default, binding operation will be done on all the time slots on E1-F interface.



Time slot 0 on E1-F interface is used for synchronization information transmission. Therefore, in practice, only time slots 1 through 31 are bound when performing binding operation on all the time slots on an E1-F interface.

Unlike CE1/PRI interface, only one channel set can be bound on an E1-F interface, and this channel set is associated with the current synchronous serial interface. On a CE1/PRI interface, however, multiple channel sets can be bound, and the system will automatically generate a synchronous serial interface accordingly whenever a channel set is formed.

4 Set Line Code Format

E1-F interfaces support line code formats AMI (Alternate Mark Inversion) and HDB3 (High Density Bipolar 3).

Perform the following configuration in E1-F interface view.

Table 151 Set line code format for E1-F interfaces

Operation	Command
Set line code format for an E1-F interface	fel code { ami hdb3 }
Restore the default line code format for an E1-F interface	undo fel code

The line code format for an E1-F interface defaults to **hdb3**.

5 Set Line Clock

If E1-F interface is used as DCE, the **slave** clock should be selected. If it is used as DTE, the **master** clock should be selected.

If the E1-F interfaces of two routers are directly connected, they must respectively work in **slave** and **master** clock modes. If the E1-F interface of the router is connected to an exchange, however, the exchange is working as DCE and provides clock, so the interface of the router should work in **master** clock mode.

Perform the following configuration in E1-F interface view.

Table 152 Set line clock for an E1-F interface

Operation	Command
Set line clock for an E1-F interface	fel clock { master slave }
Restore the line clock of the E1-F interface to the default setting	undo fel clock

By default, the clock of E1-F interface is **slave** clock.

6 Set Interface Frame Format

When an E1-F interface is working in framed mode, it supports both CRC4 (4-bit Cyclic Redundant Check) and no-CRC4 frame formats.

Perform the following configuration in E1-F interface view.

Table 153 Set frame format for an E1-F interface

Operation	Command
Set frame format for an E1-F interface	fel frame-format { crc4 no-crc4 }
Restore the default frame format of the E1-F interface	undo fel frame-format

By default, the frame format of E1-F interface is no-CRC4.

7 Enable or Disable Local Loopback/Remote Loopback

An interface should be placed in local loopback or remote loopback for some special functionality tests.

Perform the following configuration in E1-F interface view.

Table 154 Enable/Disable local/remote loopback on an E1-F interface

Operation	Command
Enable local/remote loopback on an interface	fel loopback { local remote }
Disable local/remote loopback on an interface	undo fel loopback [local remote]

By default, no E1-F interface is placed in local or remote loopback.



On an interface, using this command but with different arguments can respectively enable local loopback and remote loopback, but these two functions cannot be enabled at the same time.

Display and Debug E1-F Interface

Perform the **display** command in all views to display the state of E1-F interface and other related information.

Table 155 Display and debug E1-F interface

Operation	Command
Display configuration and state of E1-F interface	display fel [serial serial-number]
Display the operating state of E1-F interface	display serial serial-number

T1-F Interface

T1-F interface is fractional T1 interface, and it is respectively simplified CT1/PRI interface. If there is no need to use multiple channel sets or if ISDN PRI is not necessary in an T1 application, it is too much to use CT1/PRI interface. At this time, T1-F interface is more than enough for meeting the simple T1 access requirements. Compared with CT1/PRI interface, T1-F interfaces is a nice low-cost choice for T1 access.

Compared with CT1/PRI interface, T1-F interface has the following features:

- When working in framed mode, T1-F interface can only bind time slots into one channel set, but CT1/PRI interface can group timeslots randomly and bind them into multiple channel sets.
- T1-F interface does not support PRI operating mode.

T1 line comprises 24 multiplexed channels. That is, a T1 primary group frame DS1 (Digital Signal Level-1) comprises 24 DS0 (64kbps) time slots, each has 8 bits and 1 framing bit for synchronization, and thus each primary group frame has 193 bits (24 X 8+1). As DS1 can transmit 8000 frames per second, its transmission speed is 193 X 8k = 1544kbps.

T1-F interface can only work in framed mode, and it can randomly bind all time slots (time slots 1 through 24) into one channel set. T1-F interface has the rate of nx64kbps or nx56kbps, owns logical features of synchronous serial interface, and supports the data link layer protocols PPP, HDLC, Frame Relay, LAPB and X.25 as well as the network protocols IP and IPX.

Configure T1-F Interface

T1-F interface configuration includes:

- Enter the view of a specified interface
- Set interface rate after binding operation
- Set length/attenuation of transmission line
- Set line code format
- Set line clock
- Set interface frame format
- Enable or disable local/remote loopback

1 Enter the view of a Specified Interface

Unlike CT1/PRI interface, T1-F interface has no Controller view. The system identify a T1-F interface as a synchronous serial interface, so entering the view of T1-F interface is equivalent to entering the view of the corresponding serial interface.

Perform the following configuration in all views.

Table 156 Enter the view of an T1-F interface

Operation	Command
Enter the view of a T1-F interface	interface serial serial-number

T1-F interface is sequenced based on the same numbering and are numbered together with the synchronous serial interfaces. For example, insert one 1E1-F module in slot 0 on a 3Com Router, one 4SA module in slot 1, and two 1T1-F

module in slot 2. Hence, the E1-F interface will be numbered Serial 0, and the 4SA interfaces will be numbered Serial 1 through Serial 4, and the T1-F interfaces will be numbered Serial 5 and Serial 6.

2 Set Interface Rate after Binding Operation

When T1-F interface works in framed mode, time slot binding on the interfaces can be made according to user's demands.

Perform the following configuration in T1-F interface view.

Table 157 Set interface rate after binding operation

Operation	Command
Bind time slots on a T1-F interface	ft1 timeslot-list { all range } [speed { 56 64 }]
Restore the default setting for time slot binding on the interface	undo ft1 timeslots

By default, binding operation will be done on all the time slots on T1-F interface.

Unlike CT1/PRI interface, only one channel set can be bound on a T1/F interface, and this channel set is associated with the current synchronous serial interface. On a CT1/PRI interface, however, multiple channel sets can be bound, and the system will automatically generate a synchronous serial interface accordingly whenever a channel set is formed.

3 Set Length/Attenuation for Transmission Line

If a T1-F interface is connected to the transmission lines of various lengths, you should match attenuation and waveform of the interface signals with the transmission lines.

Perform the following configuration in T1-F interface view.

Table 158 Set length/attenuation of transmission line on a T1-F interface

Operation	Command
Set the T1-F interface to use long-distance transmission line	ft1 cable long decibel
Set the T1-F interface to use short-distance transmission line	ft1 cable short length
Restore the default setting of the transmission line for the T1-F interface	undo ft1 cable

By default, attenuation matched a T1-F interface is **long 0db**.

4 Set Line Code Format

T1-F interface supports line code formats AMI (Alternate Mark Inversion) and B8ZS (Bipolar 8-Zero Substitution).

Perform the following configuration in T1-F interface view.

Table 159 Set line code format for T1-F interface

Operation	Command
Set line code format for a T1-F interface	ft1 code { ami b8zs }
Restore the default line code format for a T1-F interface	undo ft1 code

The line code format for an T1-F interface defaults to **b8zs**.

5 Set Line Clock

If T1-F interface is used as DCE, the **slave** clock should be selected. If it is used as DTE, the **master** clock should be selected.

If the T1-F interfaces of two routers are directly connected, they must respectively work in **slave** and **master** clock modes. If the T1-F interface of the router is connected to an exchange, however, the exchange is working as DCE and provides clock, so the interface of the router should work in **master** clock mode.

Perform the following configuration in T1-F interface view.

Table 160 Set line clock for a T1-F interface

Operation	Command
Set line clock for a T1-F interface	ft1 clock { master slave }
Restore the line clock of the T1-F interface to the default setting	undo ft1 clock

By default, the clock of T1-F interface is **slave** clock.

6 Set Interface Frame Format

T1-F interfaces support Super Frame (SF) and Extended Super Frame (ESF). In SF, multiple frames can share the same frame synchronization and signaling information, so that more significant bits can be used for transmitting user data. In practice, the system test is often required. The application of ESF technology can ensure normal service when the system test is being carried out.

Perform the following configuration in T1-F interface view.

Table 161 Set frame format of T1-F interface

Operation	Command
Set frame format for a T1-F interface	ft1 frame-format { sf esf }
Restore the default frame format of T1-F interface	undo ft1 frame-format

By default, the frame format of T1-F interface is ESF.

7 Enable or Disable Local Loopback/Remote Loopback

An interface should be placed in local loopback or remote loopback for some special functionality tests.

Perform the following configuration in T1-F interface view.

Table 162 Enable/Disable local/remote loopback on a T1-F interface

Operation	Command
Enable local/remote loopback on an interface	ft1 loopback { local remote }
Disable local/remote loopback on an interface	undo ft1 loopback [local remote]

By default, no T1-F interface is placed in local or remote loopback.



On an interface, using this command but with different arguments can respectively enable local loopback and remote loopback, but these two functions cannot be enabled at the same time.

Display and Debug T1-F Interface

Perform the **display** command in all views to display the state of T1-F interface and other related information.

Table 163 Display and debug T1-F interface

Operation	Command
Display configuration and state of T1-F interface	display ft1 [serial <i>serial-number</i>]
Display the operating state of T1-F interface	display serial <i>serial-number</i>

CE3 Interface

Both E3 and E1 belong to ITU-T digital carrier system and are used in most areas outside the North America. The data transmission rate of E3 interface is 34.368Mbps, and the line coding/decoding is HDB3 (High-Density Bipolar 3).

CE3 interface has two operating modes:

- When working in E3 mode, the interface is equivalent to a fractional interface of data bandwidth 34.368Mbps.
- When working in CE3 mode, the interface can multiplex/demultiplex 16 channels of E1 signals. E3-to-E1 multiplex is compliant with ITU-T G.751 and G.742. Each E1 interface can be divided into 32 time slots numbered in the range of 0 to 31. The time slots between 1 and 31 can be randomly bound into N x 64Kbps logical channels (time slot 0 for transmitting frame synchronizing signals cannot participate in binding operation). Therefore, CE3 interface can be channelized into E1 channels of 64Kbps.

CE3 interface supports the link layer protocols PPP, HDLC, Frame Relay, LAPB and X.25, and the network protocols such as IP and IPX.

Configure CE3 Interface

CE3 interface configuration includes:

- Enter the view of the specified CE3 interface
- Set clock mode for the CE3 interface
- Set national bit for the CE3 interface
- Set the loopback mode of the CE3 interface
- Set E1 Frame format
- Set operating mode of CE3 interface

Depending on the networking requirements, you may need to configure the parameters such as PPP, Frame Relay and IP address for the CE3 interface. For details, refer to the involving chapters.

1 Enter view of Specified Interface for Configuration

CE3 interface uses the **controller** command to enter its view.

Perform the following configuration in system view to enter the view of the specified CE3 interface.

Table 164 Enter the view of the specified E3 interface

Operation	Command
Enter the view of CE3 interface	controller e3 number

2 Set Clock Mode of CE3 Interface

Perform the following configuration in CE3 interface view.

Table 165 Set clock mode of the CE3 interface

Operation	Command
Set clock mode of the CE3 interface	clock { master slave }
Restore the default clock mode of CE3 interface	undo clock

By default, CE3 interface uses slave clock.

The user can also set clock mode for E1 channels of CE3 interface.

Table 166 Set clock mode of the E1 channel

Operation	Command
Set clock mode of the E1 channel	e1 line-number set clock { master slave }
Restore the default clock mode of E1 channel	undo e1 line-number set clock

By default, E1 channel uses **slave** clock.

3 Set National Bit for CE3 Interface

Perform the following configuration in CE3 interface view.

Table 167 Set a national bit of the CE3 interface

Operation	Command
Set national bit of the CE3 interface	national-bit { 0 1 }
Restore the default national bit	undo national-bit

By default, national bit of CE3 interface is 1.

4 Set the Loopback Mode of CE3 Interface

Perform the following configuration in CE3 interface view.

Table 168 Set loopback mode of CE3 interface

Operation	Command
Set loopback mode of CE3 interface	loopback { local payload remote }
Disable loopback on the CE3 interface	undo loopback

By default, loopback is disabled.

Single-channel loopback can be set on the E1 channels on a CE3 interface, and the settings of individual channels are independent.

Table 169 Set loopback mode of E1 channel

Operation	Command
Set loopback mode of E1 channel	e1 line-number set loopback { local remote }
Disable loopback on the E1 channel	undo e1 line-number set loopback

5 Set E1 Frame Format

If framing has been enabled on an E1 channel, you can set its frame format. Perform the following configuration in CE3 interface view.

Table 170 Set E1 frame format

Operation	Command
Set E1 frame format	e1 line-number set frame-format { crc4 no-crc4 }
Restore the default CRC setting	undo e1 line-number set frame-format

By default, the frame format of E1 channel is **no-crc4**.

6 Configure Operating Mode of CE3 Interface

When setting the operating mode of an CE3 interface, you should set the operating modes of both the CE3 interface and the E1 channels on the interface.

Perform the following configuration in CE3 interface view.

Table 171 Set the operating mode of CE3 interface

Operation	Command
Enable E3 mode	using e3
Enable CE3 mode	using ce3
Restore the default operating mode	undo using

By default, CE3 mode is used.

When CE3 interface works in E3 mode, the system will automatically create a serial interface whose number is **serial number/0:0** and whose rate is 34.368 Mbps. The interface has the same logic feature as that of a synchronous serial interface, therefore, it can be regarded as a synchronous serial interface for further configuration.

Table 172 Set the operating mode of E1 channel

Operation	Command
Configure E1 channels of CE3 interface to work in E1 mode (unframed mode)	e1 line-number unframed
Configure E1 channels of CE3 interface to work in CE1 mode (framed mode)	undo e1 line-number unframed
Implement time slot binding on the CE1 interface	e1 line-number channel-set set-number timeslot-list range
Disable time slot binding on the CE1 interface	undo e1 line-number channel-set set-number

The operation mode of E1 channels defaults to CE1 mode.

When E1 channel works in E1 mode (unframed mode), the system will automatically create a serial interface whose number is **serial number / line-number:0** and whose rate is 2048 kbps. The interface has the same logic feature as that of a synchronous serial interface, therefore, it can be regarded as a synchronous serial interface for further configuration.

When E1 channel works in CE1 mode (framed mode), timeslot binding can be performed on it. The system will automatically create a serial interface whose number is **serial number / line-number:set-number** and whose rate is N x 64 kbps. The interface has the same logic feature as that of a synchronous serial interface, therefore, it can be regarded as a synchronous serial interface for further configuration.

Display and Debug CE3 Interface

The display and debug operations of CE3 interface include disabling interface and displaying interface information. But you should be careful when using the **shutdown** command, because disabling an interface will cause the interface to stop working.

Perform the following configuration in all views.

Table 173 Display and debug CE3 interface

Operation	Command
Disable the CE3 interface	shutdown
Enable the CE3 interface	undo shutdown
Disable the E1 channel	e1 line-number shutdown
Enable the E1 channel	undo e1 line-number shutdown
Display the CE3 interface information	display controller e3 number

The enabling/disabling operation done on the CE3 interface takes effect on CE3 interface, the demultiplexed E1 channels and the serial interfaces formed through binding operation. The enabling/disabling operation done on the E1 interface takes effect on E1 interface and the serial interfaces formed through binding operation. After executing the **shutdown** command on the specified CE3 interface, all the E1 channels and the serial interfaces formed by channel binding on the CE3 interface will be shut down, and data transmitting and receiving activities will stop. Executing the **undo shutdown** command, however, will re-enable all the E1 channels and the serial interfaces formed by channel binding operations.

CT3 Interface

Both T3 and T1 belong to the T-carrier system specified by ANSI, T3 is corresponding to the digital signal level DS-3, and the data transmission rate is 44.736Mbps.

CT3 interface has two operating modes: T3 mode (channelized mode) and CT3 mode (non-channelized mode).

- When working in T3 mode, the interface is equivalent to a fractional interface of data bandwidth 44736kbps.
- When working in CT3 mode, the interface can multiplex/demultiplex 28 channels of T1 signals. Each T1 interface can be divided into 24 time slots numbered in the range of 1 to 24. These time slots can be randomly bound into N x 64Kbps or N x 56Kbps logical channels.

CT3 interface supports the link layer protocols PPP, HDLC, Frame Relay, LAPB and X.25, and the network protocols such as IP and IPX.

Configure CT3 Interface

CT3 interface configuration includes:

- Enter the view of the specified CT3 interface
- Set clock mode
- Set cable length
- Set loopback mode
- Set frame format
- Set operating mode of CT3 interface

- Set CRC of the Serial Interface

Depending on the networking requirements, the user perhaps needs to configure the parameters such as PPP, Frame Relay and IP address for the CT3 interface. For details, refer to the involving chapters.

1 Enter the view of the specified CT3 interface

CT interface uses the **controller** command to enter its view.

Perform the following configuration in system view.

Table 174 Enter specified CT3 interface view

Operation	Command
Enter specified CT3 Interface view	controller t3 interface-number

2 Set Clock Mode

CT3 Interface supports two clock modes:

- Master clock mode: to use internal clock signal
- Slave clock mode: to use line clock signal

Perform the following configuration in CT3 Interface view.

Table 175 Set clock mode of the CT3 interface

Operation	Command
Set clock mode of the CT3 interface	clock { master slave }
Restore the default clock mode of CT3 interface	undo clock

By default, CT3 interface uses slave clock.

The user can also set clock mode for T1 channels of CT3 interface.

Table 176 Set clock mode of the T1 channel

Operation	Command
Set clock mode of the T1 channel	t1 line-number set clock { master slave }
Restore the default clock mode of T1 channel	undo t1 line-number set clock

By default, T1 channel uses **slave** clock.

3 Set Cable Length

Use the **cable** command to set the distance between the router and the cable distribution frame.

Perform the following configuration in CT3 interface view.

Table 177 Set cable length of the CT3 interface

Operation	Command
Set cable length of the CT3 interface	cable feet
Restore the default cable length	undo cable

By default, the cable length of the CT3 interface is set to 350 feet.

4 Set Loopback Mode

The CT3 interface supports loopback test on data at the rate of DS-3. Do not enable the loopback function in normal operation.

Perform the following configuration in CT3 interface view.

Table 178 Set loopback mode of the CT3 interface

Operation	Command
Set loopback mode of CT3 interface	loopback { local payload remote }
Disable loopback on the CT3 interface	undo loopback

Difference between two types of external loopback of the CT3 interface: Frame header overhead should be processed for external payload loopback (**payload**) while frame is not processed for external remote loopback (**remote**).

By default, loopback is disabled.

Single-channel loopback can be set on the T1 channels on a CT3 interface, and the settings of individual channels are independent.

Table 179 Set loopback mode of T1 channel

Operation	Command
Set loopback mode of T1 channel	t1 line-number set loopback { local remote }
Disable loopback on the T1 channel	undo t1 line-number set loopback

By default, loopback is disabled.

5 Set Frame Format

Two frame formats are used on CT3 interface: M23 and C-bit.

Perform the following configuration in CT3 interface view.

Table 180 Set frame format of the CT3 interface

Operation	Command
Set CT3 frame format	frame-format { c-bit m23 }
Restore the default setting	undo frame-format

By default, the CT3 interface uses the C-bit frame format.

When CT3 interface work in CT3 mode, single-channel frame format can be set on the T1 channels, and the settings of individual channels are independent.

Perform the following configurations in CT3 interface view.

Table 181 Set the frame format of T1 channel

Operation	Command
Set the frame format of T1 channel	frame-format { sf esf }
Restore the frame format of T1 channel to the default value	undo frame-format

By default, the frame format of T1 channel is ESF.

6 Configure Operate Mode of CT3 Interface

When setting the operating mode of a CT3 interface, you should set the operating modes of both the CT3 interface and the T1 channels on the interface.

Perform the following configuration in CT3 interface view.

Table 182 Set the operating mode of CT3 interface

Operation	Command
Configure Operate Mode of CT3 Interface	using { t3 ct3 }
Restore Operate Mode of CT3 Interface to default	undo using

By default, CT3 mode is used.

When CT3 interface works in T3 mode, the system will automatically create a serial interface whose number is **serial number/0:0** and whose rate is 44.736Mbps. The interface has the same logic feature as that of a synchronous serial interface; therefore, it can be regarded as a synchronous serial interface for further configuration.

Table 183 Set the operating mode of T1 channel

Operation	Command
Configure T1 channels of CT3 interface to work in T1 mode (unframed mode)	t1 line-number unframed
Configure T1 channels of CT3 interface to work in CT1 mode (framed mode)	undo t1 line-number unframed
Implement time slot binding on the CT1 interface	t1 line-number channel-set set-number timeslot-list range [speed { 56 64 }]
Disable time slot binding on the CT1 interface	undo t1 line-number channel-set set-number

The operation mode of T1 channels defaults to CT1 mode.

When T1 channel works in T1 mode (unframed mode), the system will automatically create a serial interface whose number is **serial number / line-number:0** and whose rate is 1544kbps. The interface has the same logic feature as that of a synchronous serial interface; therefore, it can be regarded as a synchronous serial interface for further configuration.

When T1 channel works in CT1 mode (framed mode), timeslot binding can be performed on it. The system will automatically create a serial interface whose number is **serial number / line-number: set-number** and whose rate is N x 64 kbps or N x 56 kbps. The interface has the same logic feature as that of a synchronous serial interface; therefore, it can be regarded as a synchronous serial interface for further configuration.

7 Set CRC of the Serial Interface

For the serial interface formed by T3, the one formed by T1 channel or the one bundled by T1 channel timeslots, its CRC can be configured in the corresponding serial interface view.

Table 184 Set CRC of the serial interface

Operation	Command
Set CRC of the Serial Interface	crc { 16 32 none }
Restore CRC of the Serial Interface to default value	undo crc

By default, the serial interface uses 16-bit CRC.

Display and Debug CT3 Interface

The display and debug operations of CT3 interface include disabling interface and displaying interface information. But you should be careful when using the **shutdown** command, because disabling an interface will cause the interface to stop working.

Perform the following configuration in CT3 interface view.

Table 185 Disable and Enable CT3 interface

Operation	Command
Disable CT3 Interface	shutdown
Enable CT3 Interface	undo shutdown
Disable T1 channel	t1 t1-number shutdown
Enable T1 channel	undo t1 t1-number shutdown

The enabling/disabling operation done on the CT3 interface takes effect on CT3 interface, the T1 channels and the serial interfaces formed through binding operation. The enabling/disabling operation done on the T1 interface takes effect on T1 interface and the serial interfaces formed through binding operation.

To disable/enable only the serial interface formed by T3, the serial interface formed by T1 channel or the serial interface formed by timeslot bundle of T1 channel, user can use command **shutdown/undo shutdown** in Serial interface view.

Perform the following configuration in all views.

Table 186 Display and debug of the CT3 interface

Operation	Command
Display the T3/CT3 Controller state and states of all channels	display controller t3 [interface-number]
Display the configuration and state information of the serial interface formed by the T3/CT3 interface	display interface serial interface-number

11

CONFIGURING LOGICAL INTERFACE

This chapter contains information on the following topics:

- Logical Interface Introduction
- Dialer Interface
- Loopback Interface
- Null Interface
- Sub-Interface
- Standby Center Logic Channel
- Virtual-Template and Virtual Interface

Logical Interface Introduction

The logical interface refers to the interface that can exchange data, but does not exist physically and needs to be established through configuration, including the Dialer interface, loopback interface, null interface, sub-interface, standby center logic channel and virtual-template.

Dialer Interface

Dialer interface is used for dialup. Dial-supporting interfaces on the 3Com Router series include synchronous serial interface, asynchronous serial interface, ISDN BRI interface and ISDN PRI interface. The 3Com Router realizes the Bandwidth on Demand Routing (BDR) function, and provides two BDR configuration methods: Legacy BDR and BDR profiles. Please see *Operation Manual - Dial-up* for detailed information.

Configure Dialer Interface

According to different BDR modes, configurations of Dialer interface are:

- Configure Dialer interface for Legacy BDR
- Configure Dialer interface for BDR profiles

Please see related chapters in *Operation Manual - Dial-up* for detailed description, monitoring and maintenance, typical configuration example, fault diagnosis and troubleshooting of the configurations of BDR.

Loopback Interface

It is prescribed in TCP/IP that the network segment 127.0.0.0 is loopback address. The interface with the loopback address is called loopback interface. The 3Com Router series define interface Loopback0 as the loopback interface, which can receive all the packets destined for this router. The addresses on the loopback interfaces can neither be configured nor be advertised by routing protocols.

Some applications (such as configuring local peer of SNA) requires that a local interface with specified IP address should be configured without affecting physical interface configuration. Furthermore, this address should have a 32-bit mask to reduce the use of IP addresses and it should be advertised by the routing protocols. Therefore, the loopback interface is added to meet this requirement.

Configure Loopback Interface

Loopback interface configuration includes:

- Create the loopback interface
- Configure operating parameters of the interface

1 Create loopback interface

Table 187 Create/delete loopback interface

Operation	Command
Create the loopback interface and enter loopback interface view	interface loopback number
Delete the specified loopback interface	undo interface loopback number

2 Configure operating parameters on the interface

The parameters such as IP address and IP routing can be configured on loopback interface. For detailed configuration, refer to *Operation Manual – Network Protocol*.



The 32-bit mask can be configured for the loopback interface, that is, the mask can be 255.255.255.255. The IP address with this 32-bit mask can be advertised by the routing protocols.

When configuring the ip address of loopback interface, it is recommended to configure the 32bit mask to save the ip address.

Null Interface

The 3Com Router support Null interface. Null interface is always in UP status, but cannot forward data packet or configure IP address or encapsulate other protocols.

Null interface is a virtual interface. Any network data packet sent to this interface will be dropped.

Configure Null Interface

Null interface configuration includes:

- Create the Null interface
- Configure operating parameters of the interface

1 Create the Null interface

Only one interface Null 0 can be created on the 3Com Router. Please perform the following configurations in all views.

Table 188 Create/Delete Null interface:

Operation	Command
Create the Null interface and enter Null interface view	interface null 0
Delete the Null interface	undo interface null 0

Any packet reaching the null interface will be dropped, which provides another method for packet filtering: Just sending unnecessary network traffic to Null0 interface, so that there is no need to configure ACL.

For example: Use static routing configuration command `ip route-static 192.101.0.0 255.255.0.0 null 0` will drop all the packets sent to network segment 192.101.0.0.

2 Configure operating parameters of the interface

`ip unreachable` is the only command which can be configured on the Null interface. It indicates that the router will reply the ICMP unreachable packet when it receives packets sent to the Null interface.

Please perform the following configurations in Null interface view.

Table 189 Configure/Remove the sending of ICMP unreachable packet

Operation	Command
Configure the sending of ICMP unreachable packet	<code>ip unreachable</code>
Remove the sending of ICMP unreachable packet	<code>undo ip unreachable</code>

Sub-Interface

The 3Com Router comes up with the concept of "sub-interface" and allows users to configure multiple sub-interfaces on one physical interfaces on the 3Com Router series, making it very flexible for configuration.

Sub-interfaces refer to the multiple logical virtual interfaces configured on one physical interface. These virtual interfaces share the physical layer parameters of the physical interface, meanwhile, they can be configured with their own link layer parameters and network layer parameters. Therefore, the multiple virtual interfaces corresponding to one physical are called "sub-interfaces".

- In the 3Com Router series, the physical interfaces supporting sub-interface features include:
- Ethernet interface: When the sub-interface of Ethernet has not been configured with VLAN id, the sub-interface can only support IPX network protocol. After configured with VLAN id, it will be able to support both IPX and IP protocols.
- WAN interface which link layer protocol is frame relay: Its sub-interface can support IP and IPX network protocols.

WAN interface which link layer protocol is X.25: Its sub-interface can support IP and IPX network protocols.

Configure Sub-Interface

According to different physical interfaces, sub-interface configuration includes:

- Configure sub-interfaces of Ethernet interface
- Configure sub-interfaces of WAN interface which link layer protocol is frame relay
- Configure sub-interfaces of WAN interface which link layer protocol is X.25

Configure sub-interfaces of Ethernet interface

1 Create and delete Ethernet sub-interfaces

Please use the following commands in all views.

Table 190 Create and delete Ethernet interface

Operation	Command
Create Ethernet sub-interface and enter its view	interface ethernet number.sub-number
Delete the specified Ethernet sub-interface	undo interface ethernet number.sub-number

When using the above commands, if corresponding Ethernet sub-interface has been created (the same as *sub-number*), enter the view of this sub-interface directly. Otherwise, first create Ethernet sub-interface with *sub-number* as the specified one, and then enter the view of this sub-interface.

2 Configure relevant working parameters

If the sub-interface of Ethernet has not been configured with VLAN id, it can only support IPX network protocol. Therefore, only IPX network address and other IPX working parameters can be configured on this sub-interface. After configured with VLAN id, the sub-interface of Ethernet can support IP and IPX. The detailed configuration procedure and method are similar to those of the Ethernet interface. Please refer to Chapter 9 "Configuring LAN Interface" and Chapter 20 "Configuring IP Address".

Configure sub-interfaces of WAN interface which link layer protocol is frame relay

1 Create and delete WAN sub-interfaces

Please use the following commands in all views.

Table 191 Create and delete WAN sub-interface

Operation	Command
Create WAN sub-interface and enter its view	interface serial number.sub-number [multipoint point-to-point]
Delete specified WAN sub-interface	undo interface serial number.sub-number [multipoint point-to-point]

When using the above commands, if corresponding WAN sub-interface has been created (the same as *sub-number*), enter the view of this sub-interface directly. Otherwise, first create WAN sub-interface with *sub-number* as the specified one, and then enter the view of this sub-interface.

2 Configure relevant working parameters

The following items can be configured on the sub-interface of WAN interface which link layer protocol is frame relay:

- Frame relay address mapping which is different from the affiliated WAN interface (i.e. the main interface)
- IP address which is not in the same network segment as the affiliated WAN interface

- IPX network number which is different from that of the affiliated WAN interface, and other IPX working parameters
- Virtual circuit of the sub-interface

Please see chapters in *Operation Manual - Link Layer Protocol* and *Operation Manual - Network Protocol* for details about the above configurations.

Configure sub-interfaces of WAN interface which link layer protocol is X.25

1 Create and delete WAN sub-interfaces

The command is the same as above.

2 Configure relevant working parameters

The following items can be configured on the sub-interface of WAN interface which link layer protocol is X.25:

- X.25 address mapping different from the affiliated WAN interface (i.e. the main interface)
- IP address which is not in the same network segment as the affiliated WAN interface
- IPX network number which is different from that of the affiliated WAN interface, and other IPX working parameters
- Virtual circuit of the sub-interface

Please see chapters in the *Operation Manual - Link Layer Protocol* and *Operation Manual - Network Protocol* for details about the above configurations, and sub-interface monitoring and maintenance. No further details are provided here.

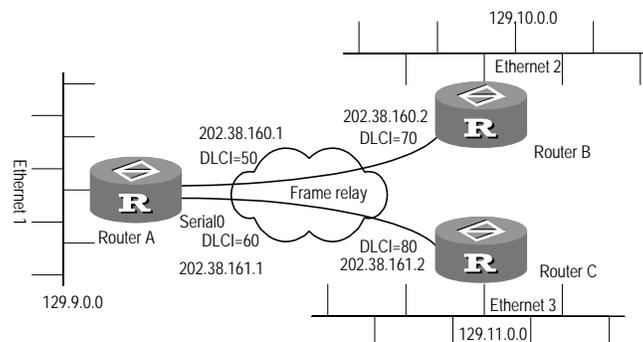
Typical WAN sub-interface configuration example

I. Networking Requirements

As shown below, WAN interface Serial0 of router A is connected with router B and router C via public frame relay network. By configuring sub-interfaces on Serial0 of router A, LAN 1 can simultaneously access LAN 2 and LAN 3 via Serial0.

II. Networking Diagram

Figure 48 Networking diagram of WAN sub-interface configuration example



III. Configuration Procedure

1 Enter the view of WAN interface Serial0 of router A

```
[Router] interface serial 0
```

2 Select frame relay link layer protocol

- ```
[Router-Serial0]link-protocol fr
```
- 3 Specify DTE as its frame relay terminal type
 

```
[Router-Serial0] fr interface-type dte
```
  - 4 Create sub-interface Serial 0.1 on WAN interface Serial0 of router A in point-to point mode, and enter its view
 

```
[Router]interface serial 0.1 point-to-point
```
  - 5 Set its IP address to 202.38.160.1 and address mask to 255.255.255.0.
 

```
[Router-Serial0.1] ip address 202.38.160.1 255.255.255.0
```
  - 6 Allocate a virtual circuit with DLCI 50 to it.
 

```
[Router-Serial0.1] fr dlci 50
```
  - 7 Create sub-interface Serial 0.2 on WAN interface Serial0 of router A in point-to point mode, and enter its view
 

```
[Router]interface serial 0.2 point-to-point
```
  - 8 Set its IP address to 202.38.161.1 and address mask to 255.255.255.0.
 

```
[Router-Serial0.2] ip address 202.38.161.1 255.255.255.0
```
  - 9 Allocate a virtual circuit with DLCI 60 to it.
 

```
[Router-Serial0.2] fr dlci 60
```
  - 10 Configure the static route from router A to LAN2 and LAN3.
 

```
[Router] ip route-static 129.10.0.0 255.255.0.0 202.38.160.2
[Router] ip route-static 129.11.0.0 255.255.0.0 202.38.161.2
```

Configurations of router B and router C are omitted here. For fault diagnosis and troubleshooting of sub-interface, please see chapters in *Operation Manual - Link Layer Protocol* and *Operation Manual - Network Protocol* in this manual.

---

## Standby Center Logic Channel

The standby center not only provides mutual backup between respective interfaces, but also chooses a certain virtual circuit belonging to X.25 or frame relay as the main interface or standby interface of the standby center. Please see relevant chapters in *Operation Manual – Reliability* for details about the standby center.

To facilitate configuration, the user can specify relevant logic channel for the above-mentioned virtual circuit and configure working parameters of the standby center in the logic channel.

### Configure Standby Center Logic Channel

For detailed description, monitoring and maintenance, typical configuration example, fault diagnosis and troubleshooting oriented to the configurations of the standby center logic channel, please see *Operation Manual – Reliability*.

---

## Virtual-Template and Virtual Interface

Virtual-template as the name implies, is a template used to configure a virtual interface, mainly used in VPN and MP.

After setting up the connection of VPN session, it is necessary to create a virtual interface to exchange data with the opposite end. At this times configuration and

dynamically create a virtual interface based on the configuration parameters of the template.

Similarly, after multiple PPP links are bound as MP, a virtual interface also needs to be created to exchange data with the opposite end. At this time, select an interface template to dynamically create a virtual interface.

## Configure Virtual-Template

In VPN and MP application environments, the system automatically creates and deletes virtual interface, which is completely transparent to the user. The user only needs to configure VPN or MP at corresponding physical interface, create and configure virtual-template and then build up relation between the virtual-template and relevant physical interface.

Virtual-template configuration includes:

- Create and delete virtual-template
- Set working parameters of the virtual-template
- Build up corresponding relation between the virtual-template and relevant physical interface.

### 1 Create and delete virtual-template

Please use the following commands in all views.

**Table 192** Create or delete virtual-template

| Operation                                  | Command                                       |
|--------------------------------------------|-----------------------------------------------|
| Create virtual-template and enter its view | <b>interface virtual-template number</b>      |
| Delete the virtual-template                | <b>undo interface virtual-template number</b> |

Here, *number* stands for template number of virtual-template ranging 1 to 25, i.e. the user can create up to 25 virtual-templates.

In executing **interface virtual-template** command, if corresponding virtual-template has been created, then directly enter the view of this virtual-template. Otherwise, first create the virtual-template with specified template number.

In deleting the virtual-template, make sure that all of its derived virtual interfaces have been removed and this virtual-template is not in use any more.

### 2 Set work parameters of virtual-template

Compared with normal physical interface, the virtual-template has the following features: the link layer protocol only supports PPP, and the network protocol supports IP and IPX. Therefore, the following working parameters can be set:

- Set working parameters of PPP
- Set IP address of virtual interface
- Set IP address (or IP address pool) allocated to PPP opposite end

Settings of these parameters on virtual-template are the same as those on normal interface. Please see related chapters of PPP configuration in *Operation Manual – Link Layer Protocol*, IP address configuration in *Operation Manual – Network Protocol* and RADIUS configuration in *Operation Manual – Security* for configuration details.

- 3 Create corresponding relation between the virtual-template and related physical interface

In VPN application environment, it is necessary to build up corresponding relations between L2TP group and virtual-template. In MP application environment, it is necessary to build up corresponding relations between MP and virtual-template.

Please see chapters in *Operation Manual – VPN* and *Operation Manual – Link Layer Protocol* for detailed description.

### Display and Debug Virtual-Template and Virtual Interface

The virtual interface, automatically created by the system if necessary, will work by using parameters of related virtual-template. So, it's unnecessary for manual configuration. The virtual interface will be deleted because of low-layer link disconnection or user intervention.

The following command can be used to display the state of virtual-template in all views.

**Table 193** Display state of the specified virtual-template

| Operation                                           | Command                                                                    |
|-----------------------------------------------------|----------------------------------------------------------------------------|
| Display the state of the specified virtual-template | <b>display interfaces<br/>virtual-template<br/>virtual-template-number</b> |

### Troubleshooting

Before checking and eliminating faults of virtual-template, first find out the virtual-template is used to create VPN virtual access interface or MP virtual interface, then locate the fault of the virtual-template in actual application environment.

#### Fault 1: Fail to create virtual interface.

Troubleshooting: the reasons may be as follows:

- The virtual-template is not configured with IP address. Therefore, PPP consultation fails and the virtual interface can't turn to Up state.
- The virtual-template is not configured with IP address (or IP address pool) allocated to the opposite end. If it is required to allocate addresses to the opposite end in actual application, the virtual interface cannot meet the requirement, nor turn to Up state.
- PPP authentication parameter is set incorrectly. If the opposite end is not the user defined by the router, PPP consultation will also fail.

Please see related chapters of *Operation Manual – VPN* and *Operation Manual – Link Layer Protocol* for more methods of fault diagnosis and troubleshooting of virtual-template.

# IV

## LINK LAYER PROTOCOL

- Chapter 12    Configuring PPP and MP
- Chapter 13    Configuring PPPoE Client
- Chapter 14    Configuring SLIP
- Chapter 15    Configuring ISDN Protocol
- Chapter 16    Configuring LAPB and X.25
- Chapter 17    Configuring Frame Relay
- Chapter 18    Configuring HDLC
- Chapter 19    Configuring Bridge



# 12

## CONFIGURING PPP AND MP

This chapter contains information on the following topics:

- PPP Overview
- MP Overview
- Configure PPP
- Configure MP
- Display and Debug PPP
- Typical PPP Configuration Example
- Typical MP Configuration Example
- Fault Diagnosis and Troubleshooting of PPP

---

### PPP Overview

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagram over point-to-point links. It gains wide applications since it can provide user authentication, support synchronous/asynchronous lines and can be expanded easily.

PPP defines a whole set of protocols, including link control protocol (LCP), network control protocol (NCP) and authentication protocols (PAP and CHAP). Of them:

- Link Control Protocol is used to negotiate some parameters of the link and is responsible for creating and maintaining the link.
- Network Control Protocol is used to negotiate the parameters of network layer protocol.

### PPP Authentication Mode

#### 1 PAP authentication

PAP (Password Authentication Protocol) is a 2-way handshake authentication protocol and it transmits username and password in plain text over the Internet. The process of PAP authentication is as follows:

The requester repeatedly sends its username/password combination across the link until the authenticator responds with an acknowledgment or until the link is broken. The authenticator may disconnect the link if it determines that the username/password combination is not valid.

#### 2 CHAP authentication

CHAP (Challenge-Handshake Authentication Protocol) is a 3-way handshake authentication protocol. It only sends the username but not the password across the link. The process of CHAP is as follows:

The authenticator sends some randomly generated packets to the requester (challenge), and at the same time it sends its configured username to the requester.

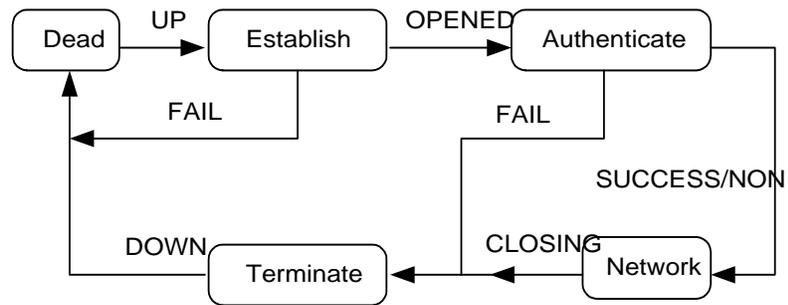
When the requester receives the challenge, it will look for the user password according to the authenticator's username and its own user list. If it finds the user in the user list with the same name as the authenticator's username, the requester builds the response with its own password, serial number of packet using MD5 algorithm, and sends the generated response and its configured username to the authenticator (response).

After receiving the response from the requester, the authenticator does the same encryption as the requester with the saved password, serial number of packet using MD5 algorithm. Then it compares the encryption result with the response from requester, and returns the response according to the comparison result (Acknowledge or Not Acknowledge).

### 3 Phases of PPP negotiation:

- a When the physical layer is unavailable, the link is in Dead phase. A link shall start from the Dead phase. When the physical layer becomes available, PPP link enters the Establish phase.
- b In **Establish** phase, PPP link carries out LCP negotiation, including negotiation of working mode (SP or MP), authentication mode and maximum transmission unit etc. After the successful LCP negotiation, the status of LCP is **Open**, indicating that the link has been established.
- c If the authentication is not configured, it begins NCP negotiation. At this time, the status of LCP is still **Open**, while the status of NCP is changed from **Initial** to **Request-sent**.
- d If the authentication is configured (the remote verifies the local or the local verifies the remote), it enters **Authenticate** phase to start CHAP or PAP authentication. If the authentication fails, it enters **Terminate** phase, the link is removed and LCP turns down. After successful authentication, the NCP negotiation begins. At this time, the status of LCP is still **Open**, while the status of NCP is changed from Initial to **Request-sent**.
- e NCP negotiation supports the negotiations of IPCP and IPXCP, of which IPCP negotiation mainly includes the IP addresses of two partners. One or more network layer protocols is selected and configured through NCP negotiation. The selected network layer protocol must be configured successfully before this network layer protocol sends packets through this link.
- f PPP link will remain in communication status until a specific LCP or NCP frame closes this link or some external events take place (for example, the intervention of user).

Phases of PPP negotiation are shown in the following diagram.

**Figure 49** Diagram of PPP negotiation phases

For detailed description of PPP, refer to RFC1661.

---

## MP Overview

MP protocol (PPP Multilink protocol) can bind multiple PPP links, so as to increase bandwidth. MP protocol can fragment large packets, and then the fragmentation will be sent to the same destination through different PPP links, so as to decrease the transmission time of large packets.

The negotiation process in MP mode is as follows (e.g: establishing MP in the virtual interface template):

- 1 Detect whether the interface of the peer works in MP mode. First begin LCP negotiation with the peer, negotiating about ordinary LCP parameters and verify whether the interface of the peer works in MP mode. If the peer does not work in MP mode, begin NCP negotiation and do not bundle MP.
- 2 Bind the interface to virtual template interface. This can be done in the following two ways: Bind directly and bind according to username or endpoint. In the former way, the router does not detect the username and endpoint, and binds the interface to a specified virtual template interface. In the latter way, the router binds the interface to the virtual template interface according to the username or endpoint.
- 3 Perform NCP negotiation. After the interface is bound to a virtual template, the router will begin NCP negotiation with the NCP parameters for this virtual template (such as IP address). The NCP parameters configured at the physical interface are not functional. If NCP negotiation is successful, MP link can be established, to transport data with wider bandwidth.

---

## Configure PPP

PPP configuration includes:

- Configure the link layer protocol of the interface to PPP
  - Configure PPP authentication
  - Configure AAA authentication and accounting parameter of PPP
  - Configure PPP negotiation parameter
  - Configure PPP compression
  - Configure PPP link quality monitoring
- 1 Configure the Link Layer Protocol of the Interface to PPP  
Perform the following configuration in the interface view.

**Table 194** Configure the link layer protocol of the interface to PPP

| Operation                                                 | Command                  |
|-----------------------------------------------------------|--------------------------|
| Configure the link layer protocol of the interface to PPP | <b>link-protocol ppp</b> |

The default link layer protocol of the interface is PPP.

## 2 Configure PPP Authentication

PPP has two authentication modes: PAP mode and CHAP mode. CHAP authentication is more secure.

- Configure PAP authentication

- a Configure the authenticator of PAP authentication

Perform the following configuration in the interface view, and use the **user** command in the system view.

**Table 195** Configure the local authenticates the peer in PAP mode

| Operation                                                          | Command                                                                        |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Enable PAP authentication                                          | <b>ppp authentication-mode pap [ callin ] [scheme { default   name-list }]</b> |
| Disable PPP authentication                                         | <b>undo ppp authentication-mode</b>                                            |
| Add the username and password of the peer into the local user list | <b>local-user user password { simple   cipher } password service-type ppp</b>  |

- b Configure the requester of PAP authentication

Perform the following configuration in the interface view.

**Table 196** Configure the peer authenticates the local in PAP mode

| Operation                                                                                | Command                                                                  |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Configure PAP username and password when the peer authenticates the local in PAP mode    | <b>ppp pap local-user username password { simple   cipher } password</b> |
| Delete the above configured username and password sent during authentication in PAP mode | <b>undo ppp pap local-user</b>                                           |

While configuring PAP authentication, note following:

- If one side originates the PAP, authenticator should add username and password for the requester in the local database (use **local-user** command). The requester should send its username and password to the authenticator (use **ppp pap local-user** command).
- If one side originates the PAP, authenticator only needs to start PAP authentication itself (use **ppp authentication-mode pap** command). The requester does not need to configure the command.
- If both sides originate PAP simultaneously, then each side is both authenticator and requester. At this time, both sides need to configure all the commands supporting the PAP authentication.
- Configure CHAP authentication
  - a Configure the authenticator of CHAP authentication

Perform the following configuration in the interface view, and use the **local-user** command in the system view.

**Table 197** Configure the local authenticates the peer in CHAP mode

| Operation                                                          | Command                                                                           |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Enable CHAP authentication                                         | <b>ppp authentication-mode chap [ call-in ] [ scheme { default   name-list }]</b> |
| Disable CHAP authentication                                        | <b>undo ppp authentication-mode</b>                                               |
| Configure the name of the local                                    | <b>ppp chap user username</b>                                                     |
| Delete the configured name of the local                            | <b>undo ppp chap user</b>                                                         |
| Add the username and password of the peer into the local user list | <b>local-user user password { simple   cipher } password</b>                      |

**b** Configure the requester of CHAP authentication

Perform the following configuration in the interface view, and use the **local-user** command in the system view.

**Table 198** Configure as the peer authenticates the local in CHAP mode

| Operation                                                           | Command                                                      |
|---------------------------------------------------------------------|--------------------------------------------------------------|
| Configure the name of the local                                     | <b>ppp chap user username</b>                                |
| Delete the configured name of the local                             | <b>undo ppp chap user</b>                                    |
| Configure the password of the local for authentication in CHAP mode | <b>ppp chap password { simple   cipher } password</b>        |
| Delete the password of the local during authentication in CHAP mode | <b>undo ppp chap password</b>                                |
| Add the username and password of the peer into the local user list  | <b>local-user user password { simple   cipher } password</b> |

Generally, when the router configures user list, it configures the command **ppp chap user username** and **local-user user password { simple | cipher } password**, to perform CHAP authentication. While configuring CHAP authentication, *user* of one end is the *username* of the other, and the *password* must be the same.

In some situation, if the router cannot configure user list then it needs to configure the command **ppp chap password { simple | cipher } password** to perform CHAP authentication.

While configuring CHAP authentication, note the following:

- If one side originates the CHAP, authenticator should add username and password for the requester in the local database (use **local-user** command), and should send its username to the requester (use **ppp chap user** command). The requester should also add username and password for the authenticator in its database (use **local-user** command), and send its username and password to the authenticator (use **ppp chap user** command).
- If one side originates the CHAP, authenticator only needs to start CHAP authentication itself (use **ppp authentication-mode chap** command). The requester does not need to configure the command.
- If both sides originate CHAP simultaneously, then each side is both authenticator and requester. At this time, both sides need to configure all the commands supporting the CHAP authentication.

**3** Configure AAA Authentication and Accounting Parameter of PPP

Whether the PPP user passes the authentication will be finally decided by AAA, which can authenticate PPP user at local or at RADIUS server.

Local authentication is to authenticate the local user configured through the **local-user user password { simple | cipher } password** command, and RADIUS server authentication is to authenticate using the user database on RADIUS server. The specific configuration commands are shown in the following table.

**Table 199** Configure AAA authentication and accounting of PPP

| Operation                                                   | Command                                                                             |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Enable AAA                                                  | <b>aaa-enable</b>                                                                   |
| Configure PPP authentication method of AAA                  | <b>aaa authentication ppp { default   list-name } [ method1   method2   ..... ]</b> |
| Configure the local first authentication of AAA             | <b>aaa authentication local-first</b>                                               |
| Configure PPP authentication method of AAA at the interface | <b>ppp authentication-mode { chap   pap } [ default   list-name ]</b>               |

For PPP authentication method of AAA, refer to *Security*. If PPP authentication method of AAA is not specified on the interface, please use the **default** authentication method.

#### 4 Configure PPP Negotiation Parameter

The following PPP negotiation parameters can be configured:

- Time interval between negotiation timeout

During PPP negotiation, if the response packet of the peer is not received within this time interval, PPP will retransmit the packet. The default time interval of timeout is 10s, and the value range is 1~10s.

- Some negotiation parameters of NCP

For the configuration of local IP address and the IP address assigned to the peer, refer to *Network Protocol*. For example, if it is necessary for the remote end to allocate an IP address for the local end, you can use the **ip address ppp-negotiate** command, while the **remote address** command can be used to designate the local to assign IP address for the peer.

**Table 200** Configure the time interval of PPP negotiation timeout

| Operation                                                   | Command                            |
|-------------------------------------------------------------|------------------------------------|
| Configure the time interval of negotiation timeout          | <b>ppp timer negotiate seconds</b> |
| Restore the default of time interval of negotiation timeout | <b>undo ppp timer negotiate</b>    |

#### 5 Configure PPP Compression

The current the 3Com Router version supports the Stac compression method.

Perform the following task in the interface view.

**Table 201** Configure PPP compression

| Operation                                                | Command                              |
|----------------------------------------------------------|--------------------------------------|
| Configure as Stac compression permitted on the interface | <b>ppp compression stac-lzs</b>      |
| Cancel the Stac compression used by the interface        | <b>undo ppp compression stac-lzs</b> |



*In MP working mode, it is not recommended to use PPP compression. To configure PPP compression negotiation on the virtual interface, PPP compression must be configured on Virtual-template interface before the subordinate physical interface can accept the PPP compression negotiation.*

## 6 Configure PPP Link Quality Monitoring

PPP link quality monitoring can be a real time monitoring the PPP link quality (including PPP links bound to MP). When link quality is lower than the Disabled Quality Percentage, link will be disabled. When link quality restores to the Restoring Link Quality Percentage, link will be automatically resumed. To ensure that links do not repeatedly oscillate between disabled status and restored status, there will be certain time delay when PPP link quality monitoring resumes the link.

Perform the following configuration in interface view.

**Table 202** Configure PPP link quality monitoring

| Operation                                    | Command                                                             |
|----------------------------------------------|---------------------------------------------------------------------|
| Enable PPP link quality monitoring function  | <code>ppp lqc forbidden-percentage [ resumptive-percentage ]</code> |
| Disable PPP link quality monitoring function | <code>undo ppp lqc</code>                                           |

By default, the parameter resumptive-percentage is equal to forbidden-percentage.



*Before PPP link quality monitoring is enabled, PP interface sends keepalive packets every period. After the function is enabled, PPP interface will replace the keepalive packets by LQR packets, that is, PPP interface will send LQR packets every period, in order to monitor the link.*



*When link quality is normal, the system will calculate the link quality in each LQR packet. If the calculation results turn out to be unqualified for two consecutive times, the link will be disabled. After the link is disabled, the system will calculate the link quality in every ten LQR packets. The link will be resumed only if the calculation results of link quality are qualified for three consecutive times. Therefore, the link can only be resumed at least 30 keepalive periods after it is disabled. If the keepalive period is set too long, it may cause no resumption of links for a long time.*

## Configure MP

The following section describes the configuration tasks of MP application on virtual template. Please Refer to *Dial-up* to know about MP configuration under BDR mode (Including MP on the interfaces of ISDN BRI/PRI).

MP application on virtual template configuration includes:

- Create Virtual Template
- Configure Operating Parameters of Virtual Template
- Configure the Physical Interface to work in MP Mode
- Bind the Physical Interface to a Virtual Template

- Configure MP Protocol Parameters
- 1 Create Virtual Template

**Table 203** Create/Delete virtual template

| Operation                                          | Command                                           |
|----------------------------------------------------|---------------------------------------------------|
| Create and enter MP virtual template interface     | <b>interface virtual-template<br/>number</b>      |
| Delete the specified MP virtual template interface | <b>undo interface virtual-template<br/>number</b> |

- 2 Configure Operating Parameters of Virtual Template

Comparing virtual template interface with general physical interface, users can find that the link layer protocol supports only PPP and the network protocol supports IP and IPX. Therefore the following operating parameters can be set:

- Set operating parameters of PPP
- Set IP address of virtual interface
- Set IP address (or IP address pool) allocated to PPP peer
- Set packet filtering rule on virtual interface

There is no difference in configuring the parameters for virtual template and for general interface. See specific configuration in related sections such as PPP configuration of *Operation Manual - Link Layer Protocol*, IP address configuration of *Operation Manual - Network Protocol* and RADIUS configuration of *Operation Manual - Security*.

- 3 Configure the Physical Interface to work in MP Mode

Perform the following configuration in interface view.

**Table 204** Configure the physical interface to work in MP mode

| Operation                                                 | Command                  |
|-----------------------------------------------------------|--------------------------|
| Configure the link layer protocol of the interface to PPP | <b>link-protocol ppp</b> |
| Configure the interface to work in MP mode                | <b>ppp mp</b>            |
| Configure the interface to work in common mode            | <b>undo ppp mp</b>       |

By default, interface does not work in MP mode.

- 4 Bind the Physical Interface to a Virtual Template

The physical interface can be bound to a virtual template in two ways.

- Bind directly

Perform the following configuration in interface view.

**Table 205** Bind the physical Interface to a Virtual Template

| Operation                                                               | Command                                                           |
|-------------------------------------------------------------------------|-------------------------------------------------------------------|
| Bind the physical Interface to a Virtual Template                       | <b>ppp mp interface<br/>virtual-template<br/>interface-number</b> |
| Remove the physical interface's binding to a virtual template interface | <b>undo ppp mp interface</b>                                      |

After this command is configured, the system will not check the username and endpoint when performing MP binding, namely, the commands **ppp mp binding-mode** and **ppp mp user** will not take effect.

- Bind according to username or endpoint

Here the username refers to the received remote username when PPP link performs PAP or CHAP authentication. Endpoint is the unique mark of a router and refers to the received remote endpoint when performing LCP negotiation. The system can implement MP binding according to the received username or endpoint and bind the interfaces that have the same username or endpoint to the same virtual template interface.

- a Specify the conditions for MP binding

Perform the following configuration in the system view.

**Table 206** Specify the conditions for MP binding

| Operation                                                  | Command                                   |
|------------------------------------------------------------|-------------------------------------------|
| Perform MP binding according to username                   | <b>ppp mp binding-mode authentication</b> |
| Perform MP binding according to endpoint                   | <b>ppp mp binding-mode descriptor</b>     |
| Perform MP binding according to both username and endpoint | <b>ppp mp binding-mode both</b>           |
| Restore the default binding conditions                     | <b>undo ppp mp binding-mode</b>           |

By default, Performs MP binding according to both username and endpoint.

- Performs MP binding according to both username

First of all, two-way authentications (CHAP or PAP) need to be configured on the interface. See configuration procedure in basic PPP configuration tasks.

Associate the PPP username with the virtual template interface. The interface with the same username will be bound to the same virtual template interface.

**Table 207** Associate the PPP username with the virtual template interface

| Operation                                                       | Command                                                   |
|-----------------------------------------------------------------|-----------------------------------------------------------|
| Associate the PPP username with the virtual template interface  | <b>ppp mp user user-name bind virtual-template number</b> |
| Dissociate the PPP username with the virtual template interface | <b>undo ppp mp user user-name</b>                         |

- Bind according to endpoint

The endpoint is determined automatically when the router is started, and each router has its own endpoint. The interfaces with the same endpoint will be bound to the same virtual template interface.

The endpoint is generated by the router automatically, and the user cannot change the configuration.

## 5 Configure MP Protocol Parameters

- a Configure maximum number of links that MP channel permits to bind

**Table 208** Configure maximum number of links MP channel permits binding

| Operation                                                                   | Command                           |
|-----------------------------------------------------------------------------|-----------------------------------|
| Set maximum link number MP channel permits for binding                      | <b>ppp mp max-bind binds</b>      |
| Restore default value of maximum link number MP channel permits for binding | <b>Undo ppp mp max-bind binds</b> |

By default, the maximum link number of links that MP channel permits to bind is 16.

- b** Configure the maximum number of fragments received by MP channel

**Table 209** Configure the maximum number of fragments received by MP channel

| Operation                                                                              | Command                               |
|----------------------------------------------------------------------------------------|---------------------------------------|
| Set the number of maximum fragments MP channel permits to receive                      | <b>ppp mp max-receive-frags frags</b> |
| Restore default value of the number of maximum fragments MP channel permits to receive | <b>undo ppp mp max-receive-frags</b>  |

By default, the maximum number of fragments that MP channel permits to receive is 4.

- c** Configure the maximum number of fragments that MP channel permits to send

**Table 210** Configure the maximum number of fragments that MP channel permits to send

| Operation                                                                           | Command                            |
|-------------------------------------------------------------------------------------|------------------------------------|
| Set the number of maximum fragments MP channel permits to send                      | <b>ppp mp max-send-frags frags</b> |
| Restore default value of the number of maximum fragments MP channel permits to send | <b>undo ppp mp max-send-frags</b>  |

By default, the maximum number of fragments that MP channel permits to send is 1.

- d** Configure virtual Baud rate of the interface

In MP channels, system controls load balancing in different links according to Baud rate of interfaces. The higher the interface Baud rate, the larger the data flow it can carry.



*For synchronous serial interfaces operating in DTE mode, Baud rate is calculated in line with 64000 bps without exception.*

Generally, the actual sending capability is basically identical to its interface Baud rate. However, in some special cases, the difference between them is large. For example, when asynchronous serial interfaces of two routers are connected via Modems, the actual transmission speed is decided by the line quality, after the Modem negotiations. In this case, the speed is usually slower than the preset interface Baud rate. Moreover, for synchronous serial interfaces running under DTE mode, system cannot obtain their correct Baud rate.

In the above cases, you should set the virtual Baud rate on interfaces. When virtual Baud rate (must not be 0) is set on an interface, system will substitute virtual Baud rate for interface Baud rate to control flows. Proper application of virtual Baud rate can make full use of the total link bandwidth and reduce network delay time, while the irrational configuration runs the opposite.

Perform the following configuration in interface view.

**Table 211** Configure virtual Baud rate on interface

| Operation                          | Command                         |
|------------------------------------|---------------------------------|
| Set virtual Baud rate on interface | <b>virtualbaudrate baudrate</b> |

|                                                                |                                   |
|----------------------------------------------------------------|-----------------------------------|
| Disable applying the setting of virtual Baud rate on interface | <code>undo virtualbaudrate</code> |
|----------------------------------------------------------------|-----------------------------------|

By default, virtual Baud rate is not set on interface.

## Display and Debug PPP

Please use the **display** and **debugging** commands in all views.

**Table 212** Display and debug PPP

| Operation                         | Command                                                                 |
|-----------------------------------|-------------------------------------------------------------------------|
| Display Multilink PPP information | <code>display ppp mp [ interface type number ]</code>                   |
| Enable the debugging of PPP       | <code>debugging ppp { event   lqr   negotiation   packet   all }</code> |

## Typical PPP Configuration Example

### PAP Authentication Example

#### I. Configuration Requirement

As shown in Figure 50, Router1 and Router2 are interconnected through interface Serial0, and router Router1 (authenticator) is required to authenticate router Router2 (requester) in PAP mode.

#### II. Networking Diagram

**Figure 50** Networking diagram of PAP and CHAP authentication example



#### III. Configuration Procedure

##### 1 Configure Router1 (authenticator):

- a** Add a user with name Router2 and password hello to the local database

```
[Router]local-user Router2 password simple hello
```

- b** Configure to start PAP authentication at this side

```
[Router]interface serial 0
```

```
[Router-Serial0]ppp authentication-mode pap
```

##### 2 Configure Router 2 (requester):

- a** Configure this side to be authenticated by the opposite side with username Router2 and password hello

```
[Router]interface serial 0
```

```
[Router-Serial0]ppp pap local-user Router2 password simple hello
```

### CHAP Authentication Example

#### I. Configuration Requirement

In Figure 50, Router1 is required to authenticate Router2 in CHAP mode.

## II. Configuration Procedure

- 1 Configure Router1:
  - a Add a user with name Router2 and password hello to the local database
 

```
[Router]local-user Router2 password simple hello
```
  - b Set local username as Router1
 

```
[Router]interface serial 0
[Router-Serial0]ppp chap user Router1
```
  - c Configure to start CHAP authentication at this side
 

```
[Router-Serial0]ppp authentication-mode chap
```
- 2 Configure router Router2:
  - a Add a user with name Router1 and password hello to the local database
 

```
[Router]local-user Router1 password simple hello
```
  - b Set local username as Router2
 

```
[Router]interface serial 0
[Router-Serial0]ppp chap user Router2
```

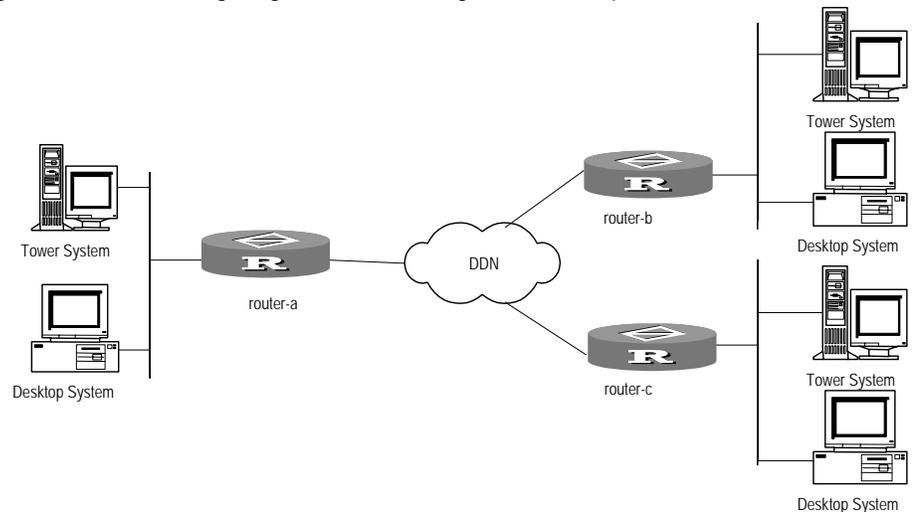
## Typical MP Configuration Example

### I. Configuration Requirement

In Figure 51, two B channels of E1 interface of router-a are bound to the B channel of router-b, and the other two B channels are bound to router-c. Suppose that four B channels on router-a are serial2:1, serial2:2, serial2:3 and serial2:4, the names of interfaces of two B channels on router-b are serial2:1 and serial2:2, and the names of interfaces of two B channels on router-c are serial2:1 and serial2:2.

### II. Networking Diagram

Figure 51 Networking diagram of MP configuration example



### III. Configuration Procedure

- 1 Configure router-a:
  - a Add a user for router-b and router-c respectively
 

```
[Router]local-user router-b password simple router-b
```

```
[Router]local-user router-c password simple router-c
```

- b** Specify the virtual interface templates for the two users and begin PPP negotiation for the NCP information using this template

```
[Router]ppp mp user router-b bind virtual-template 1
[Router]ppp mp user router-c bind virtual-template 2
```

- c** Configure virtual interface template

```
[Router]interface virtual-template 1
[Router-Virtual-Template1]ip address 202.38.166.1 255.255.255.0
[Router]interface virtual-template 2
[Router-Virtual-Template2]ip address 202.38.168.1 255.255.255.0
```

- d** Add the interfaces serial2:1, serial2:2, serial2:3 and serial2:4 into MP channel. Here, take serial2:1 as an example, and other interfaces are configured similarly.

```
[Router]interface serial 2:1
[Router-Serial2:1]link-protocol ppp
[Router-Serial2:1]ppp mp
[Router-Serial2:1]ppp authentication-mode pap
[Router-Serial2:1]ppp pap local-user router-a password simple
router-a
```

## 2 Configure router-b:

- a** Add a user for router-a

```
[Router]local-user router-a password simple router-a
```

- b** Specify the virtual interface template for this user and begin PPP negotiation for the NCP information using this template

```
[Router]ppp mp user router-a bind virtual-template 1
```

- c** Configure working parameters of the virtual interface template

```
[Router]interface virtual-template 1
[Router-Virtual-Template1]ip address 202.38.166.2 255.255.255.0
```

- d** Add the interfaces serial2:1 and serial2:2 into MP channel. Here, take serial2:1 as an example, and configure other interfaces similarly

```
[Router]interface serial2: 1
[Router-Serial2:1]ppp mp
[Router-Serial2:1]ppp authentication-mode pap
[Router-Serial2:1]ppp pap local-user router-b password simple
router-b
```

## 3 Configure router-c:

- a** Add a user for router-a

```
[Router]local-user router-a password simple router-a
```

- b** Specify the virtual interface template for this user and begin PPP negotiation for the NCP information using this template

```
[Router]ppp mp user router-a bind virtual-template 1
```

- c** Configure working parameters of the virtual interface template

```
[Router]interface virtual-template 1
[Router-Virtual-Template1]ip address 202.38.168.2 255.255. 255.0
```

- d** Add the interfaces serial2:1 and serial2:2 into MP channel. Here, take serial2: 1 as an example, and other interfaces are configured similarly.

```
[Router]interface serial2: 1
[Router-Serial2:1]ppp mp
[Router-Serial2:1]ppp authentication-mode pap
[Router-Serial2:1]ppp pap local-user router-c password simple
router-c
```

## Fault Diagnosis and Troubleshooting of PPP

### Fault 1: Link always fails to turn to up status.

Troubleshooting: It is possible that PPP authentication parameter is not configured correctly, resulting in the failure of PPP authentication.

Turn on the debugging switch of PPP, if LCP negotiation is successful and turns to Up status, then begin PAP or CHAP negotiation and LCP turns to Down status.

### Fault 2: Physical link fails to turn to Up status.

Troubleshooting: Execute `display interface serial interface-number` command to view the current interface status, including five status:

`serial number is administratively down, line protocol is down`

Indicates that the interface is shutdown.

`serial number is down, line protocol is down`

Indicates that the interface is not activated or the physical layer does not turn to Up status.

`serial number is up, line protocol is up(spoofing)`

Indicates that this interface is a dialup interface and the call is not connected successfully.

`serial number is up, line protocol is up`

Indicates that data can be transmitted through this interface.

`serial number is up, line protocol is down`

Indicates that this interface is activated, but link negotiation is not successful.

### Fault 3: Fail to ping through the peer although the link is UP and LCP and IPCP are all opened.

Troubleshooting:

- Execute the `display running-configcurrent-configuration interface` command on the local end to check whether the IP address is configured and whether IP address negotiation is configured with the `ip address ppp-negotiate` command.
- Check the configuration of the peer to see whether it assigns IP address to the local end with the `remote address` command.
- Directly specify IP address for the local end or assign IP address to the peer. Then reset the interface with the `shutdown` and `undo shutdown` command.

# 13

## CONFIGURING PPPoE CLIENT

This chapter contains information on the following topics:

- PPOE Overview
- Configure PPPoE Client
- Display and Debug PPPoE Client
- Typical PPPoE Configuration Example

---

### PPoE Overview

Point-to-Point Protocol over Ethernet (PPPoE) can be used for connecting Ethernet hosts to a remote access concentrator through a simple bridging device. With PPPoE, the remote access device can control and implement billing on the accessed subscribers. Compared with traditional access approaches, PPPoE is more cost-effective. Therefore, it is widely put in many applications, such as residential quarter networks. As a popular broadband access approach at present, ADSL (Asymmetric Digital Subscriber Line), adopts this protocol.

PPPoE adopts the client/server approach, encapsulates PPP packets in Ethernet frames, and provides PPP connection over Ethernet.

PPPoE is implemented at two phases, the discovery phase and the PPP session phase.

- Discovery phase

When a host initiates a PPP session, it must first go through the discovery phase to confirm the remote Ethernet MAC address, and establish a PPPoE session ID. Different from PPP, PPPoE establishes a client/server relationship at this phase, whereas PPP establishes a peer relationship. Through the discovery phase, the host (client) can discover an access concentrator (server). After this phase ends normally, the host and the access concentrator can establish a PPPoE session by using the MAC address and the session ID.

- PPP session phase

As the PPP session begins, the host and the access concentrator implement negotiation and transmit PPP data according to PPP. The PPP packets are encapsulated in Ethernet frames as payload of PPPoE frames, and transmitted to the peers of the PPPoE link. In this case, all the Ethernet frames are unicast.

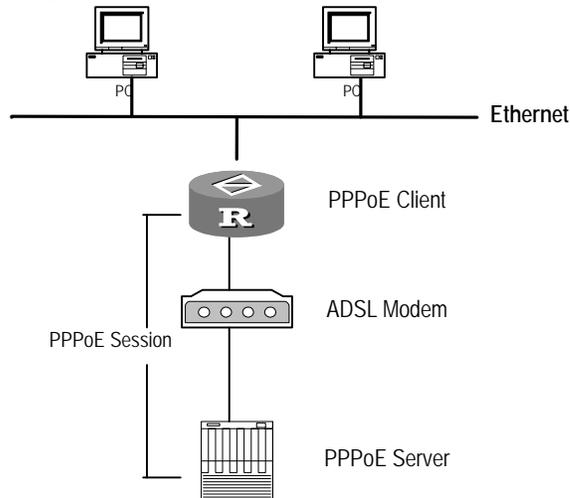
Refer to RFC2516 for PPPoE.

### Introduction to PPPoE client

PPPoE is widely used in ADSL broadband access. Normally, if a host wants to access the Internet via ADSL, it must have been installed with a PPPoE client dial-up software. The 3Com Router series can work as PPPoE clients (that is,

implement the client dial-up function of PPPoE), so the subscribers can access the Internet without installing a PPPoE client software on PCs. Furthermore, all the PCs on the same LAN can share an ADSL account.

**Figure 52** Networking for PPPoE



As shown in the above figure, the PCs on an Ethernet are connected to a 3Com Router running PPPoE client. The data destined for the Internet first reach the router where PPPoE encapsulates the data, and then go through the ADSL access server via the ADSL Modem attached to the router, and finally access the Internet. The overall Internet-accessing process can be implemented, without requiring the subscribers to install any PPPoE client dial-up software.

## Configure PPPoE Client

The fundamental PPPoE configuration includes:

- Configure dialer interface
- Configure PPPoE session

The high-level PPPoE configuration includes:

- Reset or delete PPPoE session

### 1 Configure Dialer Interface

Before configuring a PPPoE session, you should configure a dialer interface and a dialer bundle on the interface. Each PPPoE session should uniquely associates with a dialer bundle, which is uniquely associated to a dialer interface. In other words, only a PPPoE session can be created on a dialer interface.

Perform the commands **dialer-rule** and **interface dialer** in system view and other commands in dialer interface view.

**Table 213** Configure a dialer interface

| Operation                 | Command                                                                              |
|---------------------------|--------------------------------------------------------------------------------------|
| Configure a dialer rule   | <b>dialer-rule dialer-group { protocol-name { permit   deny }   acl acl-number }</b> |
| Create a dialer interface | <b>interface dialer number</b>                                                       |

|                                             |                                                          |
|---------------------------------------------|----------------------------------------------------------|
| Assign an IP address to the interface       | <code>ip address { address mask   ppp-negotiate }</code> |
| Configures a dialer bundle on the interface | <code>dialer bundle bundle-number</code>                 |
| Assigns the interface to a dialer group     | <code>dialer-group group-number</code>                   |

Depending on the needs, it is probably required to configure the parameters such as PPP authentication on a dialer interface. The dialer interface configuration will not be covered in this section, however. Please see *Operation Manual - Dial-up* for reference.

## 2 Configure PPPoE Session

Perform the following configuration in Ethernet interface view.

**Table 214** Configure PPPoE session

| Operation                                        | Command                                                                                                         |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Configure a PPPoE session (permanently online)   | <code>pppoe-client dial-bundle-number number [ no-hostuniq ]</code>                                             |
| Configure a PPPoE session (triggered by packets) | <code>pppoe-client dial-bundle-number number [ no-hostuniq ] idle-timeout seconds [ hold-queue packets ]</code> |
| Delete the PPPoE session                         | <code>undo pppoe-client dial-bundle-number number</code>                                                        |

The 3Com Router support two types of PPPoE connections, which are permanent connections and packet-triggered connections.

- In permanent connection, the router will originate a PPPoE call to automatically and immediately set up a PPPoE session. And this session will be always in place unless the user uses the `undo pppoe-client` command to delete it.
- In packet-triggered connection, the router will not originate a PPPoE call immediately. Instead, the router will originate a PPPoE call to establish a PPPoE session only when there is data waiting for transmission. And the router will automatically terminate the PPPoE session if the PPPoE link has been idle for the specified period.

## 3 Reset or delete PPPoE Session

Perform the `reset pppoe-client` command in all views and the `undo pppoe-client` command in Ethernet interface view.

**Table 215** Reset or delete PPPoE session

| Operation                                                 | Command                                                             |
|-----------------------------------------------------------|---------------------------------------------------------------------|
| Reset a PPPoE session but it will be re-established later | <code>reset pppoe-client { all   dial-bundle-number number }</code> |
| Delete a PPPoE session and it will not be re-established  | <code>undo pppoe-client dial-bundle-number number</code>            |

The commands `reset pppoe-client` and `undo pppoe-client` differ in the sense that the former only resets a PPPoE session temporarily whereas the latter deletes a PPPoE session permanently.

If a permanent PPPoE session has been reset by executing the `reset pppoe-client` command, the router will automatically re-establish the PPPoE session 16 seconds later. If a packet-triggered PPPoE session has been reset by executing the same command, however, the router will re-establish the session only when there is data waiting for transmission.

Regardless of whether a PPPoE session is permanent or packet-triggered, executing the `undo pppoe-client` command will permanently delete the session. Hence, you need to make reconfiguration for establishing a new PPPoE session.

## Display and Debug PPPoE Client

Perform the `display` and `debugging` command in all views.

**Table 216** Display and debug PPPoE Client

| Operation                                                                | Command                                                                                     |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Display state of the PPPoE session and the statistic information as well | <code>display pppoe-client session { summary   packet } [dial-bundle-number number ]</code> |
| Enable debugging of PPPoE client                                         | <code>debugging pppoe-client option [ interface type number ]</code>                        |

## Typical PPPoE Configuration Example

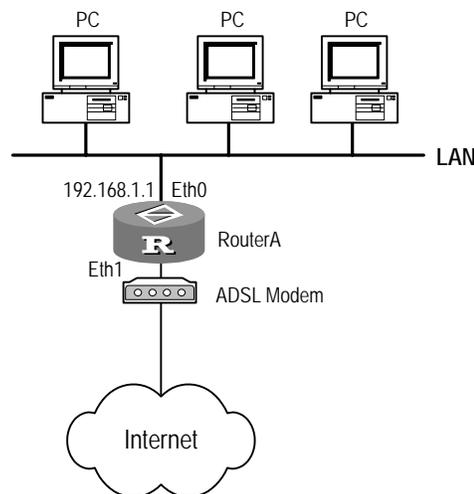
### Access a LAN to the Internet via ADSL

#### I. Networking Requirements

The PCs on a LAN access the Internet via RouterA, and RouterA adopts the permanent approach to accesses the Internet via ADSL. It uses "3com" as the user name of the ADSL account, and the password is 12345. Enable the PPPoE client function on the router, so that the hosts on the LAN can access the Internet, even installed with no PPPoE client software.

#### II. Networking Diagram

**Figure 53** Access a LAN to the Internet via ADSL



#### III. Configuration Procedure

- 1 Configure a dialer interface
 

```
[Router]dialer-rule 1 ip permit
[Router]interface dialer 1
[Router-Dialer1]dialer bundle 1
[Router-Dialer1]dialer-group 1
```

```
[Router-Dialer1] ip ppp-negotiate
[Router-Dialer1] ppp pap local-user 3com password cipher 12345
```

## 2 Configure a PPPoE session

```
[Router] interface ethernet 1
[Router-Ethernet1] pppoe-client dial-bundle-number 1
```

## 3 Configure the LAN interface and the default route

```
[Router] interface ethernet 0
[Router-Ethernet0] ip address 192.168.1.1 255.255.255.0
[Router] ip route-static 0.0.0.0 0.0.0.0 dialer 1
```

If the IP addresses assigned to the PCs on the LAN are private addresses, Network Address Translation (NAT) should also be configured on the router. For the NAT configuration, refer to the related chapters contained in *Operation Manual - Network Protocol*.

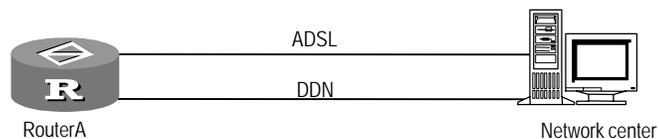
## Use ADSL as Standby Line

### I. Networking Requirements

RouterA uses both DDN leased line and ADSL to connect with the network center and ADSL is used as a standby for the DDN leased line. Thus, if the DDN leased line fails, RouterA can still originate PPPoE call for connection to the network center across ADSL. If ADSL has been idle for two minutes, the PPPoE session will be terminated. If new packets are generated for transmission after that, PPPoE session will be re-established.

### II. Networking Diagram

Figure 54 Typical networking for PPPoE



### III. Configuration Procedure

#### 1 Configure a dialer interface

```
[Router] dialer-rule 1 ip permit
[Router] interface dialer 1
[Router-Dialer1] dialer bundle 1
[Router-Dialer1] dialer-group 1
[Router-Dialer1] ip address ppp-negotiate
```

#### 2 Configure a PPPoE session

```
[Router] interface ethernet 1
[Router-Ethernet1] pppoe-client dial-bundle-number 1 idle-timeout 120
```

#### 3 Configure the DDN interface Serial 0

```
[Router] interface serial 0
[Router-Serial0] ip address 10.1.1.1 255.255.255.0
[Router-Serial0] standby interface dialer 1
```



# 14

## CONFIGURING SLIP

This chapter contains information on the following topics:

- SLIP Overview
- Configure SLIP
- Display and Debug SLIP
- Typical SLIP Configuration Example

---

### SLIP Overview

SLIP (Serial Link Internet Protocol) can transmit data over the asynchronous serial link. Through SLIP, the user can dial up to access the Internet. Compared with other link layer protocols, SLIP is very simple. It does not provide protocol address, error check, header compression. In addition, SLIP does not distinguish packet types, so it supports only one type of network protocol at one time.

For further details about SLIP, you can refer to RFC1055.

---

### Configure SLIP

Because SLIP does not negotiate the name of the remote end, SLIP dialer can only be used with the standard BDR.

SLIP dialer on the physical port configuration includes:

- Configure the synchronous/asynchronous serial interface to asynchronous mode
- Configure the incoming and outgoing call authorities of Modem
- Enable BDR
- Configure the link layer protocol of the interface to SLIP
- Configure Dialer Group and Dialer Rule of activated calls
- Configure the dial string of interface

For the specific configuration methods of BDR and Modem, please refer to related chapters of BDR, Modem in *Operation Manual – Dial-up*.

#### 1 Configure the Sync/Async Serial Interface to Work in Async Mode

Perform the following task in the interface view.

**Table 217** Configure the synchronous/asynchronous serial interface to work in asynchronous mode

| Operation                                                                            | Command                          |
|--------------------------------------------------------------------------------------|----------------------------------|
| Configure the synchronous/asynchronous serial interface to work in asynchronous mode | <code>physical-mode async</code> |

By default, the synchronous/asynchronous serial interface operates in synchronous mode

**2** Configure the link layer protocol of the interface to SLIP

Perform the following task in the asynchronous interface view.

**Table 218** Configure the link layer protocol of the interface to SLIP

| Operation                                                  | Command                   |
|------------------------------------------------------------|---------------------------|
| Configure the link layer protocol of the interface to SLIP | <b>link-protocol slip</b> |

By default, the link layer protocol of the interface is PPP.

Note the following:

- The link layer protocol of the interface can be set to SLIP only when it operates in the asynchronous mode.
- When link layer protocol LAPB, X.25, HDLC or Frame Relay is operating on the interface, the physical attributes of the interface cannot be modified to asynchronous mode. At this time, you should first modify the link layer protocol of the interface to PPP and then you may change the interface attribute to asynchronous mode.

**Display and Debug SLIP**

Perform the following task in all views to monitor the current state of SLIP in real time.

**Table 219** Enable/Disable the information debugging of SLIP

| Operation                                       | Command                                              |
|-------------------------------------------------|------------------------------------------------------|
| Enable the information debugging of SLIP packet | <b>debugging slip { hexadecimal   packet   all }</b> |

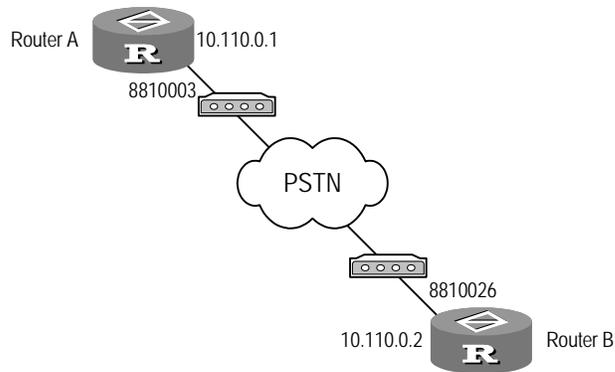
**Typical SLIP Configuration Example**

**I. Networking Requirement**

Interconnect two Router routers via PSTN and run IP.

**II. Networking Diagram**

Figure 3-1 Networking diagram of SLIP dialer



### III. Configuration Procedure

#### 1 Configure Router A:

##### a Configure Dialer Rule

```
[Router]dialer-rule 1 ip permit
```

##### b Configure the synchronous/asynchronous interface to asynchronous mode

```
[Router]interface serial 0
[Router-Serial0]physical-mode async
```

##### c Configure IP address of synchronous/asynchronous interface

```
[Router-Serial0]ip address 10.110.0.1 255.0.0.0
```

##### d Configure the incoming and outgoing call authorities of Modem

```
[Router-Serial0]modem
```

##### e Enable BDR

```
[Router-Serial0]dialer enable-legacy
```

##### f Configure the Dialer String to router B

```
[Router-Serial0]dialer number 8810026
```

##### g Configure the link layer protocol of the interface to SLIP

```
[Router-Serial0]link-protocol slip
```

##### h Specify Dialer Group

```
[Router-Serial0]dialer-group 1
```

##### i Configure the default route to Route B

```
[Router]ip route-static 0.0.0.0 0.0.0.0 10.110.0.2
```

#### 2 Configure Router B:

##### a Configure Dialer Rule

```
[Router]dialer-rule 1 ip permit
```

##### b Configure the synchronous/asynchronous interface to asynchronous mode

```
[Router]interface serial 0
[Router-Serial0]physical-mode async
```

##### c Configure IP address of synchronous/asynchronous interface

```
[Router-Serial0]ip address 10.110.0.2 255.0.0.0
```

##### d Configure the incoming and outgoing call authorities of Modem

```
[Router-Serial0]modem
```

##### e Enable BDR

```
[Router-Serial0]dialer enable-legacy
```

##### f Configure the Dialer Number to router A

```
[Router-Serial0]dialer number 8810003
```

##### g Configure the link layer protocol of the interface to SLIP

```
[Router-Serial0]link-protocol slip
```

##### h Specify Dialer Group

```
[Router-Serial0]dialer-group 1
```

##### i Configure the default route to Route A

```
[Router]ip route-static 0.0.0.0 0.0.0.0 10.110.0.1
```

# 15

## CONFIGURING ISDN PROTOCOL

This chapter contains information on the following topics:

- ISDN Overview
- Configure ISDN
- Display and Debug ISDN
- Typical Configuration Example
- Fault Diagnosis and Troubleshooting of ISDN

---

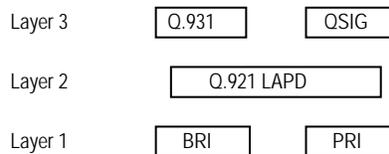
### ISDN Overview

ISDN (Integrated Services Digital Network), developed from telephone integrated digital network (IDN), provides end-to-end digital connection, so as to support wide range of services (including voice and non-voice services).

ISDN provides the user with a group of standard multifunctional user-network interfaces. In ITU-T I.412 recommendations, two types of user-network interfaces are specified: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). The bandwidth of BRI is 2B+D, and that of PRI is 30B+D or 23B+D. Here:

- B channel is a user channel, used to transmit the voice, data and other user information with the transmission rate 64kbps.
- D channel is a control channel and used to transmit the common channel signaling, controlling the calls on B channels of the same interface. The rate of D channel is 64kbit/s (PRI) or 16kbps (BRI). ITU-T Q.921, the data link layer protocol of D channel, defines the rules by which the information is exchanged between layer-2 entities on the user-network interface through D channel. Meanwhile, it supports the access of layer-3 entity. ITU-T Q.931, the network layer protocol of D channel, provides methods to establish, maintain and terminate the network connection between communication application entities.

**Figure 55** Protocol stack of ISDN D channel



---

### Configure ISDN

ISDN configuration includes:

- Configure ISDN signaling type
- Configure QSIG signaling parameters

- Set the called number or sub-address to be checked in digital incoming call
- 1 Configure ISDN Signaling Type

Perform the following configurations in either system view or interface view.

**Table 220** Configure type of signaling on ISDN interface

| Operation                                                      | Command                         |
|----------------------------------------------------------------|---------------------------------|
| Set ISDN signaling to QSIG                                     | <b>isdn protocol-type qsig</b>  |
| Set ISDN signaling to DSS1 (Digital Subscriber Signaling No.1) | <b>isdn protocol-type dss1-</b> |

By default, DSS1 signaling is used on ISDN PRI interfaces.



*The **isdn protocol-type** command can take effect only on ISDN PRI interfaces. For an ISDN BRI interface, it does not take effect. In other words, an ISDN BRI interface can use only DSS1 signaling, whereas an ISDN PRI interface can use either DSS1 signaling or QSIG signaling.*



*Using the **isdn protocol-type** command in system view will not affect the existing ISDN PRI interface, and it will only change the default type of signaling on the newly created ISDN PRI interface.*

- 2 Configure the QSIG Signaling Parameters

If QSIG signaling is used on an ISDN PRI interface, you can configure the QSIG signaling parameters. The following configuration commands can be used only when the ISDN PRI interface adopts QSIG signaling.

- a Length of call reference

Call reference is the flag used to distinguish the communication entities. A call reference uniquely identifies a call.

Perform the following configurations in interface view.

**Table 221** Configure the length of call reference

| Operation                                   | Command                |
|---------------------------------------------|------------------------|
| Set the length of call reference to 1 byte  | <b>isdn crlength 1</b> |
| Set the length of call reference to 2 bytes | <b>isdn crlength 2</b> |

By default, the length of call reference is two bytes.

- b Mode in which a called number is received

A router can receive called numbers in two modes: overlap receiving and complete receiving. You can set the receiving mode on the router according to the transmitting mode on the peer.

Perform the following configurations in interface view.

**Table 222** Configure the receiving mode

| Operation                        | Command                            |
|----------------------------------|------------------------------------|
| Overlap receiving mode is used.  | <b>isdn overlap-receiving</b>      |
| Complete receiving mode is used. | <b>undo isdn overlap-receiving</b> |

By default, ISDN PRI interfaces receive called numbers in overlap receiving mode.

- c Mode in which a called number is sent

When a router originates a call to PBX, it usually contains all called number information in the SETUP message. However, you can configure the command to determine whether the Sending-Complete Information Element (SCIE) should be carried in the SETUP message.

Perform the following configurations in interface view.

**Table 223** Configure the sending mode

| Operation                                                                                                             | Command                           |
|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| Enable the router to carry the Sending-Complete Information Element (SCIE) in the SETUP message when sending a number | <b>isdn sending-complete</b>      |
| Disable the router to carry the Sending-Complete Information Element in the SETUP message when sending the number     | <b>undo isdn sending-complete</b> |

By default, when a router sends a number, the Sending-Complete Information Element is carried in the SETUP message.

#### d Interval of QSIG signaling timer

Perform the following configurations in interface view.

**Table 224** Configure interval for QSIG signaling timer

| Operation                                                        | Command                                          |
|------------------------------------------------------------------|--------------------------------------------------|
| Set interval for a QSIG signaling timer                          | <b>isdn qsig-timer timer-name time-interval</b>  |
| Restore the default interval value(s) of QSIG signaling timer(s) | <b>undo isdn qsig-timer { timer-name   all }</b> |

You can configure the QSIG signaling timers, including T301, T302, T303, T304, T305, T308, T309, T310, T313, T316 and T322. Also, you can use the **display isdn qsig-timer** command to view the default values of all the QSIG signaling timers.

### 3 Verify the called number in an ISDN incoming call

Whenever an ISDN called party receives an incoming call, it can verify the called number in the incoming call from the remote end. If the called number in the remote call differs from the local configuration, the call will be denied. Otherwise, the call will be accepted.

Perform the following configurations in interface view.

**Table 225** Set the called number or sub-address to be checked in digital incoming call

| Operation                                                                      | Command                                                           |
|--------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Set the called number or sub-address to be checked in digital incoming call    | <b>isdn check-called-number [ called-party ] [ :sub-address ]</b> |
| Remove the called number or sub-address to be checked in digital incoming call | <b>undo isdn check-called-number</b>                              |

By default, no called number or sub-address is configured.

The commands are used to set the items to be checked in the digital incoming call. If the sub-address is set, call of the opposite will be rejected when the sub-address is not sent or is sent incorrectly.

**Configure ISDN DoV** ISDN call includes voice call and digital call. Different communication mode makes different calls. In common circumstances, users initiate voice call when making voice communication and initiate digital call when making data transmission. ISDN DoV (Data over Voice) can firstly establish connections by voice call, and then begins data transmission. ISDN DoV can apply to such conditions as digital call is disabled (for example, long-distance call). However compared with digital call, ISDN DoV has some disadvantages. It cannot guarantee correct data transmission all the time and needs ISDN network support.

### 1 Configure Calling Method for Initiating a Connection on an Interface

For an interface generating ISDN calls, you must set the call type to either voice call or data call.

Perform the following configuration in dialer interface or ISDN interface view.

**Table 226** Configure an interface for voice calls

| Operation                                                       | Command                       |
|-----------------------------------------------------------------|-------------------------------|
| Configure an interface to initiate connection using voice calls | <b>dialer data2voice</b>      |
| Configure the interface to initiate connection using data calls | <b>undo dialer data2voice</b> |

### 2 Configure Call Processing Method on an Interface

On an interface receiving ISDN calls, you can configure it to process calls as either voice calls or data calls. Regardless of how it processes a call, however, the packets transmitted over the established connection are data packets.

Perform the following configuration in ISDN interface view.

**Table 227** Configure an interface to receive voice calls

| Operation                                                           | Command                     |
|---------------------------------------------------------------------|-----------------------------|
| Configure an interface to process the received calls as voice calls | <b>Isdn voice2data</b>      |
| Configure the interface to process the received calls as data calls | <b>undo isdn voice2data</b> |

## Display and Debug ISDN

Perform the **display** and **debugging** commands in all views.

**Table 228** Display and debug ISDN

| Operation                                                        | Command                                                      |
|------------------------------------------------------------------|--------------------------------------------------------------|
| Display the current activated call information of ISDN interface | <b>display isdn active-channel [ interface type number ]</b> |
| Display the value of ISDN DSS1 signaling timer                   | <b>display isdn q931-timer</b>                               |
| Display the value of ISDN QSIG signaling timer                   | <b>display isdn qsig-timer [ interface type number ]</b>     |
| Display the current status of ISDN interface                     | <b>display isdn call-info [ interface type number ]</b>      |
| Enable the debugging of ISDN CC                                  | <b>debugging isdn cc [ interface type number ]</b>           |
| Enable the debugging of ISDN q921 protocol                       | <b>debugging isdn q921 [ interface type number ]</b>         |
| Enable the debugging of ISDN q931 protocol                       | <b>debugging isdn q931 [ interface type number ]</b>         |

|                                      |                                                                                                                         |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Enable ISDN QSIG signaling debugging | <code>debugging isdn qsig { alarm   call-state   error   information   message   all } [ interface type number ]</code> |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------|

## Typical Configuration Example

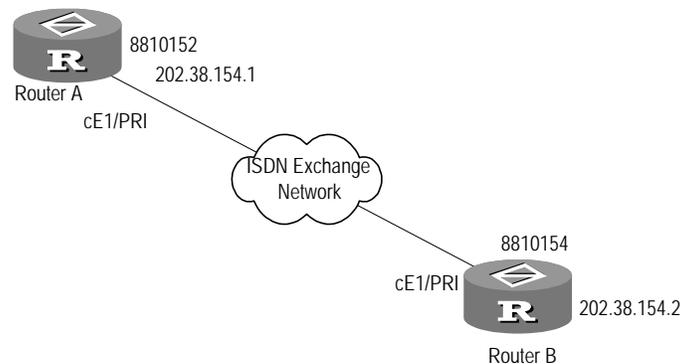
### Interconnect Routers for Data Transmission via ISDN PRI Line

#### I. Networking Requirement

Router A is connected with router B via WAN, as shown in the following diagram.

#### II. Networking Diagram

**Figure 56** Networking diagram of ISDN protocol configuration example



#### III. Configuration Procedure

##### 1 Configure Router A:

- a Create an ISDN PRI interface.

```
[Router] controller e1 0
[Router-E1-0] pri-set
[Router-E1-0] quit
```

- b Configure the ISDN PRI interface.

```
[Router] interface serial 0:15
[Router-Serial0:15] ip address 202.38.154.1 255.255.0.0
[Router-Serial0:15] dialer route-info ip 202.38.154.2 8810154
[Router-Serial0:15] dialer-group 1
[Router-Serial0:15] quit
[Router] dialer-rule 1 ip permit
```

##### 2 Configure Router B:

The parameter configuration on Router B is almost the same as Router A, so it will not be mentioned here.

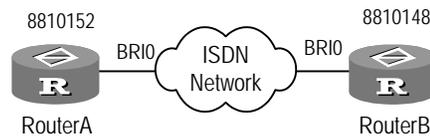
### Typical ISDN DoV Configuration Example

#### I. Networking Requirements

RouterA and Router are connected over an ISDN and RouterA will initiate a call to RouterB. The call is handled in the way of processing a voice call, and RouterA and RouterB transmit data after the call is set up.

## II. Networking Diagram

Figure 57 Networking for ISDN DoV



## III. Configuration Procedure

### 1 Configure Router A:

```
[Router]dialer-rule 1 ip permit
[Router]interface bri 0
[Router-Bri0]ip address 100.1.1.1 255.255.255.0
[Router-Bri0]dialer-group 1
[Router-Bri0]dialer route ip 100.1.1.2 8810148
[Router-Bri0]dialer data2voice
```

### 2 Configure Router B:

```
[Router]dialer-rule 1 ip permit
[Router]interface bri 0
[Router-Bri0]ip address 100.1.1.2 255.255.255.0
[Router-Bri0]dialer-group 1
[Router-Bri0]dialer route ip 100.1.1.1 8810152
[Router-Bri0]isdn voice2data
```

## Fault Diagnosis and Troubleshooting of ISDN

**Fault: Two routers are connected via an ISDN PRI line, but pinging the routers is not successful.**

Troubleshooting:

- 1 Execute the `display isdn call-info` command. If the system prompts "there is no isdn port", it means that there is no ISDN PRI port, and you should configure one. For the configuration, refer to the section "cE1/PRI Interface and cT1/PRI Interface Configuration" in *Operation Manual - Interface*.
- 2 If enabling Q.921 information debugging and debugging information "ISDN-D send data error" is output, it indicates that the physical layer is not activated. You can try to use the commands `shutdown` and `undo shutdown` to disable and re-enable the related interface.
- 3 Check whether the dialer is configured correctly. If the dialer is configured correctly and no "ISDN-D send data error" is displayed, then it's possible the ISDN line is not connected well.

# 16

## CONFIGURING LAPB AND X.25

This chapter contains information on the following topics:

- X.25 and LAPB Protocols Overview
- Configure LAPB
- Configure X.25
- Configure X.25 over Other Protocols
- Display and Debug LAPB and X.25
- Typical LAPB Configuration Example
- Typical X.25 Configuration Example
- Fault Diagnosis and Troubleshooting of LAPB
- Fault Diagnosis and Troubleshooting of X.25

---

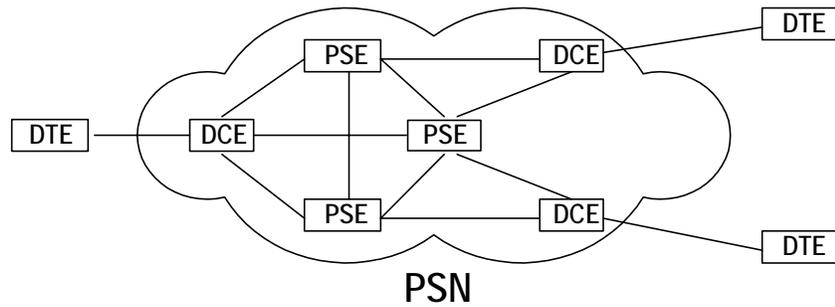
### **X.25 and LAPB Protocols Overview**

X.25 protocol is the interface procedure between the data terminal equipment (DTE) and data circuit-terminating equipment (DCE). In 1974, CCITT issued the first draft of X.25, whose initial files were based on the experiences and recommendations of Telenet and Tymnet of USA and Datapac packet-switched networks of Canada. It was revised in 1976, 1978, 1980 and 1984, added many optional service functions and facilities.

With X.25, two DTE can communicate with each other via the existing telephone network. X.25 sessions are established when one DTE device contacts another to request a communication session. The DTE device that receives the request can either accept or refuse the connection. If the request is accepted, the two systems begin full-duplex information transfer. Either DTE device can terminate the connection. After the session is terminated, any further communication requires the establishment of a new session.

X.25 is the protocol of point-to-point interaction between DTE and DCE. DTE usually refers to the host or terminal at the user side, and DCE usually refers to the synchronous modem. DTE is connected with DCE directly, DCE is connected to a port of packet switching exchange, and some connections are established between the packet switching exchanges, thus forming the paths between different DTE. In an X.25 network, the relation between entities is shown in the following diagram:

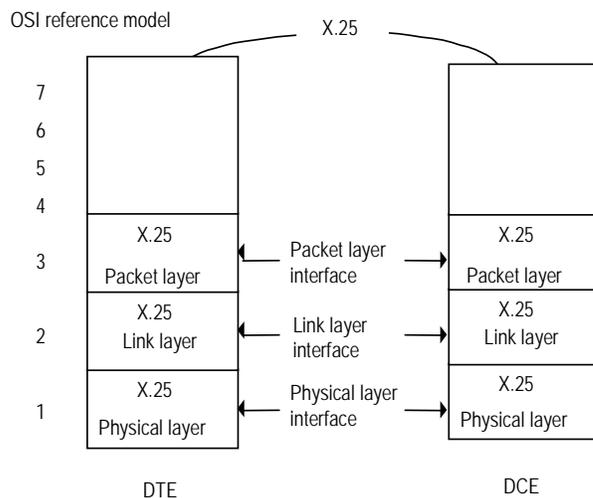
**Figure 58** X.25 network model



DTE: Data Terminal Equipment  
 DCE: Data Circuit-terminating Equipment  
 PSE: Packet Switching Equipment  
 PSN: Packet Switching Network

The X.25 protocol suite maps to the lowest three layers of the OSI (Open System Interconnection) reference model. The following protocols are typically used in X.25 implementations: Packet-Layer Protocol (PLP), Link Access Procedure Balanced (LAPB), and other physical-layer serial interfaces. X.25 layer 3 (packet-layer protocol) describes the format of packet used by the packet layer and the procedure of packet switching between two layer 3 entities. X.25 layer 2 (link-layer protocol), also called LAPB (Link Access Procedure Balanced), defines the format and procedure of interactive frames between DTE and DCE. X.25 layer 1 (physical-layer protocol) defines some physical and electrical characteristics in the connection between DTE and DCE. The above relation is shown in the following diagram.

**Figure 59** DTE/DCE interface

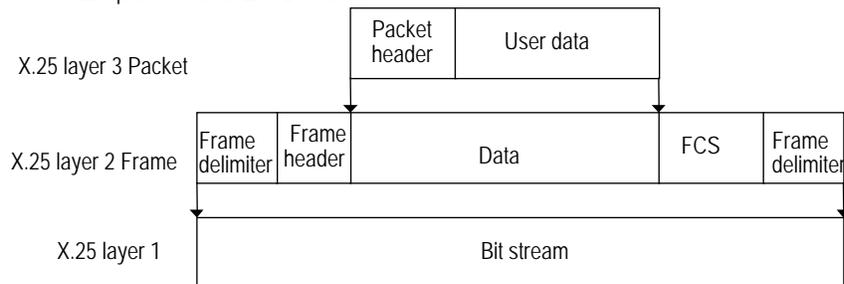


A virtual circuit is a logical connection created to ensure reliable communication between two network devices. A virtual circuit denotes the existence of a logic, bi-directional path from one DTE device to another across an X.25 network. Two types of X.25 virtual circuits exist: permanent virtual circuit (PVC) and switched virtual circuit (SVC). PVCs are permanently established connections used for frequent and consistent data transfers, whereas SVCs are temporary connections used for sporadic data transfers.

Once a virtual circuit is established between a pair of DTEs, it is assigned with a unique virtual circuit number. When one DTE is to send a packet to the other, it numbers this packet (with virtual circuit number) and sends it to DCE. According to the number on the packet, DCE determines the method to switch this packet within the switching network, so that this packet can reach the destination. Since the X.25 layer 3 multiplexes the link established between DTE and DCE by the X.25 layer 2 (LAPB), what finally viewed by the user will be multiple usable virtual circuits.

The relation between packets and frames in various X.25 layers is shown in the following diagram.

**Figure 60** X.25 packet and LAPB frame



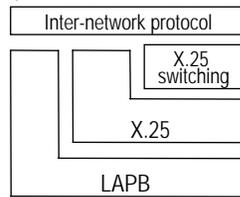
X.25 link layer specifies the frame switching process between DTE and DCE. In terms of hierarchy, the link layer seems to bridge the packet layer interface of DTE and that of DCE. Through this bridge, the packets can be transmitted continuously between the packet layer of DTE and that of DCE. The link layer has such main functions as follows:

- Transmit the data effectively between DTE and DCE
- Ensure the synchronization of information between the receiver and transmitter
- Detect and correct the error in the transmission
- Identify and report the procedure error to the higher layer protocol
- Inform the packet layer of the link layer state

As specified in international standards, X.25 link layer protocol LAPB adopts the frame structure of high-level data link control (HDLC) and the frame structure is a subset of LAPB. The bi-directional link will be established when either site sends an SABM (Set Asynchronous Balanced mode) command and the other replies with UA.

Defined as X.25 layer-2 protocol, LAPB is actually a separate link layer protocol, which can transmit the data with LAPB bearing non-X.25 upper layer protocol. 3Com Router series can configure the link protocol of serial interface to LAPB and perform simple local data transmission. Meanwhile, X.25 of 3Com Router series has switching function, that is to say, the router can be used as a small X.25 packet switch. The following diagram shows the relations among LAPB, X.25 and X.25 switching.

**Figure 61** Relations among LAPB, X.25 and X.25 switching



## Configure LAPB

LAPB configuration includes:

- Configure the link protocol of the interface to LAPB
  - Configure LAPB protocol parameters
- 1 Configure the Link Layer Protocol of the Interface to LAPB

Perform the following command in the interface view.

**Table 229** Configure the link layer protocol of the interface to LAPB

| Operation                                                  | Command                                              |
|------------------------------------------------------------|------------------------------------------------------|
| Configure the link layer protocol of the interface to LAPB | <code>link-protocol lapb [ dte   dce ] [ ip ]</code> |

If not specified, the working mode of LAPB is DTE by default.

- 2 Configure LAPB Protocol Parameter

- a Configure LAPB operating mode (also called modulo)

There are two LAPB modulus: Modulo 8 and Modulo128. Each data frame (l frame) is numbered by sequence, the number can be any from 0 to modulo minus 1, and the sequence number is selected periodically within the range of the modulo.

In the interface view, configure as follows:

**Table 230** Configure LAPB frame numbering mode

| Operation                                                | Command                              |
|----------------------------------------------------------|--------------------------------------|
| Configure LAPB frame numbering mode (also called modulo) | <code>lapb modulo { 128   8 }</code> |

By default, the LAPB modulus is Modulo 8.

- b Configure LAPB parameter K

The parameter K in the LAPB window represents the maximum number of l frames numbered in sequence that is to be identified by the DTE or DCE in any specified time.

In the interface view, configure as follows:

**Table 231** Configure LAPB window parameter K

| Operation                                            | Command                               |
|------------------------------------------------------|---------------------------------------|
| Configure LAPB window parameter K                    | <code>lapb window-size k-value</code> |
| Restore the default value of LAPB window parameter K | <code>undo lapb window-size</code>    |

By default, k is 7.

- c Configure LAPB N1, N2

N1 value represents the maximum number bits of I frame that DCE or DTE wants to receive from DTE or DCE.

N2 value represents the maximum number of times that DCE or DTE tries to successfully send a frame to DTE or DCE.

**Table 232** Configure LAPB N1, N2

| Operation                                      | Command                        |
|------------------------------------------------|--------------------------------|
| Configure LAPB parameter N1                    | <b>lapb max-frame n1-value</b> |
| Restore the default value of LAPB parameter N1 | <b>undo lapb max-frame</b>     |
| Configure LAPB parameter N2                    | <b>lapb retry n2-value</b>     |
| Restore the default value of LAPB parameter N2 | <b>undo lapb retry</b>         |

By default, n1 is 12032, and n2 is 10.

**d** Configure LAPB T1, T2, T3

LAPB T1, the retransmission timer (T1) determines how long a frame that is already sent, can remain unacknowledged before retransmission. The value of T1 should be larger than the maximum interval between sending a frame and receiving its response frame. Retransmission timer is started after sending the frame but if response is not received and timer is expired then frame will be retransmitted.

LAPB T2, the receiving timer (T2) determines when to send a confirmation frame to the opposite DCE (or DTE) before T1 expires ( $T2 < T1$ ).

LAPB T3, the idle channel timer, determines when to report the long-time idle channel state to the packet layer. The timer value must be larger than T1 in DCE ( $T3 > T1$ ). If T3 is 0, it indicates that the timer is not set.

**Table 233** Configure LAPB system timer T1, T2, T3

| Operation                                                 | Command                                                       |
|-----------------------------------------------------------|---------------------------------------------------------------|
| Configure LAPB system timer T1, T2, T3                    | <b>lapb timer { t1 t1-value   t2 t1-value   t3 t3-value }</b> |
| Restore the default value of LAPB system timer T1, T2, T3 | <b>undo lapb timer{ t1   t2   t3 }</b>                        |

By default, T1 is 2000ms; T2 is 1000ms and T3 is 0ms.

## Configure X.25

X.25 configuration includes:

- Configure X.25 interface
- Configure X.25 interface supplementary parameter
- Configure X.25 datagram transmission
- Configure the supplementary parameters of X.25 datagram transmission
- Configure X.25 sub interface
- Configure X.25 switching
- Configure X.25 load balancing

Besides configuring X.25, appropriate modification to some LAPB parameters in certain cases can also optimize the performance of X.25.

## Configure X.25 Interface

The configuration of X.25 interface includes:

- Configure X.121 address
- Configure X.25 working mode
- Configure X.25 virtual circuit range
- Configure X.25 modulo
- Configure X.25 default flow control parameter

Only when configured as an X.25 interface, can an interface transmit data with X.25 protocol.



*In the following configuration commands, only “Configure X.25 working mode” is mandatory, and other configuration items are optional, depending on the specific condition of X.25 network that is accessed.*

### 1 Configure X.121 address

If the 3Com Router series does not originate or terminate calls but only participates in X.25 switching, there is no need to configure an X.121 address. However, if the 3Com Router series is attached to a X.25 Network, you should configure an X.121 address for the interface, and usually, the address is provided by the ISP.

To set/cancel the X.121 address, perform the following task in interface view.

**Table 234** Set/Cancel the X.121 address of the interface

| Operation                                     | Command                                   |
|-----------------------------------------------|-------------------------------------------|
| Set the X.121 address of the interface        | <b>x25 x121-address<br/>x.121-address</b> |
| Cancel the set X.121 address of the interface | <b>undo x25 x121-address</b>              |

### 2 Configure X.25 working mode

To configure X.25 working mode, perform the following task in the interface view.

**Table 235** Set X.25 working mode

| Operation                                                | Command                                                           |
|----------------------------------------------------------|-------------------------------------------------------------------|
| Set the working mode and packet format of X.25 interface | <b>link-protocol x25 [ dte  <br/>dce ] [ nonstandard   ietf ]</b> |

Layer 3 of X.25 supported by 3Com Router series can work in both DTE mode and DCE mode. It can also specify the datagram format among the two optional formats: IETF and Nonstandard.

Note that generally speaking, public X.25 packet switching network requires the router to access at DTE side and requires the IETF format. Therefore, the working mode of X.25 should be DTE and the format should be IETF. If a pair of serial interfaces of two routers is directly connected for data transmission, make sure the two transmission ends are DTE and DCE and the formats are the same.

For X.25 supported by 3Com Router series, default working mode is DTE and default format is IETF.

### 3 Configure X.25 virtual circuit range

X.25 protocol can multiplex multiple virtual connection over a real physical link between DTE and DCE, also called virtual circuit (VC) or logical channel (LC). X.25 can establish up to 4095 virtual connections numbered from 1 to 4095. The number that can be employed to identify each virtual circuit (or logical channel) is called logical channel identifier (LCI) or virtual circuit number (VCN).



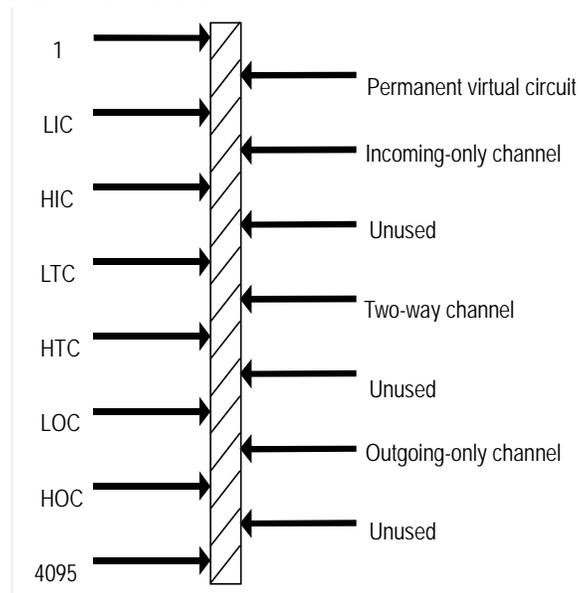
*Strictly speaking, virtual circuit and logical channel are two different concepts. However, they are not much different at the user side.*

X.25 protocol divides the logical channel into 4 areas. (listed here in numerically increasing order): Permanent virtual circuits (PVCs), Incoming-only circuits, Two-way circuits, Outgoing-only circuits.

According to the X.25 recommendation proposed by ITU-T, DCE selects an available logical channel with a smaller number from the "one-way incoming call channel range" and "two-way channel range" to initiate a call, while DCE selects an available logical channel with a larger number from the "one-way incoming call channel range" and "two-way channel range" to initiate a call. Thus, we can avoid the case that one side of the communication occupies all the channels, and minimize the possibility of call collision.

In X.25 protocol, six parameters are employed to delimit the four sections, as shown in the diagram below.

**Figure 62** X.25 channel delimitation



For the meanings of these six parameters, please refer to the following table.

**Table 236** X.25 channel delimitation parameters

| Parameter | Meaning                       |
|-----------|-------------------------------|
| LIC       | Lowest Incoming-only Channel  |
| HIC       | Highest Incoming-only Channel |
| LTC       | Lowest Two-way Channel        |
| HTC       | Highest Two-way Channel       |
| LOC       | Lowest Outgoing-only Channel  |
| HOC       | Highest Outgoing-only Channel |

Perform the following task in the interface view:

**Table 237** Set/cancel X.25 virtual circuit range

| Operation                                                                                                                                  | Command                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Set X.25 virtual circuit range                                                                                                             | <b>x25 vc-range</b> { <b>in-channel</b> <i>hic lic</i>   <b>bi-channel</b> <i>htc ltc</i>   <b>out-channel</b> <i>hoc loc</i> } |
| Cancel the set <b>vc-range</b> { <b>in-channel</b> <i>hic lic</i>   <b>bi-channel</b> <i>htc ltc</i>   <b>out-channel</b> <i>hoc loc</i> } | <b>undo x25 vc-range</b>                                                                                                        |

The above shows that each section (except the permanent virtual circuit section) is defined by two parameters: upper limit and lower limit, the value of which ranges between 1 and 4095 (including 1 and 4095). Correct configuration must satisfy the following conditions:

- In strict numerically increasing order, i.e. 1licic<lthtc<lochoc4095.
- If the upper limit (or lower limit) of a section is 0, then the lower limit (or upper limit) shall also be 0, (which indicates this section is prohibited to use).

Finally, the following should be noted:

- At the two sides (i.e. DTE and DCE) of a physical connection, the six parameters of X.25 must be equal correspondingly, otherwise, the procedure will possibly operate abnormally, resulting in data transmission failure.
- During the configuration, after ensuring the numerically increasing order, pay attention to the default values of various parameters, and set the parameters according to actual condition.
- Because X.25 protocol requires DTE and DCE to have the same virtual circuit range parameters, the new configuration can not take effect immediately after successful X.25 protocol negotiation. It is necessary to first execute **shutdown** and **undo shutdown** commands.

#### 4 Configure X.25 modulo

The implementation of X.25 in 3Com Router series supports both modulo 8 and modulo 128 packet sequence numbering. Module 8 is the default.

To set/cancel the packet sequence numbering, perform the following task in the interface view:

**Table 238** Set/Cancel X.25 packet numbering modulo

| Operation                                     | Command                                     |
|-----------------------------------------------|---------------------------------------------|
| Set the packet sequence numbering mode        | <b>x25 modulo</b> { <b>8</b>   <b>128</b> } |
| Cancel the set packet sequence numbering mode | <b>undo x25 modulo</b>                      |

By default, X.25 interface use modulo 8 mode.



*Please note that X.25 procedure requires DTE and DCE to have the same packet numbering mode, therefore the configuration will take effect by executing the **shutdown** and **undo shutdown** commands.*



*Besides, the packet sequence numbering mode of X.25 layer 3 is different from the frame sequence numbering mode of LAPB (X.25 layer 2). When modulo 128 numbering mode is employed in the DTE/DCE interface with high throughput rate, for LAPB, only the efficiency of local DTE/DCE interface is affected, that is point-to-point efficiency increases. While for X.25 layer 3, the efficiency of*

*end-to-end is affected, that is, the efficiency between two sets of communicating DTE increases.*

5 Configure X.25 flow control parameter

It is essential to set correct default flow control parameters (window size and packet size) for the operation of the link because X.25 protocol is good at traffic control. However, most public X.25 packet networks use the default window size and maximum packet size specified in ITU-T X.25 Recommendation, which is also true for 3Com Router series. Therefore, this task may be optional without special requirements of service provider.

After setting window size and maximum packet size, the SVCs that can be established only with call process will use these values if related parameters are not negotiated in the call process. The PVCs that can be established without call process will also use these values if no window size or packet size option is assigned when specifying PVC.

X.25 transmitting end will fragment the too long data packet of upper layer according to the maximum packet size and mark in the last fragment packet (M bit is not set). When the packet reaches the receiving end, X.25 reassembles all these fragment packets, and judges whether a complete packet is received according to M bit marker. Therefore, too small value of the maximum packet size will consume too much router resources on packet fragmenting and assembling, thus lowering efficiency.

Finally, the following two points should be noted:

- Maximum packet size < MTU\*8 < LAPB N1.
- New configuration will take effect only after executing **shutdown** and **undo shutdown** commands

To set/cancel the default flow control parameter, perform the following tasks.

**Table 239** Set the default flow control parameter

| Operation                                                           | Command                                       |
|---------------------------------------------------------------------|-----------------------------------------------|
| Set the receiving window and sending window size of virtual circuit | <b>x25 window-size in-packets out-packets</b> |
| Cancel the set receiving and sending window size of virtual circuit | <b>undo x25 window-size</b>                   |
| Set the receiving and sending maximum packet length                 | <b>x25 packet-size in-packets out-packets</b> |
| Cancel the set receiving and sending maximum packet length          | <b>undo x25 packet-size</b>                   |

**Configure X.25 Interface Supplementary Parameter**

- The Configuration of X.25 interface supplementary parameter includes:
- Configure the time delay of X.25 layer 3 timer
- Configure the attributes related to X.25 address, including the following configuration items:
- Configure the alias of interface address
- Configure to skip the calling or called address
- Configure whether to check the address code block in call accepting packet.
- Configure whether to carry the address code block in call accept packet
- Configure default upper layer protocol

- Prohibit the restart of X.25 layer 3

It is necessary to configure certain supplementary X.25 parameters in some special network environments.

## 1 Configure the delay of X.25 layer 3 timer

X.25 protocol defines a series of timers to facilitate its procedure. After X.25 sends a control packet, if it does not receive the response before the timeout of the corresponding timer, X.25 protocol will take corresponding measure to handle this abnormal event. The names and corresponding procedures of these timers are shown in the following table.

**Table 240** X.25 layer 3 timer

| Procedure name | Timer name |          |
|----------------|------------|----------|
|                | DTE side   | DCE side |
| Restart        | T20        | T10      |
| Call           | T21        | T11      |
| Restore        | T22        | T12      |
| Clear          | T23        | T13      |
| Register       | T28        |          |

In the table, T28 is the timer of "sending register request", and is only defined at the DTE side. It is used to dynamically apply to stop the selective services in the network. Its reference value is 300 seconds, and cannot be modified. Perform the following tasks in the interface view.

**Table 241** Set X.25 layer 3 timer delay

| Operation                                                                                   | Command                      |
|---------------------------------------------------------------------------------------------|------------------------------|
| Set the timer delay value of restart procedure<br>Default value (second): DTE: 180 DCE: 60  | <b>x25 timer tx0 seconds</b> |
| Cancel the set timer delay value of restart procedure                                       | <b>undo x25 timer tx0</b>    |
| Set the timer delay value of call procedure<br>Default value (second): DTE: 200 DCE: 180    | <b>x25 timer tx1 seconds</b> |
| Cancel the set timer delay value of call procedure                                          | <b>undo x25 timer tx1</b>    |
| Set the timer delay value of restore procedure<br>Default value (second): DTE: 180 DCE: 60  | <b>x25 timer tx2 seconds</b> |
| Cancel the set timer delay value of restore procedure                                       | <b>undo x25 timer tx2</b>    |
| Set the timer delay value of clearing procedure<br>Default value (second): DTE: 180 DCE: 60 | <b>x25 timer tx3 seconds</b> |
| Cancel the set timer delay value of clearing procedure                                      | <b>undo x25 timer tx3</b>    |

## 2 Configure the attribute related to X.25 address

- To establish a SVC with a call, X.25 address is needed, which adopts the address format specified in ITU-T Recommendation X.121. X.121 address is a character string consists of the Arabic numerals from 0 to 9, and it is of 0 to 15 characters.
- Configure an alias for the interface

When an X.25 call is forwarded across the network, different networks will be likely to make some modifications on the called address according to their own needs, such as adding or deleting the prefix. In such cases, the destination address

of a call that reaches X.25 interface may be inconsistent with X.121 address of the destination interface (because the destination address of this call is modified within the network), still the interface will accept this call. At this time, one or multiple aliases should be specified for this interface by performing the following tasks in the interface view:

**Table 242** Specify/Cancel an alias for the interface

| Task                                                   | Command                                              |
|--------------------------------------------------------|------------------------------------------------------|
| Specify an alias for the interface                     | <b>x25 alias-policy match-type alias-string</b>      |
| Cancel the specification of an alias for the interface | <b>undo x25 alias-policy match-type alias-string</b> |

To satisfy the requirements of different networks, nine matching modes and the formats of corresponding alias strings are defined for X.25 in 3Com Router series, as shown in the following table.

**Table 243** Alias match modes and meanings

| Matching mode | Meaning                                                                               | Example                                                                                          |
|---------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Free          | Free matching, the alias string is in the form of 1234                                | 1234 will match with 561234, 1234567 and 956123478, but will not match with 12354.               |
| free-ext      | Extended free matching, the alias string is in the form of ...1234..                  | ...1234.. will match with 678123459, but will not match with 68123459, 67812345 and 6781234591.  |
| Left          | Left-justified matching mode, the alias string is in the form of \$1234               | \$1234 will match with 1234567 and 12346790, but will not match with 3123478 and 123784.         |
| left-ext      | Extended left-justified matching mode, the alias string is in the form of \$1234...   | \$1234... will match with 1234679 and 1234872, but will not match with 123468 and 12346890.      |
| Right         | Right-justified match mode, the alias string is in the form of 1234\$                 | 1234\$ will match with 791234 and 6901234, but will not match with 7912345 and 6212534.          |
| right-ext     | Extended right-justified matching mode, the alias string is in the form of ....1234\$ | ....1234\$ will match with 79001234 and 86901234, but will not match with 7912345 and 506212534. |
| Strict        | Strict matching mode, the alias string is in the form of \$1234\$                     | \$1234\$ can only match with 1234                                                                |
| Whole         | Whole matching mode, the alias string is in the form of .....                         | ..... will match with all the valid X.121 addresses with the length of 8                         |
| whole-ext     | Extended whole matching mode, the alias string can only be *                          | * will match with all the valid X.121 addresses                                                  |

### 3 Configure the attributes related to the address code block in the call packet or call accept packet

As specified in X.25 protocol, the call packet must carry the information set of both the calling DTE address (source address) and the called DTE address (destination address). This address information set is called the address code block. While in call accept packet, some networks require that both (the calling DTE address and the called DTE address) be carried, some networks require that only one of the two be carried, while some others require that neither should be carried. X.25 in 3Com Router series enables users to make choices according to the requirement of specific network. Perform the following task in interface view.

**Table 244** Configure/Cancel the attributes related to the address code block in the call packet or call accept packet

| Operation                                                                                                   | Command                                               |
|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Not carrying the called DTE address information when a call is originated<br>Default: carry                 | <b>x25 ignore called-address (by default)</b>         |
| Cancel not carrying the called DTE address information when a call is originated                            | <b>undo x25 ignore called-address</b>                 |
| Not carrying the calling DTE address information when a call is originated<br>Default: carry                | <b>x25 ignore calling-address (by default)</b>        |
| Cancel not carrying of the calling DTE address information in a call                                        | <b>undo x25 ignore calling-address</b>                |
| Not carrying the called DTE address information when the originated call is accepted<br>Default: not carry  | <b>x25 response called-address</b>                    |
| Cancel not carrying of the called DTE address information when the originated call is accepted              | <b>undo x25 response called-address (by default)</b>  |
| Not carrying the calling DTE address information when the originated call is accepted<br>Default: not carry | <b>x25 response calling-address</b>                   |
| Cancel not carrying the calling DTE address information when the originated call is accepted                | <b>undo x25 response calling-address (by default)</b> |
| Check the address code block after the response of the call is received<br>Default: check                   | <b>x25 check-response-address (by default)</b>        |
| Cancel check the address code block after the response of the call is received                              | <b>undo x25 check-response-address</b>                |

#### 4 Configure default upper layer protocol

X.25 call request packet includes a CUD field (Call User Data), which shows the upper layer protocol type X.25 protocol carries. When receiving X.25 calls, the router will check packet CUD field; when receiving calls carrying the CUD fields that cannot be identified, it will reject them. But an upper layer protocol can be specified as the default protocol borne on the X.25 of the 3Com Router series. When the X.25 of the 3Com Router series receives a call with an unrecognizable CUD, it will treat it as the default upper layer protocol specified by user.

In the interface view, perform the following task to set/cancel the default upper layer protocol borne on X.25.

**Table 245** Set/Cancel the default upper layer protocol borne on X.25

| Operation                                                               | Command                                       |
|-------------------------------------------------------------------------|-----------------------------------------------|
| Specify the default upper layer protocol borne on X.25<br>Default: IP   | <b>x25 default-protocol [ ip   ipx ]</b>      |
| Cancel the specifying of the default upper layer protocol borne on X.25 | <b>undo x25 default-protocol [ ip   ipx ]</b> |

By default, the upper protocol carried by X.25 is IP protocol.

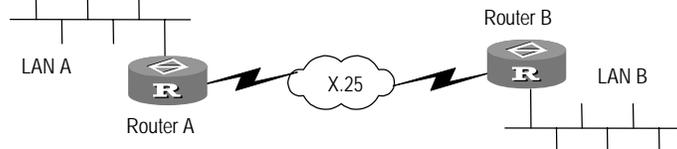
## Configure X.25 Datagram Transmission

The configuration of X.25 datagram transmission includes:

- Create the mapping from the protocol address to X.121 address
- Create the permanent virtual circuit

In the most frequently used X.25 service, data is transmitted remotely between two hosts using the X.25 protocol via X.25 public packet network. As shown in the figure below, LAN A and LAN B are far apart, and X.25 packet switching network can be used to realize information exchange between them.

**Figure 63** LAN interconnection via X.25



The datagram uses IP address to communicate data and information between LAN A and LAN B, whereas X.121 address is used inside X.25. Therefore, we setup correct mapping between the IP address and X.121 address.

### 1 Create the mapping from the protocol address to X.121 address

An X.25 interface has its own X.121 address and inter-network protocol (such as IP protocol) address. When X.25 initiates a call through this interface, the source address (calling DTE address) it carries in the call request packet is the X.121 address of this interface.

For a datagram with a definite destination IP address, its corresponding X.121 destination address is located by the configured address mapping. The called destination, just like a calling source, also has its own protocol address and X.121 address. Establish the mapping between the destination protocol address and the X.121 address at the calling source, you can find the destination X.121 address according to the destination protocol address, and successfully initiate a call.

In the interface view, perform the following commands to create/delete an address mapping.

**Table 246** Create/Delete the mapping from the protocol address to X.121 address

| Operation                                                                 | Command                                                                                          |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Create the mapping from the destination protocol address to X.121 address | <code>x25 map { ip   ipx }<br/>protocol-address x121-address<br/>x.121-address [ option ]</code> |
| Delete the mapping from the destination protocol address to X.121 address | <code>undo x25 map protocol<br/>protocol-address</code>                                          |



*The protocol-address and x.121-address in the command line refer to the protocol address and X.121 address of the destination, not those of the source.*



*An address mapping should be created for every destination.*



*While creating an address mapping, specify its attributes with the option items. The meanings and specific content of these options will be described in subsequent sections.*

### 2 Create the permanent virtual circuit (PVC)

A permanent virtual circuit can be created for large-traffic and stable data transmission on leased line. Permanent virtual circuits (PVCs) do not need any call

process and it always exists. An address mapping will be created implicitly while a permanent virtual circuit is created.

To create/delete a permanent virtual circuit, perform the following tasks in interface view.

**Table 247** Create/Delete permanent virtual circuit

| Operation                          | Command                                                                                   |
|------------------------------------|-------------------------------------------------------------------------------------------|
| Create a permanent virtual circuit | <b>x25 pvc pvc-number protocol protocol-address x121-address x.121-address [ option ]</b> |
| Delete a permanent virtual circuit | <b>undo x25 pvc pvc-number</b>                                                            |

The format of this command shows that while a permanent virtual circuit is created, an address mapping is also created for it. Similarly, the *protocol-address* and *x.121-address* in the command also refer to the destination address. While creating a permanent virtual circuit, some attributes of the PVC can also be selected via the option. This [option] is a subset of [option] in the command "**x25 map..... [option]**".

For configuration example of permanent virtual circuit, refer to subsequent sections.

### Configure Additional Parameters of X.25 Datagram Transmission

The Configuration additional parameters of X.25 datagram transmission includes:

- Specify the maximum idle time of SVC
- Specify the maximum number of SVCs that is associated with the same address mapping
- Specify the pre-acknowledgement of packet
- Configure X.25 user facility
- Set the length of virtual circuit queue
- Broadcast via X.25
- Restrict the use of address mapping
- Configure the interface with the standby center

The X.25 of the 3Com Router series allows adding some additional characteristics, including a series of optional user facilities stipulated in ITU-T Recommendation X.25.

This section shows how to configure such additional characteristics, including the options in the two commands of "**x25 map .....**" and "**x25 pvc .....**". Please select and configure these additional characteristics according to the actual needs, X.25 network structure and the services provided by service provider.

#### 1 Configure SVC maximum idle time

Specify a time period, and if SVC is idle within this period (no packet interaction), then X.25 of the 3Com Router series will automatically clear this SVC to avoid unnecessary expenses. Before the data packet is sent next time, this SVC will be reestablished. So the activation of this characteristic will not affect data transmission.

In the interface view, this task can be accomplished in two different ways. For details, refer to the table as follows.

**Table 248** Specify/Cancel SVC maximum idle time

| Operation                                                            | Command                                                                                            |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Specify maximum idle time for all the SVCs on an interface           | <b>x25 timer idle minutes</b>                                                                      |
| Specify maximum idle time for SVC associated with an address mapping | <b>x25 map protocol<br/>protocol-address<br/>x121-address x.121-address<br/>timer idle minutes</b> |
| Cancel specify maximum idle time for all the SVCs on an interface    | <b>undo x25 timer idle</b>                                                                         |

By default, the value of SVC maximum idle time is 0 minute, which means this SVC will not be disconnected for idle times out.

### 2 Configure the maximum number of SVCs that are associated with the same address mapping

The maximum number of virtual circuits to be set up on the same address mapping can be specified. The X.25 of the 3Com Router series can establish up to 8 virtual circuits on one address mapping. In case of large traffic and low line rate, this parameter can be increased properly to reduce data loss. By default, one address mapping is associated with only one virtual circuit.

In the interface view, perform the following commands.

**Table 249** Specify/Cancel the maximum number of SVCs associated with the same address mapping

| Operation                                                                                    | Command                                                                                          |
|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Specify the maximum number of SVCs associated with all address mappings on an X.25 interface | <b>x25 vc-per-map count</b>                                                                      |
| Specify the maximum number of SVCs associated with an address mapping                        | <b>x25 map protocol<br/>protocol-address<br/>x121-address x.121-address<br/>vc-per-map count</b> |
| Cancel the maximum number of SVCs associated with all address mappings on an X.25 interface  | <b>undo x25 vc-per-map</b>                                                                       |

By default, the value of nvc is 1.

### 3 Configure the pre-acknowledgment of packets

According to X.25 protocol, the receiving party will send an acknowledgment only after the receiving window is full (the number of received packets equals the **window-size in-packets** value). However, in some X.25 networks, the delays may be long, resulting in low efficiency of sending and receiving. Therefore, we specify a value. Each time the number of received packets reaches the value, the acknowledgment will be sent to the peer, thus improving receiving and sending efficiency. This value, called a "receive-threshold", ranges between 0 and **window-size in-packets**. If it is set to 1, every packet will be acknowledged. If it is set to **window-size in-packets**, the acknowledgment will be sent only after the receiving window is full. In applications requiring a high response speed, this function is especially important.

In the interface view, perform the following task.

**Table 250** Specify/Cancel packet pre-acknowledgement

| Operation                          | Command                                             |
|------------------------------------|-----------------------------------------------------|
| Set packet acknowledgment value    | <b>x25 receive-threshold</b><br><b>packet-count</b> |
| Cancel packet acknowledgment value | <b>undo x25 receive-threshold</b>                   |

By default, the number of pre-acknowledged packets is 0.

#### 4 Configure X.25 user facility

X.25 protocol defines various user facility options. The user can choose and configure the facilities. These configurations can be modified in two ways:

Configuration based on X.25 interface (use "**x25 call-facility.....**" command); configuration based on address mapping (use "**x25 map.....**" command).

The configuration based on X.25 interface will be effective in every call originated from this X.25 interface, while the configuration based on address mapping will be effective only in the calls originated from this address mapping.

In the interface view, perform the following task.

**Table 251** Configure X.25 user facility

| Operation                                                          | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Specify CUG (Closed User Group)                                    | <b>x25 call-facility</b><br><b>closed-user-group group-number</b><br>Or<br><b>x25 map protocol protocol-address</b><br><b>x121-address x.121-address</b><br><b>closed-user-group group_number</b>                                                                                                                                                                                                                                                      |
| Cancel CUG number                                                  | <b>undo x25 call-facility</b><br><b>closed-user-group</b>                                                                                                                                                                                                                                                                                                                                                                                              |
| Perform flow control parameter negotiation while initiating a call | <b>x25 call-facility packet-size</b><br><b>in-size out-size <sup>1</sup></b><br>Or<br><b>x25 map protocol protocol-address</b><br><b>x121-address x.121-address</b><br><b>packet-size in-size out-size <sup>1</sup></b><br><br><b>x25 call-facility window-size</b><br><b>in-size out-size <sup>1</sup></b><br>Or<br><b>x25 map protocol protocol-address</b><br><b>x121-address x.121-address</b><br><b>window-size in-size out-size <sup>1</sup></b> |
| Cancel flow control parameter negotiation while initiating a call  | <b>undo x25 call-facility packet-size</b><br>Or<br><b>undo x25 call-facility window-size</b>                                                                                                                                                                                                                                                                                                                                                           |
| Request reverse charging while initiating a call                   | <b>x25 call-facility</b><br><b>reverse-charge-request</b><br>Or<br><b>x25 map protocol protocol-address</b><br><b>x121-address x.121-address</b><br><b>reverse-charge-request</b>                                                                                                                                                                                                                                                                      |
| Cancel the request of reverse charging while initiating a call     | <b>undo x25 call-facility</b><br><b>reverse-charge-request</b>                                                                                                                                                                                                                                                                                                                                                                                         |

|                                                                            |                                                                                                                                                                     |
|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Receive calls with reverse charging requests                               | <b>x25 reverse-charge-accept</b><br>Or<br><b>x25 map protocol protocol-address<br/>x121-address x.121-address<br/>reverse-charge-accept</b>                         |
| Request throughput-level negotiation while initiating a call               | <b>x25 call-facility threshold in out</b><br>Or<br><b>x25 map protocol protocol-address<br/>x121-address<br/>x.121-addresssthreshold in out</b>                     |
| Cancel the request of throughput-level negotiation while initiating a call | <b>undo x25 call-facility threshold</b>                                                                                                                             |
| Carry transmission delay request while initiating a call                   | <b>x25 call-facility send-delay<br/>milliseconds</b><br>Or<br><b>x25 map protocol protocol-address<br/>x121-address x.121-address<br/>send-delay milliseconds</b>   |
| Cancel the carrying of transmission delay request while initiating a call  | <b>undo x25 call-facility send-delay</b>                                                                                                                            |
| Specify the use of ROA (Recognized operating Agency)                       | <b>x25 call-facility roa-name name <sup>2</sup></b><br>Or<br><b>x25 map protocol protocol-address<br/>x121-address x.121-address<br/>roa-name name <sup>2</sup></b> |
| Cancel the use of ROA                                                      | <b>undo x25 call-facility roa-name</b>                                                                                                                              |

**window-size** and **packet-size** options are also supported in **x25 pvc** command. However, in **x25 pvc** command, these two options specify the window size and maximum packet length of the set PVC. If these two options are not selected in the **x25 pvc** command, the set PVC will choose the default value of X.25 interface.

*name* is the name of the ROA ID list configured by the command **x25 roa-list** in the system view, for example:

```
[Router]x25 roa-list list1 12 34 567
```

In the serial port view, list1 can be quoted:

```
[Router-Serial0]x25 call-facility roa-name list1
```

## 5 Configure the sending queue length of virtual circuit

The sending and receiving queue lengths of the virtual circuit can be specified for the X.25 of the 3Com Router series to adapt to different network environments. The default queue length can contain 500 packets, but if data flow is very large, or the transmission rate of the X.25 network is low, the queue length can be increased to avoid unexpected data packet loss.

In the interface view, perform the following tasks to specify the length of virtual circuit queue.

**Table 252** Configure the sending queue length of virtual circuit

| Operation                                           | Command                                |
|-----------------------------------------------------|----------------------------------------|
| Set the length of X.25 virtual circuit queue        | <b>x25 queue-length<br/>queue-size</b> |
| Cancel set the length of X.25 virtual circuit queue | <b>undo x25 queue-length</b>           |

## 6 Broadcast via X.25

Generally, inter-network protocols will need to send some broadcast datagrams for specific purposes. On the broadcasting physical networks (such as Ethernet), such requirements are naturally supported. But for non-broadcasting networks like X.25, how to realize the broadcasting?

The X.25 of the 3Com Router series can enable this to decide if the broadcast packet should be duplicated and sent to a destination. This is very important. For instance, the broadcast-based application layer routing protocol will request broadcasting datagram sent by X.25 to exchange routing information on the X.25 network.

It can be specified whether to send broadcasting data packets on the related virtual circuits of both SVC and PVC.

**Table 253** Set broadcast via X.25

| Operation                                                                                            | Command                                                                                  |
|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Enable to send broadcasting data packets to the peer of the SVC associated with this address mapping | <b>x25 map protocol protocol-address x121-address x.121-address broadcast</b>            |
| Enable to send broadcasting data packets to the peer of this PVC                                     | <b>x25 pvc pvc-number protocol protocol-address x121-address x.121-address broadcast</b> |

## 7 Restrict the use of address mapping

X.25 calls are closely related to address mapping: before a destination is called, this destination must be found in the address mapping table. Before a call is received, the source of this call must also be found in the address mapping table. But in some cases, some address mappings are used for calling out only, while others are used for calling in only.

The X.25 of the 3Com Router series allows restricting the use of this address mapping addition by adding some option items, as shown in the following table.

**Table 254** Restrict the use of address mapping

| Operation                                          | Command                                                                        |
|----------------------------------------------------|--------------------------------------------------------------------------------|
| Inhibit outgoing call through this address mapping | <b>x25 map protocol protocol-address x121-address X.121-address no-callout</b> |
| Inhibit incoming call through this address mapping | <b>x25 map protocol protocol-address x121-address X.121-address no-calling</b> |

## 8 Configure interface with standby center

The powerful standby function of the 3Com Router series is provided by the "standby center". To add an X.25 interface into the standby center, perform the following task in the interface view.

**Table 255** Set interface with standby center

| Operation                                                                      | Command                                                                                                    |
|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Set the logical interface number of this address mapping in the standby center | <b>x25 map protocol protocol-address x121-address x.121-address logic-channel logical-interface-number</b> |

### Configure X.25 Sub-Interface

X.25 sub-interface is a virtual interface with its own protocol address and virtual circuit. Multiple sub-interfaces can be created on a physical interface, so the networks can be interconnected via one physical interface. The sub-interface of X.25 falls into two types: point-to-point sub-interface, used to connect a single remote end and point-to-multipoint sub-interface, used to connect multiple remote ends in the same network segment. All the sub-interfaces under the main interface and the main interface share a X.121 address.

In the interface view, perform the following task to configure X.25 sub-interface.

**Table 256** Configure X.25 sub-Interface

| Operation                                                              | Command                                                                                                                                                                                   |
|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enter X.25 interface                                                   | <code>interface serial number</code>                                                                                                                                                      |
| Configure X.25 protocol                                                | <code>link-protocol x25</code>                                                                                                                                                            |
| Create X.25 sub-interface                                              | <code>interface serial number.subinterface-number{multipoint point-to-point}</code>                                                                                                       |
| Configure address mapping<br>Or<br>Configure permanent virtual circuit | <code>x25 map protocol protocol-address x121-address x.121-address [option]</code><br>or<br><code>x25 pvc pvc-number protocol protocol-address x121-address x.121-address [option]</code> |

### Configure X.25 Switching

#### X.25 Switching Function

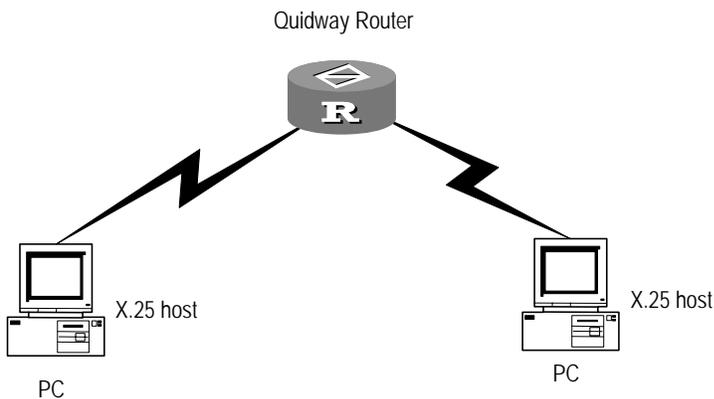
A packet network consists of many nodes interconnected in a certain topological structure. From the source to its destination, a packet will pass through many nodes, each of which must have packet switching capability.

X.25 packet switching means to receive packets from one X.25 port, and send them out from the X.25 port selected according to related destination address information contained in the packets. X.25 switching enables the 3Com Router series to perform packet switching function in the packet layer, and to be used as a small packet switching exchange.

The 3Com Router series provides such X.25 switching functions as follows:

- SVC switching function
- Support parameter negotiation on window size and packet size
- PVC switching

The following describes how to configure X.25 switching tables for PVC and SVC.

**Figure 64** X.25 switching networking diagram**1** Enable or disable X.25 switching

In the system view, perform the following task to enable or disable X.25 switching.

**Table 257** Enable or disable X.25 switching

| Operation              | Command                         |
|------------------------|---------------------------------|
| Enable X.25 switching  | <code>x25 switching</code>      |
| Disable X.25 switching | <code>undo x25 switching</code> |

Add or delete a PVC route

**Table 258** Add or delete a PVC route

| Operation          | Command                                                                    |
|--------------------|----------------------------------------------------------------------------|
| Add a PVC route    | <code>x25 switch pvc number interface serial port-number pvc number</code> |
| Delete a PVC route | <code>undo x25 switch pvc number</code>                                    |

After configuration, the `display x25 switch-vc-table pvc` command can be used to show the virtual circuit route table.

**2** Add/Delete an SVC route

In the system view, the commands in the following table can be used to add or delete an SVC route.

**Table 259** Add or delete an SVC route

| Operation           | Command                                                                                                                                             |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Add an SVC route    | <code>x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] interface serial interface-number</code>          |
| Delete an SVC route | <code>undo x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] [ interface serial interface-number ]</code> |

After the configuration, use `display x25 switch-vc-table svc` command to display the switching route table.

## Configure X.25 Load Balancing

### Introduction to X.25 Load Balancing

Using the property of hunt group of X.25 protocol, ISPs can provide load balancing function in X.25 packet switching networks. X.25 load balancing can implement the load balancing in different DTEs or different links of a single DTE,

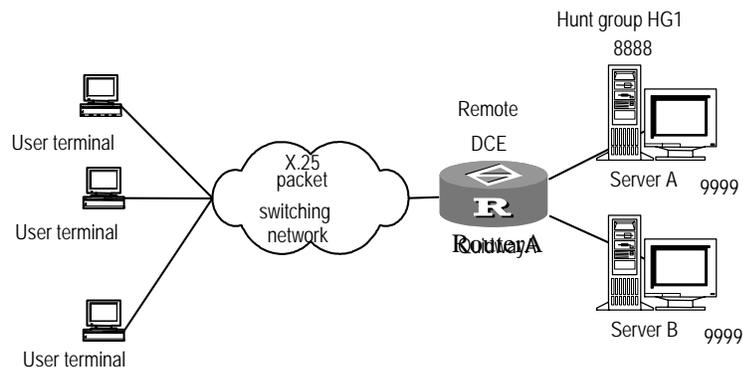
which guarantees no occurrence of link overload when an address is accessed by a large number of subscribers.

X.25 load balancing is provided by DCEs. In order to implement the load balancing in X.25 networks, a group of DTE/DCE interfaces (synchronous serial interfaces or XOT Tunnels) need to be configured at the remote DCE on the network as a hunt group. And it is necessary to allocate an X.121 address to such hunt group. When other equipment in the network accesses the DTE inside the hunt group, they need to call the hunt group address. After receiving the call request packets, the remote DCE will, according to diverse channel selection policies (round-robin or vc-number), select a line in the hunt group and send the incoming call packets. Different calls will be allocated to the lines in the hunt group, thus achieving load balancing.

It should be noted that X.25 hunt group can dynamically select different transmission lines only in the process of the establishment of virtual circuit call. Once the whole virtual circuit is established and enters into the stage of data transmission, hunt group will be ineffective and data transmission will be processed in accordance with the normal virtual circuit. After being established, PVC stays at the data transmission stage without the process of call establishment and call deletion, therefore X.25 load balancing is ineffective on PVC and functions only on SVC.

Within a single X.25 hunt group, all DTEs hold identical status and have the same X.121 addresses. The DTEs in a hunt group can call other DTEs outside the hunt group in a normal mode. When equipment outside the hunt group access the hunt group, they cannot know which equipment they will access, because the line selection is controlled by the DCEs configured with hunt group.

DTE addresses in a hunt group may be identical or different to the hunt group addresses. X.25 hunt group supports the substitutions of source address and destination address. The function of destination address substitution enables us to hide the addresses of DTEs inside the hunt group, thus external DTEs only know the hunt group address, which enforces the security of the internal network of hunt group. The function of source address substitution can hide the addresses of DTEs outside a hunt group, therefore internal DTEs can only know the substituted source address instead of the source address a call is connected to, which protects subscribers' privacy.

**Figure 65** Diagram of X.25 network load balancing

As shown in the above figure, Server A and Server B concurrently provide subscribers with identical services. They are configured as a hunt group named hg1. Server A and Server B have the same address of 9999 and the hunt group address is 8888. Enable the function of destination address substitution on Router RouterA for changing calls connected to address 8888 to calls connected to address 9999. When a subscriber processes a service, the subscriber terminal will send a call to the destination address 8888. The calls from various terminals will be substituted on the router RouterA with the calls to 9999 and transmitted to Server A and Server B respectively. Thus load balancing is realized between Server A and Server B, and the pressure on a single server is decreased.

X.25 hunt group supports two types of call channel selection policies: round-robin mode and vc-number mode, but a hunt group can only utilize one type of channel selection policy.

- In round-robin mode, cyclic selection method is adopted to select the next interface or the XOT Tunnel for every call request. For example, as shown in Figure1-1, if hunt group hg1 adopts rotary mode, calls will be sent to Server A and Server B by turns.
- vc-number mode selects the interfaces with the free logical channels in a hunt group for every call request. For example, as shown in the above Figure1-1, if hunt group hg1 adopts vc-number mode, there will be 500 residual logical channels in the lines between Server A and DCE and 300 residual logical channels in the lines between Server B and DCE. Thus all the first 200 calls will be sent to Server A, and the calls following the first 200 ones will be sent to Server A and Server B by turns.

X.25 hunt group supports synchronous serial interfaces and XOT Tunnels. It can indiscriminately select the available lines between synchronous serial interfaces and XOT Tunnels. But XOT Tunnels cannot calculate the number of logical channels, therefore it cannot be added into a hunt group adopting vc-number selection policy.

### List of Configuration Tasks of X.25 Load Balancing

The load balancing of X.25 networks is configured on DCE equipment. The 3Com Router is generally utilized as a DTE equipment in X.25 networks. If load balancing is provided by ISPs on packet switching exchanges, routers need no special configuration. The specific configuration procedure can be seen in the previous chapters. If the 3Com Router is used as an X.25 switching exchange (it serves as a

DCE equipment in X.25 networks to provide the function of load balancing for DTE equipment) then configuration of X.25 load balancing needs to be made on the routers.

The main configuration tasks of X.25 load balancing are as follows:

- Start X.25 switching
- Create X.25 hunt group
- Add interfaces and XOT Tunnels to hunt group
- Configure the X.25 switching route whose forward address is hunt group
- Configure other X.25 switching routes



*Hunt group addresses do not need separate configuration. Only the destination addresses need to be set as hunt group addresses on source DTEs.*

#### 1 Start X.25 switching

Perform the following configuration in system view.

**Table 260** Start /Close X.25 switching function

| Operation             | Command                   |
|-----------------------|---------------------------|
| Start X.25 switching  | <b>x25 switching</b>      |
| Close X. 25 switching | <b>undo x25 switching</b> |

#### 2 Create X.25 hunt group

Perform the following configuration in system view.

**Table 261** Create/Delete X.25 hunt group

| Operation              | Command                                                               |
|------------------------|-----------------------------------------------------------------------|
| Create X.25 hunt group | <b>x25 hunt-group hunt-group-name {<br/>round-robin   vc-number }</b> |
| Delete X.25 hunt group | <b>undo x25 hunt-group hunt-group-name</b>                            |

#### 3 Add interfaces and XOT Tunnels to hunt group

Perform the following configuration in X.25 hunt group view.

**Table 262** Add/Delete interfaces or XOT Tunnels in hunt group

| Operation                                    | Command                                                           |
|----------------------------------------------|-------------------------------------------------------------------|
| Add interfaces to hunt group                 | <b>channel interface interface-type<br/>interface-number</b>      |
| Delete specified interfaces from hunt group  | <b>undo channel interface<br/>interface-type interface-number</b> |
| Add XOT Tunnels to hunt group                | <b>channel xot ip-address</b>                                     |
| Delete specified XOT Tunnels from hunt group | <b>undo channel xot ip-address</b>                                |

It should be noted that a hunt group can have ten synchronous serial interfaces or XOT Tunnels at most. XOT Tunnels cannot be added to the hunt group that adopts vc-number channel selection policy.

#### 4 Configure X.25 switching route which is forwarded to hunt group

Perform the following configuration in system view.

**Table 263** Add/Delete X.25 switching route whose forwarding address is hunt group

| Operation                                                             | Command                                                                                                                                      |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Add an X.25 switching route whose forwarding address is hunt group    | <code>x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] hunt-group hunt-group-name</code>          |
| Delete an X.25 switching route whose forwarding address is hunt group | <code>undo x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] [ hunt-group hunt-group-name ]</code> |

## 5 Configure other X.25 switching routes

**Table 264** Add/delete other X.25 switching routes

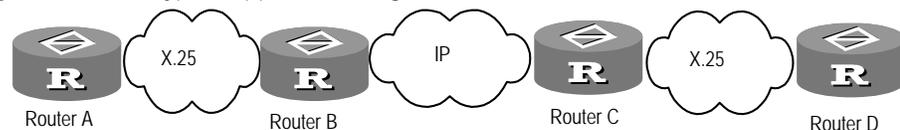
| Operation                                                             | Command                                                                                                                                                                              |
|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add an X.25 switching route whose forwarding address is interface     | <code>x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] interface serial interface-number</code>                                           |
| Delete an X.25 switching route whose forwarding address is interface  | <code>undo x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] [ interface serial interface-number ]</code>                                  |
| Add an X.25 switching route whose forwarding address is XOT Tunnel    | <code>x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] xot ip-address1 [ ip-address2 ] ... [ ip-address6 ] [ xot-option ]</code>          |
| Delete an X.25 switching route whose forwarding address is XOT Tunnel | <code>undo x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] [ xot ip-address1 [ ip-address2 ] ... [ ip-address6 ] ] [ xot-option ]</code> |

## Configure X.25 over Other Protocols

### Configure X.25 over TCP (XOT)

#### Introduction to XOT Protocol

XOT (X.25 Over TCP) is a protocol that is supported by TCP, and implements the connection of two X.25 networks through IP network. The practical application environment is shown in the following figure.

**Figure 66** XOT typical application diagram

Since the application of IP network is broader and broader, the practical applications of supporting X.25 data through IP net and connecting X.25 networks are becoming more and more. The conventional X.25 protocol is the third layer of the OSI seven-layer model, i.e., the network layer, for which the LAPB

protocol provides reliable data transmission link. Because TCP has the mechanism of error redirection and window flow controlling to guarantee the reliability of links, it can be used by X.25. XOT builds a TCP tunnel connection between the two X.25 networks, and the X.25 packets are supported by TCP as data of application layer, i.e., TCP serves as the “link layer” of X.25. You can regard the middle RouterB, RouterC and IP net as a big “X.25 switch”, and data is directly switched from RouterA to RouterD through this “switch”.

The XOT features implemented in the 3Com Router accords with RFC1613 recommendation, and it possess the following features:

- Supporting SVC application. The two routers can dynamically set up a SVC by sending call packet, and the VC will automatically be cleared when no data is transmitted.
- Supporting PVC application. After the two routers configure a PVC, they directly enter the data transmission status without the process of call establishing. If no data is transmitted, this VC will not be cleared automatically.
- Supporting the Keepalive attribute of TCP. If Keepalive is not configured, TCP connection will not be cleared after a long period of time when the line is disconnected. If Keepalive is configured, TCP check the usability of the links in time, and it will automatically clear the TCP connection if it does not receive the answer of the opposite side for certain times.

Implementing theory of XOT (taking SVC as an example):

As shown in the former figure, when it has data to transmit, RouterA first send a request packet to set up a VC. After RouterB receive the call packet and judges that it is XOT application, it first set up a TCP connection with RouterC, and then stick the XOT packet header to X.25 call packet which is encapsulated in TCP header to send to RouterC. RouterC takes off the TCP and XOT packet headers and send the call request packet to RouterD through X.25 local switch. After RouterD receives the call request packet, it answers the call to confirm until the link is completely set up and enters the data transmission status. To RouterA and RouterD, the whole process of setting up and applying TCP connection is transparent, and they do not and cannot care whether the data is forwarded through IP net or X.25 net.

### Configure XOT

XOT configuration includes:

- Start X.25 switching
- Configure IP side interface
- Configure local switching (SVC)
- Configure XOT route
- Configure Keepalive and xot-source attributes
- Start X.25 switching

Because the XOT is the extension of X.25 switch, first you have to start X.25 switch.

Perform the following tasks in system view.

**Table 265** Start X.25 switching

| Operation             | Command                    |
|-----------------------|----------------------------|
| Enable X.25 switching | <code>x25 switching</code> |

- 1 By default, do not start X.25 switch.
- 2 Configure IP side interface

Because the XOT implements the connection of two X.25 nets through IP net, first you should ensure that the IP net is expedite. For the specific configuration, refer to chapters of *Operation Manual - Network protocol*.

- 3 Configure local switching (SVC)

For SVC, when it receives the packets from the remote side, it must send out the packets through local switch interface, so you have to configure local switching.

The following commands determine: In SVC, through which switch interface the packets getting to local side will be sent out.

Perform the following tasks in system view.

**Table 266** Configure local switching

| Operation                      | Command                                                                                                                                             |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure X.25 local switching | <code>x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] interface serial interface-number</code>          |
| Delete X.25 local switching    | <code>undo x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] [ interface serial interface-number ]</code> |

- 4 Configure XOT route

The following configuration determines how the X.25 side packets received are forwarded through IP net. There are different views for SVC and PVC.

For SVC, perform the following tasks in system view.

**Table 267** Configure SVC XOT switching

| Operation                 | Command                                                                                                                                                                              |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure a SVC XOT route | <code>x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] xot ip-address1 [ ip-address2 ] ... [ ip-address6 ] [ xot-option ]</code>          |
| Delete a SVC XOT route    | <code>undo x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] [ xot ip-address1 [ ip-address2 ] ... [ ip-address6 ] ] [ xot-option ]</code> |



*The local X.25 route must be configured in the SVC mode.*

For PVC, perform the following tasks in interface view.

**Table 268** Configure PVC XOT switching

| Operation              | Command                                                        |
|------------------------|----------------------------------------------------------------|
| Add a PVC XOT route    | <b>x25 xot pvc pvc-number ip address interface type number</b> |
| Delete a PVC XOT route | <b>undo x25 xot pvc pvc-number</b>                             |

### 5 Configure Keepalive and xot-source attributes

After the TCP link is established, TCP will not be easily cleared even if the link is disconnected. But after configuring Keepalive, the router will send checking packets in time to check the usability of the link. If it cannot get confirmation after sending out packets several times, it will consider the link failure and clear it automatically.

**Table 269** Configure Keepalive and xot-source attributes

| Operation                                         | Command                                                                                                                                                                        |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure SVC Keepalive and xot-source attributes | <b>x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] xot ip-address1 [ ip-address2 ] ... [ ip-address6 ] [ xot-option ]</b>          |
| Configure PVC Keepalive and xot-source attributes | <b>undo x25 switch svc x.121-address [ sub-dest destination-address ] [ sub-source source-address ] [ xot ip-address1 [ ip-address2 ] ... [ ip-address6 ] ] [ xot-option ]</b> |

## Configure X.25 over Frame Relay (Annex G)

### Configure Annex G Data Interoperation

ANSI T1.617 Annex G defines how to transmit X.25 packets over Frame Relay DCLIs. With the integrated acknowledgement, retransmission and flow control mechanisms of X.25, Annex G DLCI can provide reliable transmission service, as well as interconnect X.25 networks via Frame Relay networks. Annex G is a stopgap between X.25 network and Frame Relay network, which can effectively protect the investment that the user has made.

This section covers how to make configurations so that Annex G DLCI can be used to transmit IP data. For the configurations of X.25 switching over Annex G DLCIs, refer to the subsequent section.

**Table 270** Configure an Annex G DLCI

| Operation                                                 | Command                                      |
|-----------------------------------------------------------|----------------------------------------------|
| Configure a Frame Relay interface                         | <b>link-protocol fr</b>                      |
| Configure an IP address for the interface                 | <b>ip address { A.B.C.D } { A.B.C.D }</b>    |
| Configure a Frame Relay DLCI                              | <b>fr dlci dlci-number</b>                   |
| Configure the Frame Relay DLCI to be Annex G DLCI         | <b>annexg { dce   dte }</b>                  |
| Map the Frame Relay address to the destination IP address | <b>fr map ip { A.B.C.D } { dlci-number }</b> |



*Annex G DLCI does not support IARP (Inverse Address Resolution Protocol), so the user should configure a static map between the destination IP address and the Frame Relay address.*

When configuring an Annex G DLCI, the user must explicitly configure it with the argument **DCE** or **DTE**. In addition, the configurations on the routers of a connection should not be the same. That is, if a router is configured to work as DTE, the other router must be configured as DCE.

**Table 271** Configure the X.25 attributes for an Annex G DLCI

| Operation                                                                           | Command                                                            |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Create an X.25 template                                                             | <b>x25 template { name }</b>                                       |
| Configure the local X.25 address in the X.25 template                               | <b>x25 x121-address x.121 address</b>                              |
| Map the destination X.25 address to the destination IP address in the X.25 template | <b>x25 map ip { A.B.C.D } { x121-address x.121 address }</b>       |
| Configure other LAPB/X.25 parameters in the X.25 template                           | <b>For details, refer to the LAPB/X.25 configuration commands.</b> |
| Associate the parameters configured in the X.25 template to an Annex G DLCI         | <b>x25-template { name }</b>                                       |



*It is necessary to properly understand the differences between the Frame Relay address map configured in interface view and the X.25 address map configured in X.25 template view. The former specifies the DLCI from which the packets destined to an IP address can be sent, whereas the latter specifies the X.25 address to which the packets must originate X.25 calls in order to reach the destination IP address. IP packets can be properly sent and received on the Annex G DLCI only if the two address maps are configured.*



*The LAPB/X.25 attributes configured in an X.25 template and those configured on an X.25 interface are similar. To ensure that an X.25 call can be set up, the configurations on the routers of a connection should keep in consistency.*

#### 1 Configure the X.25 Attributes for a DLCI

Frame Relay is mainly applied to data transmission. However, it does not provide acknowledgement mechanism or error correction function. In other words, transmission over Frame Relay networks is unreliable. To ensure reliable transmission of signals for call set up and termination in dynamic calling mode, these signals are transmitted over an X.25 VC (Virtual Circuit). Thereby, reliable transmission can be ensured through the X.25 message acknowledgement mechanism. A DLCI needs to be configured with X.25 attributes only when VoFR (Voice over Frame Relay) adopts dynamic calling mode.

The **x.25 template** command is performed in system view. Creating an X.25 template will enter x.25 template mode at the same time. Perform the commands **x25** and **lapb** in x.25 template mode, and **x25-template** in interface DLCI mode.

**Table 272** Configure the X.25 attributes for an DLCI

| Operation                                                     | Command                     |
|---------------------------------------------------------------|-----------------------------|
| Create an X.25 template                                       | <b>x25 template name</b>    |
| Delete the X.25 template                                      | <b>no x25 template name</b> |
| Configure the X.25 attributes                                 | <b>x25</b>                  |
| Restore the X.25 attributes to default settings               | <b>no x25</b>               |
| Configure the LAPB attributes                                 | <b>lapb</b>                 |
| Restore the LAPB attributes to default settings               | <b>no lapb</b>              |
| Associate the X.25 template with a DLCI                       | <b>x25-template name</b>    |
| Remove the association between the X.25 template and the DLCI | <b>no x25-template</b>      |

By default, X.25 template is not applied on DLCIs.

## Display and Debug LAPB and X.25

In the all views, perform the following tasks to enable real-time monitoring of the current status of LAPB and X.25.

**Table 273** Display and debug LAPB and X.25

| Operation                                    | Command                                                                        |
|----------------------------------------------|--------------------------------------------------------------------------------|
| Display interface information                | <code>display interface [ type number ]</code>                                 |
| Display X.25 alias table                     | <code>display x25 alias-policy</code>                                          |
| Display X.25 hunt group information          | <code>display x25 hunt-group-info [ hunt-group-name ]</code>                   |
| Display X.25 address mapping table           | <code>display x25 map</code>                                                   |
| Display X.25 switching route table           | <code>display x25 switch-vc-table svc</code>                                   |
| Display X.25 switching virtual circuit table | <code>display x25 switch-vc-table pvc</code>                                   |
| Display X.25 virtual circuit                 | <code>display x25 vc lci-number</code>                                         |
| Enable X.25 information debugging            | <code>debugging x25 all [interface interface-type interface-number ]</code>    |
| Enable X.25 event debugging                  | <code>debugging x25 event [interface interface-type interface-number ]</code>  |
| Enable X.25 packet debugging                 | <code>debugging x25 packet [interface interface-type interface-number ]</code> |
| Enable XOT debugging                         | <code>debugging x25 xot</code>                                                 |

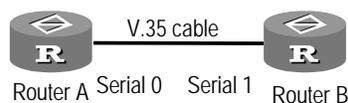
## Typical LAPB Configuration Example

### I. Networking Requirement

Two routers are directly connected via serial ports with LAPB protocol to transmit IP data packets directly.

### II. Networking Diagram

**Figure 67** Direct connection between two routers via serial ports



### III. Configuration Procedure

As shown in the diagram above, perform the following configuration tasks:

**1** Configure Router A:

**a** Select interface

```
[Router] interface serial 0
```

**b** Specify IP address for this interface

```
[Router-Serial0] ip address 202.38.160.1 255.255.255.0
```

**c** Configure the link layer protocol of the interface to LAPB and specify its working mode as DTE

```
[Router-Serial0] link-protocol lapb dte
```

**d** Configure other Lapb parameters (if the link is of good quality, and a higher rate is required, the flow control parameter modulo can be increased to 128, k to 127, but they must be the same for both ends in the direct connection)

```
[Router-Serial0]lapb module 128
[Router-Serial0]lapb window-size 127
```

## 2 Configure Router B:

### a Select interface

```
[Router]configure
[Router]interface serial 1
```

### b Specify IP address for this interface

```
[Router-Serial1]ip address 202.38.160.2 255.255.255.0
```

### c Configure the link layer protocol of the interface to LAPB and specify its working mode as DCE

```
[Router-Serial1]link-protocol lapb dce
```

### d Configure other LAPB parameters (if the link quality is good, and a higher rate is required, the flow control parameter modulo can be increased to 128, k to 127, but they must be the same for both ends in the direct connection)

```
[Router-Serial1]lapb modulo 128
[Router-Serial1]lapb window-size 127
```

---

## Typical X.25 Configuration Example

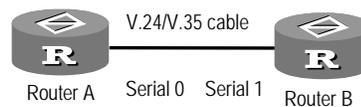
### Back to Back Direct Connection of Two Routers via Serial Interface

#### I. Networking Requirement

As shown in the diagram below, two routers are to be directly connected back to back; the X.25 protocol is used between the serial ports for IP data packet transmission.

#### II. Networking Diagram

**Figure 68** Direct connection of two routers via serial ports



#### III. Configuration Procedure

## 1 Configure Router A:

### a Select interface

```
[Router]interface serial 0
```

### b Specify IP address for this interface

```
[Router-Serial0]ip address 202.38.160.1 255.255.255.0
```

### c Configure the link layer protocol of the interface to X.25 and specify its working mode as DTE

```
[Router-Serial0]link-protocol x25 dte
```

### d Specify X.121 address of this interface

```
[Router-Serial0]x25 x121-address 20112451
```

- e Specify address mapping to the peer

```
[Router-Serial0]x25 map ip 202.38.160.2 x121-address 20112452
```

- f As this is a direct connection, the flow control parameters can be increased slightly

```
[Router-Serial0]x25 packet-size 1024 1024
```

```
[Router-Serial0]x25 window-size
```

## 2 Configure Router B:

- a Select interface

```
[Router]interface serial 1
```

- b Specify IP address for this interface

```
[Router-Serial1]ip address 202.38.160.2 255.255.255.0
```

- c Configure the link layer protocol of the interface to X.25 and specify its working mode as DCE

```
[Router-Serial1]link-protocol x25 dce
```

- d Specify X.121 address of this interface

```
[Router-Serial1]x25 x121-address 20112452
```

- e Specify address mapping to the peer

```
[Router-Serial1]x25 map ip 202.38.160.1 x121-address 20112451
```

- f As this is a direct connection, the flow control parameters can be increased slightly

```
[Router-Serial1]x25 packet-size 1024 1024
```

```
[Router-Serial1]x25 window-size 5 5
```

## Connect the Router to X.25 Public Packet Network

### I. Networking Requirement

As shown in the diagram below, three routers A, B and C are connected to the same X.25 network for mutual communication. The requirements are:

- IP addresses of the interfaces Serial0 of three routers are 168.173.24.1, 168.173.24.2 and 168.173.24.3 respectively.
- X.121 addresses assigned to the three routers by the network are 30561001, 30561002 and 30561003 respectively.
- Standard window size supported by the packet network: both receiving window and sending window are 5.
- Standard maximum packet length: both maximum receiving packet length and maximum sending packet length are 512.
- Channel range: permanent virtual circuit section, incoming-only channel section and outgoing-only channel section are disabled, two-way channel section is [1, 31].

## II. Networking Diagram

**Figure 69** Connect the router to X.25 public packet network



## III. Configuration Procedure

### 1 Configure Router A:

#### a Configure interface IP address

```
[Router]interface Serial 0
[Router-Serial0]ip address 168.173.24.1 255.255.255.0
```

#### b Connect to public packet network, make the router as DTE side

```
[Router-Serial0]link-protocol x25 dte
[Router-Serial0]x25 x121-address 30561001
[Router-Serial0]x25 window-size 5 5
[Router-Serial0]x25 packet-size 512 512
[Router-Serial0]x25 map ip 168.173.24.2 x121-address 30561002
[Router-Serial0]x25 map ip 168.173.24.3 x121-address 30561003
```

### 2 Configure Router B:

#### a Configure interface IP address

```
[Router]configure
[Router]interface Serial 0
[Router-Serial0]ip address 168.173.24.2 255.255.255.0
```

#### b Connect to public packet network, make the router as DTE side

```
[Router-Serial0]link-protocol x25 dte
[Router-Serial0]x25 x121-address 30561002
[Router-Serial0]x25 window-size 5 5
[Router-Serial0]x25 packet-size 512 512
[Router-Serial0]x25 map ip 168.173.24.1 x121-address 30561001
[Router-Serial0]x25 map ip 168.173.24.3 x121-address 30561003
```

### 3 Configure Router C:

#### a Configure interface IP address

```
[Router]interface Serial 0
[Router-Serial0]ip address 168.173.24.3 255.255.255.0
```

#### b Connect to public packet network, make the router as DTE side

```
[Router-Serial0]link-protocol x25 dte
[Router-Serial0]x25 x121-address 30561003
[Router-Serial0]x25 window-size 5 5
[Router-Serial0]x25 packet-size 512 512
```

```
[Router-Serial0]x25 map ip 168.173.24.1 x121-address 30561001
[Router-Serial0]x25 map ip 168.173.24.2 x121-address 30561002
```

### Configure Virtual Circuit Range

#### I. Networking Requirement

The link layer protocol of router's interface Serial0 is X.25I, with the virtual circuit range: permanent virtual circuit section [1, 8], incoming-only channel section [9, 16], two-way channel section [17, 1024], and the outgoing-only channel section is disabled.

#### II. Configuration Procedure

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25
[Router-Serial0]x25 vc-range in-channel 9 16 bi-channel 17 1024
```

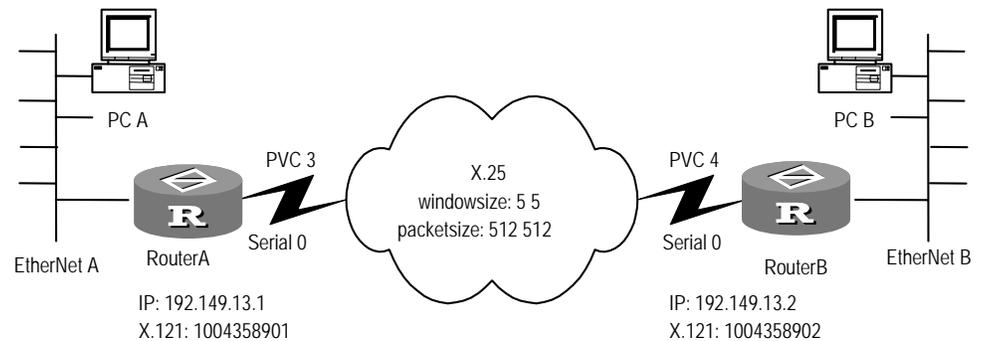
### Transmit IP Datagram via X.25 PVC

#### I. Networking Requirement

In the following diagram, the permanent virtual circuit section allowed by the packet network is [1,8], the PVC numbers assigned to Router A and Router B are 3 and 4 respectively. The IP network addresses of Ethernet A and B are 202.38.165.0 and 196.25.231.0 respectively. It is required to exchange routing information between Ethernet A and B with RIP routing protocol, so that PC A and PC B can exchange information without adding static route.

#### II. Networking Diagram

Figure 70 X.25 PVC bearing IP data packet



#### III. Configuration Procedure

##### 1 Configure Router A:

```
[Router]interface ethernet 0
[Router-Ethernet0]ip address 202.38.165.1 255.255.255.0
[Router-Ethernet0]interface serial 0
[Router-Serial0]ip address 192.149.13.1 255.255.255.0
[Router-Serial0]link-protocol x25
[Router-Serial0]x25 x121-address 1004358901
[Router-Serial0]x25 vc-range bi-channel 9 1024
[Router-Serial0]x25 pvc 3 ip 192.149.13.2 x121-address 1004358902
broadcast packet-size 512 512 window-size 5 5
[Router-Serial0]quit
[Router]rip
```

##### 2 Configure Router B:

```
[Router]interface ethernet 0
```

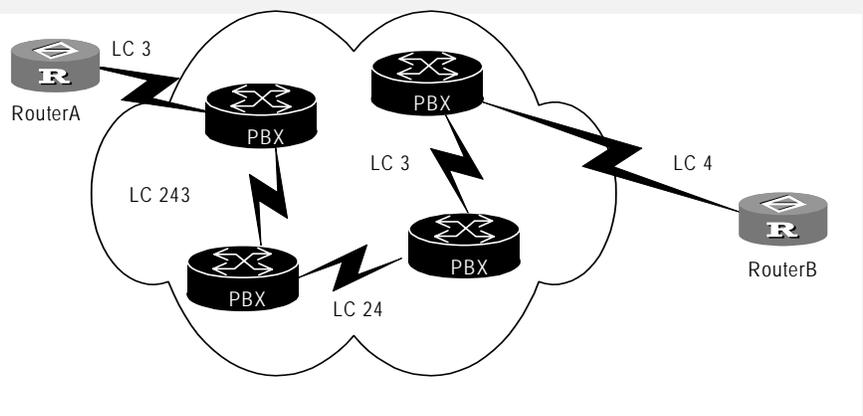
```

[Router-Ethernet0]ip address 196.25.231.1 255.255.255.0
[Router-Ethernet0]interface serial 0 [Router-Serial0]ip address
192.149.13.2 255.255.255.0
[Router-Serial0]link-protocol x25
[Router-Serial0]x25 x121-address 1004358902
[Router-Serial0]x25 vc-range bi-channel 8 1024
[Router-Serial0]x25 pvc 4 ip 192.149.13.1 x121-address 1004358901
broadcast packet-size 512 512 window-size 5 5
[Router-Serial0]quit
[Router]rip

```

In above configuration, the permanent virtual circuit numbers of routers A and B are different: 3 and 4 respectively. Virtual circuit refers to the end-to-end logical link between the calling DTE and the called DTE, while logical channel refers to the logical link between two directly connected devices (either between DTE and DCE, or between the ports of two packet switching exchanges). A virtual circuit consists of several logical channels, and each logical channel has a separate number. The virtual circuit between routers A and B is shown in (suppose this virtual circuit passes four packet switching exchanges in the network).

**Figure 71** A virtual circuit consisting of several logical channels



Therefore, the PVC 3 and PVC 4 mentioned above actually refer to the numbers of the logical channels between the router and the switch directly connected to it. However, on one side of this virtual circuit, the logical channel number can be used to identify this virtual circuit without causing misunderstanding. This is why no strict distinction is made between "virtual circuit" and "logical channel".

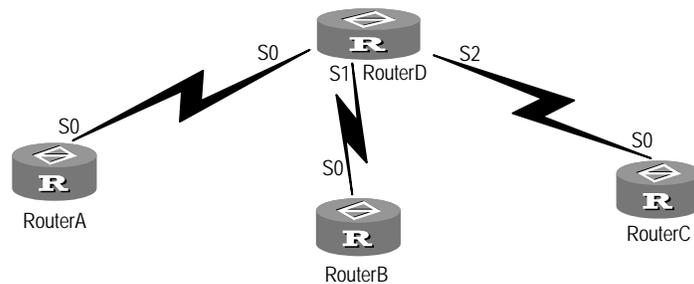
### Typical X.25 Sub-Interface Configuration Example

#### I. Networking Requirement

Multiple sub-interfaces are configured on a physical interface to connect with multiple peers of different network sections. In the following diagram, Router A is configured with two sub-interfaces, respectively interconnected with Router B and Router C.

## II. Networking Diagram

Figure 72 Diagram of X.25 sub-interface configuration



## III. Configuration Procedure

### 1 Configure Router A:

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dte
[Router-Serial0]x25 x121-address 100
[Router-Serial0]interface serial 0.1
```

#### a Create sub-interface serial 0.1

```
[Router-Serial0.1]ip address 10.1.1.2 255.255.0.0
[Router-Serial0.1]x25 map ip 10.1.1.1 x121-address 200
```

#### b Create sub-interface serial 0.2

```
[Router-Serial0.1]interface serial 0.2
[Router-Serial0.2]ip address 20.1.1.2 255.255.0.0
[Router-Serial0.2]x25 map ip 20.1.1.1 x121-address 300
```

### 2 Configure Router B:

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dte
[Router-Serial0]x25 x121-address 200
[Router-Serial0]x25 map ip 10.1.1.2 x121-address 100
```

### 3 Configure Router C:

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dte
[Router-Serial0]x25 x121-address 300
[Router-Serial0]x25 map ip 20.1.1.2 x121-address 100
```

### 4 Configure Router D:

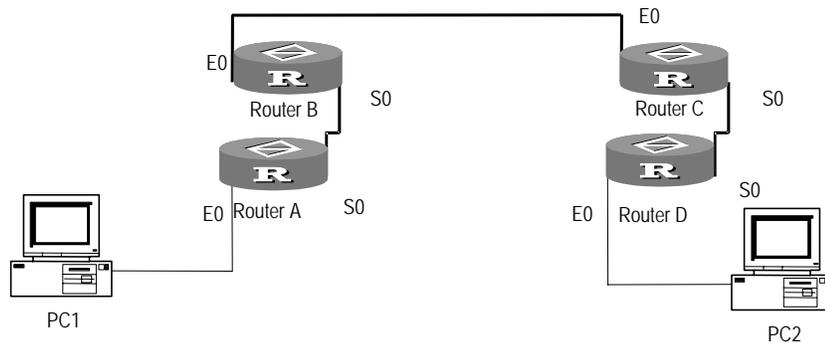
```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dce
[Router-Serial0]interface serial 1
[Router-Serial1]link-protocol x25 dce
[Router-Serial1]interface serial 2
[Router-Serial2]link-protocol x25 dce
[Router-Serial2]quit
[Router]x25 switching
[Router]x25 switch svc 100 interface serial 0
[Router]x25 switch svc 200 interface serial 1
[Router]x25 switch svc 300 interface serial 2
```

## SVC Application of XOT I. Networking Requirement

Router B and C connect through Ethernet interface, and build TCP connection between them. X.25 packets forward through TCP, and configure SVC to implement the SVC function.

## II. Networking Diagram

**Figure 73** SVC application networking diagram of XOT



## III. Configuration Procedure

### 1 Configure Router A

#### a Basic X.25 Configuration

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dte ietf
[Router-Serial0]x25 x121-address 1
[Router-Serial0]x25 map ip 1.1.1.2 x121-address 2
[Router-Serial0]ip address 1.1.1.1 255.0.0.0
```

### 2 Configure Router D

#### a Basic X.25 Configuration

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dte ietf
[Router-Serial0]x25 x121-address 2
[Router-Serial0]x25 map ip 1.1.1.1 x121-address 1
[Router-Serial0]ip address 1.1.1.2 255.0.0.0
```

### 3 Configure Router B

#### a Start X.25 switching

```
[Router]x25 switching
```

#### b Configure X.25 local switching

```
[Router]x25 switch svc 1 interface serial 11/0/2
```

#### c Configure XOT switching

```
[Router]x25 switch svc 2 xot 10.1.1.2
```

#### d Configure ethernet 0.

```
[Router]interface ethernet 0
[Router-Ethernet0]ip address 10.1.1.1 255.0.0.0
```

#### e Configure Serial 11/0/2

```
[Router-Ethernet0]interface serial 0
[Router-Serial0]link-protocol x25 dce ietf
```

4 Configure Router C

a Start X.25 switching

```
[Router]x25 switching
```

b Configure X.25 local switching

```
[Router]x25 switch svc 2 interface serial 0
```

c Configure XOT switching

```
[Router]x25 switch svc 1 xot 10.1.1.1
```

d Configure Ethernet 0

```
[Router]interface ethernet 0
```

```
[Router-Ethernet0]ip address 10.1.1.2 255.0.0.0
```

e Configure Serial 0

```
[Router-Ethernet0]interface serial 0
```

```
[Router-Serial0]link-protocol x25 dce ietf
```

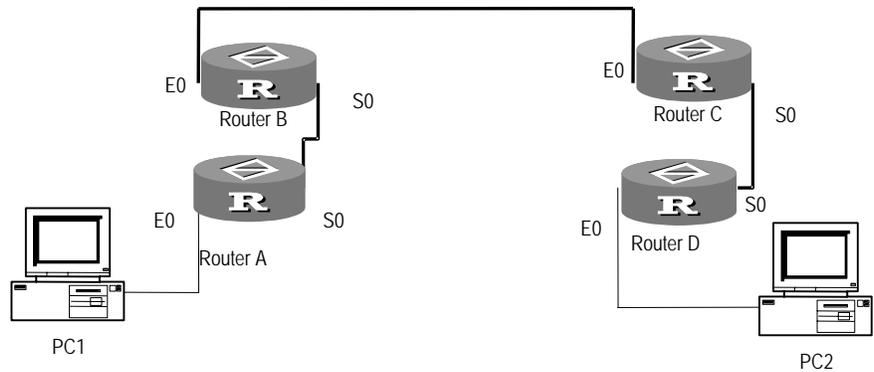
PVC Application of XOT

I. Networking Requirement

Router B and C connect through Ethernet interface, and build TCP connection between them. X.25 packets forward through TCP, and configure PVC to implement the PVC function.

II. Networking Diagram

Figure 74 PVC application networking diagram of XOT



III. Configuration Procedure

1 Configure Router A

a Basic X.25 Configuration

```
[Router]interface serial 0
```

```
[Router-Serial0]link-protocol x25 dte ietf
```

```
[Router-Serial0]x25 x121-address 1
```

```
[Router-Serial0]x25 vc-range in-channel 10 20 bi-channel 30 1024
```

```
[Router-Serial0]x25 pvc 1 ip 1.1.1.2 x121-address 2
```

```
[Router-Serial0]ip address 1.1.1.1 255.0.0.0
```

2 Configure Router D

a Basic X.25 configuration

```
[Router]interface serial 0
```

```
[Router-Serial0]link-protocol x25 dte ietf
```

```
[Router-Serial0]x25 x121-address 2
[Router-Serial0]x25 x25 vc-range in-channel 10 20 bi-channel 30 1024
[Router-Serial0]x25 pvc 1 ip 1.1.1.1 x121-address 1
[Router-Serial0]ip address 1.1.1.2 255.0.0.0
```

### 3 Configure Router B

#### a Start X.25 switching

```
[Router]x25 switching
```

#### b Configure Ethernet 0

```
[Router]interface ethernet 0
[Router-Ethernet0]ip address 10.1.1.1 255.0.0.0
```

#### c Configure Serial 0

```
[Router-Ethernet0]interface serial 0
[Router-Serial0]link-protocol x25 dce ietf
[Router-Serial0]x25 x25 vc-range in-channel 10 20 bi-channel 30 1024
[Router-Serial0]x25 xot pvc 1 10.1.1.2 interface serial 0 pvc 1
```

### 4 Configure Router C

#### a Start X.25 switching

```
[Router]x25 switching
```

#### b Configure Ethernet 0

```
[Router]interface ethernet 0
[Router-Ethernet0]ip address 10.1.1.2 255.0.0.0
```

#### c Configure Serial 0.

```
[Router-Ethernet0]interface serial 0
[Router-Serial0]link-protocol x25 dce ietf
[Router-Serial0]x25 vc-range in-channel 10 20 bi-channel 30 1024
[Router-Serial0]x25 xot pvc 1 10.1.1.1 interface serial 0 pvc 1
```

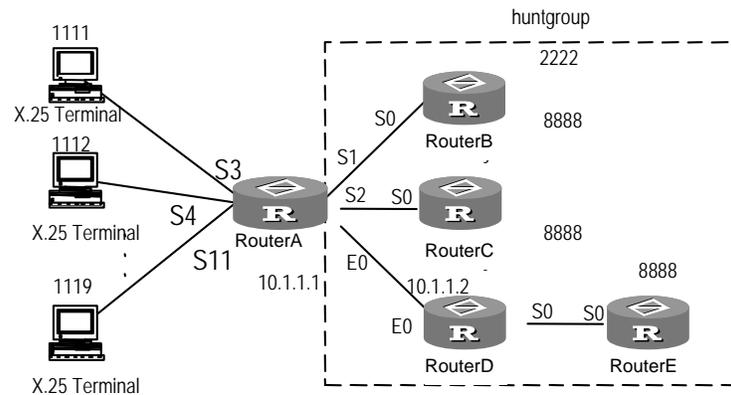
## Application of X.25 Load Balancing

### I. Networking Requirements

Configure hunt group on Server RouterA which serves as an X.25 switch and simultaneously enable the function of substitution of destination address and source address, so that the caller can treat router RouterB, RouterC and RouterE equally as one destination, and the calls of X.25 terminal can be sent to routers RouterB, RouterC and RouterE to achieve load balancing. Therefore the load balancing of routers on X.25 network can be implemented. As an X.25 switching exchange, router RouterD performs the XOT function and connects RouterA and RouterE. Router RouterB, RouterC and RouterE are DTEs in a hunt group. They provide X.25 terminals with identical services.

## II. Networking Diagram

**Figure 75** Networking diagram of typical configuration of X.25 hunt group



## III. Configuration Procedure

### 1 Configure RouterA

- a Configure the link layer protocol of interface Serial1 to X.25 and specify it to operate in DCE mode.

```
[Router] interface serial 1
[Router-Serial1] link-protocol x25 dce
```

- b Configure the link layer protocol of other synchronous serial interfaces to X.25 and specify it to operate in DCE mode. Their configuration is identical to the configuration of interface Serial 1.

- c Configure IP addresses on interface Ethernet 0.

```
[Router] interface ethernet 0
[Router-Ethernet0] ip address 10.1.1.1 255.255.255.0
```

- d Enable X.25 switching in system view.

```
[Router] x25 switching
```

- e Create X.25 hunt group named hg1 with property of rotary in system view.

```
[Router] x25 hunt-group hg1 round-robin
```

- f Add Serial 1, Serial 2 and XOT Tunnel to hunt group.

```
[Router-x25-huntgroup-hg1] interface serial 1
[Router-x25-huntgroup-hg1] interface serial 2
[Router-x25-huntgroup-hg1] channel xot 10.1.1.2
```

- g Configure X.25 switching route whose forwarding address is hunt group hg1 and enable the substitution of destination address and source address.

```
[Router] x25 switch svc 2222 sub-dest 8888 sub-source 3333 hunt-group hg1
```

- h Configure X.25 switching route to forward to X.25 terminal.

```
[Router] x25 switch svc 1111 interface serial 3
[Router] x25 switch svc 1119 interface serial 11
```

### 2 Configure RouterB

- a Configure the interface Serial0's link layer protocol to X.25 and specify it to operate in DTE mode.

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dte
[Router-Serial0]x25 x121-address 8888
```

The configurations of RouterC and RouterE are identical with the configuration of RouterB

### 3 Configure RouterD

- a Configure link layer protocol of interface Serial 0 to X.25 and specify it to operate in DCE mode.

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dce
```

- b Configure IP addresses on interface Ethernet 0.

```
[Router]interface ethernet 0
[Router-Ethernet0]ip address 10.1.1.2 255.255.255.0
```

- c Enable X.25 switching in system view.

```
[Router]x25 switching
```

- d Configure X.25 switching route whose forwarding address is XOT Tunnel.

```
[Router]x25 switch svc 1111 xot 10.1.1.1
```

- e Configure X.25 switching route that is forwarded to router RouterE

```
[Router]x25 switch svc 8888 interface serial 0
```

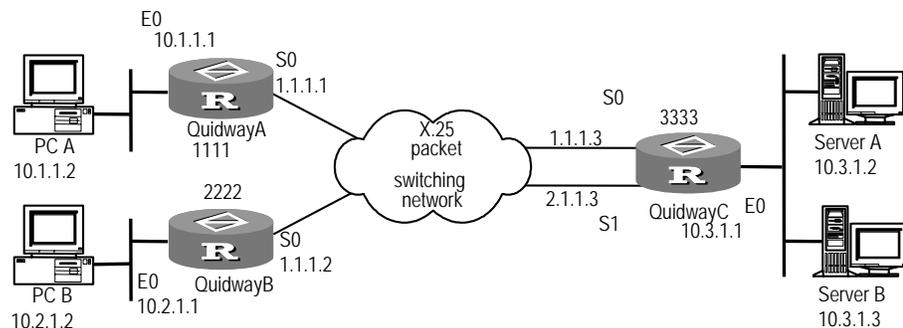
## X.25 Load Balancing Carrying IP Data Transmission

### I. Networking Requirements

X.25 packet switching networks interconnect IP networks in different areas and X.25 networks carry IP data. At the same time, ISPs provide the function of X.25 network load balancing and implement the configuration of load balancing with subscribers, to achieve the line load balancing when a server is accessed by different clients.

### II. Networking Diagram

Figure 76 X.25 hunt group carrying IP data transmission



### III. Configuration Procedure

In this example, ISP performs the configuration of load balancing on packet switching exchange, therefore only the common X.25 configuration needs to be implemented on routers.

Note that you must configure a virtual IP address and two static routes on interface Serial 1 to deceive the router because two lines connected to the same peer exist in router RouterC. Thus load balancing can be achieved because router RouterC will deem that there are two routes connected to network segment 10.1.1.0.

## 1 Configure RouterA

### a Configure interface Ethernet 0.

```
[Router]interface ethernet 0
[Router-Ethernet0]ip address 10.1.1.1 255.255.255.0
```

### b Configure interface Serial 0.

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dte
[Router-Serial0]x25 x121-address 1111
[Router-Serial0]ip address 1.1.1.1 255.255.255.0
[Router-Serial0]x25 map ip 1.1.1.3 x121-address 3333
[Router-Serial0]x25 vc-per-map 2
```

### c Configure static route to RouterC.

```
[Router]ip route-static 10.3.1.0 24 1.1.1.3
```

## 2 Configure RouterB

### a Configure interface Ethernet 0.

```
[Router]interface ethernet 0
[Router-Ethernet0]ip address 10.2.1.1 255.255.255.0
```

### b Configure interface Serial 0.

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dte
[Router-Serial0]x25 x121-address 2222
[Router-Serial0]ip address 1.1.1.2 255.255.255.0
[Router-Serial0]x25 map ip 1.1.1.3 x121-address 3333
[Router-Serial0]x25 vc-per-map 2
```

### c Configure static route to RouterC.

```
[Router]ip route-static 10.3.1.0 24 1.1.1.3
Configure router RouterC
```

### d Configure interface Ethernet 0.

```
[Router]interface ethernet 0
[Router-Ethernet0]ip address 10.3.1.1 255.255.255.0
```

### e Configure interface Serial 0.

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dte
[Router-Serial0]x25 x121-address 3333
[Router-Serial0]ip address 1.1.1.3 255.255.255.0
[Router-Serial0]x25 map ip 1.1.1.1 x121-address 1111
[Router-Serial0]x25 map ip 2.1.1.1 x121-address 1111
[Router-Serial0]x25 map ip 1.1.1.2 x121-address 2222
[Router-Serial0]x25 map ip 2.1.1.2 x121-address 2222
```

### f Configure interface Serial 1.

```
[Router]interface serial 1
[Router-Serial1]link-protocol x25 dte
```

```
[Router-Serial1]x25 x121-address 3333
[Router-Serial1]ip address 2.1.1.3 255.255.255.0
[Router-Serial1]x25 map ip 1.1.1.1 x121-address 1111
[Router-Serial1]x25 map ip 2.1.1.1 x121-address 1111
[Router-Serial1]x25 map ip 1.1.1.2 x121-address 2222
[Router-Serial1]x25 map ip 2.1.1.2 x121-address 2222
```

**g** Configure the static route to RouterA and RouterB.

```
[Router]ip route-static 10.1.1.0 24 1.1.1.1
[Router]ip route-static 10.1.1.0 24 2.1.1.1
[Router]ip route-static 10.2.1.0 24 1.1.1.2
[Router]ip route-static 10.2.1.0 24 2.1.1.2
```

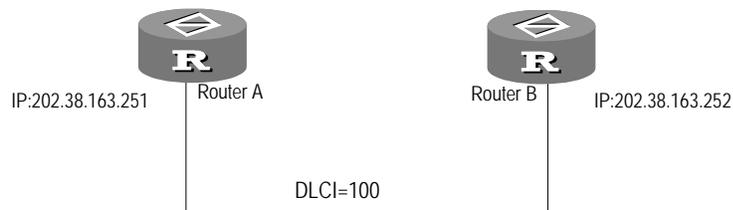
## Interconnect LANs via Annex G DLCIs

### I. Networking Requirements

Two Routers are directly connected via serial interfaces. Router A works as Frame Relay DCE whereas Router B as Frame Relay DTE.

### II. Networking Diagram

**Figure 77** Interconnect LANs via an Annex G DLCI



### III. Configuration Procedure

**1** Configure RouterA:

**a** Create an X.25 template.

```
[Router]x25 template profile1
```

**b** Configure the local X.25 address.

```
[Router-x25-profile1]x25 x121-address 10094
```

**c** Map the destination X.25 address to the destination IP address.

```
[Router-x25-profile1]x25 map ip 202.38.163.252 x121-address 20094
[Router-x25-profile1]quit
```

**d** Configure an IP address for the local interface.

```
[Router]interface serial 1
[Router-Serial1]ip address 202.38.163.251 255.255.255.0
```

**e** Configure the link layer protocol of the interface to Frame Relay.

```
[Router-Serial1]link-protocol fr
[Router-Serial1]fr interface-type dce
```

**f** Configure a Frame Relay DLCI.

```
[Router-Serial1]fr dlci 100
```

**g** Configure the DLCI to be Annex G DLCI.

```
[Router-fr-dlci-100]annexg dce
```

**h** Associate the X.25 template with the DLCI.

```
[Router-fr-dlci-100]x25-template profile1
[Router-fr-dlci-100]quit
```

- i Map the Frame Relay address to the destination IP address.

```
[Router-Serial1]fr map ip 202.38.163.252 100
```

## 2 Configure RouterB:

- a Create an X.25 template.

```
[Router]x25 template profile1
```

- b Configure the local X.25 address.

```
[Router-x25-profile1]x25 x121-address 20094
```

- c Map the destination X.25 address to the destination IP address.

```
[Router-x25-profile1]x25 map ip 202.38.163.251 x121-address 10094
[Router-x25-profile1]quit
```

- d Configure an IP address for the local interface.

```
[Router]interface serial 1
[Router-Serial1]ip address 202.38.163.252 255.255.255.0
```

- e Configure the link layer protocol of the interface to Frame Relay.

```
[Router-Serial1]link-protocol fr
[Router-Serial1]fr interface-type dte
```

- f Configure a Frame Relay DLCI.

```
[Router-Serial1]fr dlci 100
```

- g Configure the DLCI to be Annex G DLCI.

```
[Router-fr-dlci-100]annexg dte
```

- h Associates an X.25 template with the DLCI.

```
[Router-fr-dlci-100]x25-template profile1
[Router-fr-dlci-100]quit
```

- i Map the Frame Relay address to the destination IP address.

```
[Router-Serial1]fr map ip 202.38.163.251 100
```

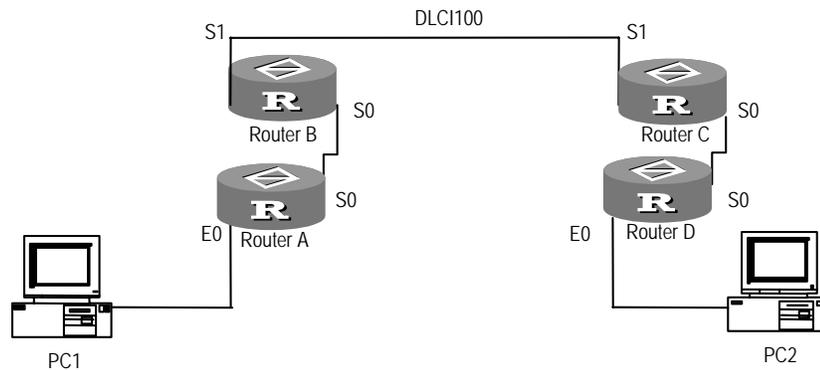
## SVC Application of X.25 over Frame Relay

### I. Networking Requirements

RouterA and RouterC are respectively connected to RouterB and RouterD through X.25. RouterB and RouterC are connected through Frame Relay. Configure Annex G DLCI 100 for Frame Relay on both RouterB and RouterC to interconnect the two X.25 networks. Thereby, PC1 and PC2 can access each other.

## II. Networking Diagram

**Figure 78** Networking for the SVC application of X.25 over Frame Relay



## III. Configuration Procedure

### 1 Configure the router Router A:

#### a Configure the basic X.25 parameters.

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dte ietf
[Router-Serial0]x25 x121-address 1
[Router-Serial0]x25 map ip 1.1.1.2 x121-address 2
[Router-Serial0]ip address 1.1.1.1 255.0.0.0
```

### 2 Configure the router Router D:

#### a Configure the basic X.25 parameters:

```
[Router]config
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dte ietf
[Router-Serial0]x25 x121-address 2
[Router-Serial0]x25 map ip 1.1.1.1 x121-address 1
[Router-Serial0]ip address 1.1.1.2 255.0.0.0
```

### 3 Configure the router Router B:

#### a Enable X.25 switching.

```
[Router]x25 switching
```

#### b Enable switching on Frame Relay DCE.

```
[Router]fr switching
```

#### c Configure Serial 0 as the X.25 interface.

```
[Router]interface serial 0
[Router-Serial0]switching x25 dce ietf
```

#### d Configure Serial 1 as the Frame Relay interface.

```
[Router]interface serial 1
[Router-Serial1]link-protocol frame-relay
[Router-Serial1]fr interface-type dce
```

#### e Configure a Frame Relay Annex G DLCI.

```
[Router-Serial1]fr dlci 100
[Router-fr-dlci-100]annexg dce
```

#### f Configure local X.25 switching.

```
[Router]x25 switch svc 1 interface serial 0
```

**g** Configure X.25 over Frame Relay switching.

```
[Router]x25 switch svc 2 interface serial 1 dlci 100
```

**4** Configure the router Router C:

**a** Enable X.25 switching.

```
[Router]x25 switching
```

**b** Configure Serial 0 as the X.25 interface.

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dce ietf
```

**c** Configure Serial 1 as the Frame Relay interface.

```
[Router]interface serial 1
[Router-Serial1]link-protocol fr
```

**d** Configure the Frame Relay Annex G DLCI.

```
[Router-Serial1]fr dlci 100
```

**e** Configure local X.25 switching.[Router-fr-dlci-100]annexg dte

```
[Router]x25 switch svc 2 interface serial 0
```

**f** Configure X.25 over Frame Relay switching.

```
[Router]x25 switch svc 1 interface serial 1 dlci 100
```

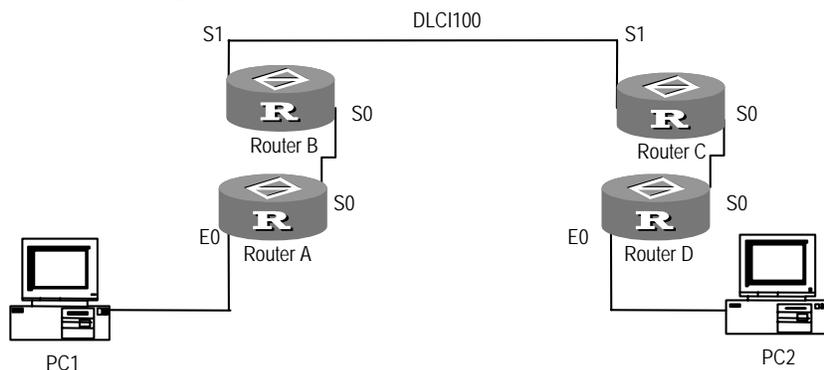
## PVC Application of X.25 over Frame Relay

### I. Networking Requirements

RouterA and RouterC are respectively connected to RouterB and RouterD through X.25. RouterB and RouterC are connected through Frame Relay. Configure Frame Relay Annex G DLCI 100 on both RouterB and RouterC to set up an X.25 PVC to interconnect the two X.25 networks. Thereby, PC1 and PC2 can access each other.

### II. Networking Diagram

**Figure 79** Networking for the PVC application of X.25 over Frame Relay



### III. Configuration Procedure

**1** Configure Router A:

**a** Configure the basic X.25 parameters.

```
[Router]interface serial 0
[Router-Serial0]switch svc x25 dte ietf
```

```
[Router-Serial0]x25 x121-address 1
[Router-Serial0]x25 vc-range in-channel 10 20 bi-channel 30 1024
[Router-Serial0]x25 pvc 1 ip 1.1.1.2 x121-address 2
[Router-Serial0]ip address 1.1.1.1 255.0.0.0
```

## 2 Configure Router D:

- a Configure the basic X.25 parameters.

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dte ietf
[Router-Serial0]x25 x121-address 2
[Router-Serial0]x25 vc-range in-channel 10 20 bi-channel 30 1024
[Router-Serial0]x25 pvc 1 ip 1.1.1.1 x121-address 1
[Router-Serial0]ip address 1.1.1.2 255.0.0.0
```

## 3 Configure Router B:

- a Enable X.25 switching.

```
[Router]x25 switching
```

- b Enable switching on Frame Relay DCE.

```
[Router]fr switching
```

- c Configure Serial 0 as the X.25 interface.

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dce ietf
[Router-Serial0]x25 vc-range in-channel 10 20 bi-channel 30 1024
```

- d Configure an X.25 template.

```
[Router]x25 template profile1
[Router-x25-profile1]x25 vc-range in-channel 10 20 bi-channel 30
1024
[Router-x25-profile1]x25 pvc 1 interface serial 0 pvc 1
```

- e Configure S1 as the Frame Relay interface.

```
[Router]interface serial 1
[Router-Serial1]link-protocol fr
[Router-Serial1]fr interface-type dce
```

- f Configure a Frame Relay Annex G DLCI.

```
[Router-Serial1]fr dlci 100
[Router-fr-dlci-100]annexg dce
```

- g Apply the X.25 template to Annex G DLCI 100 (which is equivalent to configure X.25 attributes for the Annex G DLCI).

```
[Router-fr-dlci-100]x25-template profile1
```

## 4 Configure Router C:

- a Enable X.25 switching.

```
[Router]x25 switching
```

- b Configure Serial 0.

```
[Router]interface serial 0
[Router-Serial0]link-protocol x25 dce ietf
[Router-Serial0]x25 vc-range in-channel 10 20 bi-channel 30 1024
```

- c Configure an X.25 template.

```
[Router]x25 template profile1
```

```
[Router-x25-profile1]x25 vc-range in-channel 10 20 bi-channel 30
1024
[Router-x25-profile1]x25 pvc 1 interface serial 0 pvc 1
```

## 5 Configure Serial 1.

a Configure S1 as the Frame Relay interface.

```
[Router]interface serial 1
[Router-Serial1]link-protocol frame-relay
```

b Configure a Frame Relay Annex G DLCI.

```
[Router-Serial1]fr dlci 100
[Router-fr-dlci-100]annexg dte
```

c Apply the X.25 template to Annex G DLCI 100 (which is equivalent to configure X.25 attributes for the Annex G DLCI).

```
[Router-fr-dlci-100]x25-template profile1
```

---

### Fault Diagnosis and Troubleshooting of LAPB

**Fault 1: Two connected sides use X.25 link layer protocol (or LAPB), but the protocol is always disconnected. Turn on the debugging switch. It is found that one end sends SABM frame, while the other end sends FRMR frame circularly.**

Troubleshooting: this is because both sides worked in the same working mode (DTE or DCE). Change the working mode of one side to solve the problem.

**Fault 2: Two connected sides use X.25 link layer protocol, and the protocol is already in UP status, but cannot ping through the peer. Turn on the debugging switch and it is found that the received frames are discarded on one end instead of being forwarded up to the packet layer.**

Troubleshooting: The maximum frame bits of this end may be too small. Change the configuration.

---

### Fault Diagnosis and Troubleshooting of X.25

This section describes some common faults and the troubleshooting methods.

Assuming that the connection of the X.25 layer 2 (LAPB) is completely correct.

**Fault 1: LAPB is already in "Connect" status, but the X.25 protocol can not enter "UP" status.**

Troubleshooting: It is possible that the local working mode has been configured wrong, for example, both sides of a connection are DTE or DCE. Try again after changing the interface working mode.

**Fault 2: X.25 protocol is "UP", but virtual circuit can not be established, i.e., unable to ping through.**

This may be caused by one of the following:

- Local X.121 address not configured
- Address mapping to the peer not configured
- Opposite X.121 address not configured
- Address mapping from peer to local not configured
- Channel range not correct

- Facility options inhibited by network have been carried.

Troubleshooting: if the address is configured incorrectly, change the configuration. For the last two causes, please consult the network management department for correct channel range and permissible facility options.

**Fault 3: The virtual circuit can be established, but is frequently reset or cleared during data transmission.**

Troubleshooting: It is very likely that the flow control parameters are set incorrectly. For the back to back direct connection, check the sending window and receiving window of the local and peer to see whether they match each other. In case it is connected to public packet networks, consult the network management department to correct flow control parameters.

**Fault 4: The request to set Permanent virtual circuits (PVCs) is rejected.**

Troubleshooting: if the channel section of the permanent virtual circuit is disabled, the X.25 will reject the request to set a permanent virtual circuit. In this case, simply enable the permanent virtual circuit channel section.

**Fault 5: After configuring SVC application of XOT, you cannot ping through**

Troubleshooting: there are various reasons. You may first check if the physical and protocol statuses of the interface are UP. If the interface status is DOWN, check if the physical connection and bottom configuration are correct. If the interface is properly configured, then check the SVC configuration. If SVC is also properly configured, check the XOT configuration.

**Fault 6: After configuring PVC application of XOT, you cannot ping through**

Troubleshooting: there are various reasons. You may first check if the physical and protocol statuses of the interface are UP. If the interface status is DOWN, check if the physical connection and configuration are correct. If the interface is properly configured, then check the PVC configuration. If PVC is also properly configured, check the XOT configuration.

**Fault 7: Annex G DLCI is used for interconnection, the link layer protocol is up, and DLCI has been in place after negotiation. However, the remote end cannot be pinged.**

Troubleshooting:

- Check whether the X.25 protocol is up at both ends of the Annex G DLCI by using the `display fr pvc-info` command. Both the Frame Relay interface and DLCI number should be explicitly specified in the command.
- Check whether the proper map between the Frame Relay address and the destination IP address has been configured on the router at each ends.
- Check whether the proper X.25 template has been configured for the Annex G DLCI on each ends, and whether the local X.121 address has been correctly mapped to the X.25 address for the destination IP address on each ends.
- Check whether X.25 SVC has been correctly set up by executing the `display x25 vc` command.

- If receiving the ping packet forwarded from the router at one end, check whether the returning route has been configured in the routing table. In addition, if the destination IP address for returning the packets is different from that configured in the Frame Relay address map and X.25 address map, you need to reconfigure the maps.
- If multiple X.25 address maps for reaching the same destination X.121 address have been configured in an X.25 template, check whether the **x25 vc-per-map** command has been configured so that multiple X.25 SVC calls can be placed with the same X.25 address map. Use the **debugging x25** command to debug the X.25 protocol.



# 17

## CONFIGURING FRAME RELAY

This chapter contains information on the following topics:

- Frame Relay Protocol Overview
- Configure Frame Relay
- Configure Frame Relay QoS
- Configure Frame Relay over Other Protocols
- Display and debug Frame Relay
- Typical Frame Relay Configuration Example
- Fault Diagnosis and Troubleshooting of Frame Relay

---

### Frame Relay Protocol Overview

Frame Relay protocol is a fast-packaging switching technology, which develops on the basis of X.25 technology. Compared with X.25 protocol, Frame Relay only implements the core function of the link layer, easily and efficiently.

A Frame Relay network provides capacity of data communication between user equipment (such as routers and hosts), also called data terminal equipment (DTE). The equipment that provides access for DTE is data circuit-terminating equipment (DCE). A Frame Relay network can be a public network, a private enterprise network, or a network formed by direct connection between data equipment.

The Frame Relay protocol is a statistics multiplexing protocol, providing multiple virtual circuits on a single physical transmission line. Each virtual circuit is identified by a DLCI (Data Link Connection Identifier), which is valid only on the local interface and the corresponding opposite interface. This means that in the same Frame Relay network, the same DLCI on different physical interfaces does not indicate the same virtual connection. A user interface in the Frame Relay network supports up to 1024 virtual circuits, among which the DLCI range available to the user is 16~1007. As a Frame Relay virtual circuit is connection oriented, different local DLCIs are connected to different opposite equipment. Therefore, the local DLCI can be considered as the "Frame Relay address" of the opposite equipment.

Frame relay address mapping associates the opposite equipment's protocol address with its Frame Relay address (local DLCI), so that the upper layer protocol can locate the opposite equipment by using its protocol address. Frame Relay mainly bears IP. In sending IP packet, only the next hop address of the packet can be obtained from the route table, so this IP address must be used to determine the corresponding DLCI before sending. This process can be performed by searching for the Frame Relay address mapping table, because the mapping relation between the opposite IP address and the next hop DLCI is stored in the address mapping table. The address mapping table can be manually configured, or maintained dynamically by the Inverse ARP protocol.

Virtual circuits can be divided into permanent virtual circuit and switching virtual circuit, according to their different configuration method. Virtual circuits configured manually are called Permanent virtual circuits (PVCs), and those created by protocol negotiation are called switching virtual circuits (SVCs), which are automatically created and deleted by Inverse ARP protocol. At present, the most frequently used in Frame Relay is the permanent virtual circuit mode, i.e., manually configured virtual circuit.

In the permanent virtual circuit mode, test the availability of the virtual circuit, which is accomplished by the local management interface (LMI) protocol. The 3Com Router supports three LMI protocols: LMI complying with ITU-T Q.933 Appendix A, LMI complying with ANSI T1.617 Appendix D and non-standard LMI. Their basic function is: DTE sends one Status Enquiry packet to query the virtual circuit status at certain interval, after the DCE receives the packet, it will immediately use the Status packet to inform DTE the status of all the virtual circuits on current interface.

The status of Permanent virtual circuits (PVCs) on DTE is completely determined by DCE. And the network determines the status of Permanent virtual circuits (PVCs) of DCE. In case that the two network devices are directly connected, the equipment administrator sets the virtual circuit status of DCE. In The 3Com Router, the quantity and status of the virtual circuits are set at the time when address mapping is set (with the **fr map** command). They can also be configured with the Frame Relay local virtual circuit configuration command (**fr dlci** command).

## Configure Frame Relay

Frame Relay configuration includes:

- Configure the Link Layer Protocol of the Interface to Frame Relay
  - Configure Frame Relay Terminal Type
  - Configure Frame Relay LMI Type
  - Configure the Related Parameters of Frame Relay LMI Protocol
  - Configure Frame Relay Address Mapping
  - Configure Frame Relay Local Virtual Circuit Number
  - Configure Frame Relay Sub-Interface
  - Configure Frame Relay PVC Switching
  - Configure Multilink Frame Relay (FRF.16)
  - Configure Frame Relay Payload Compression (FRF.9)
  - Enable/Disable TCP/IP Header Compression on Interfaces
  - Configure Frame Relay Fragment(FRF.12)
- 1 Configure the Link Layer Protocol of the Interface to Frame Relay

Perform the following task in the interface view.

**Table 274** Configure the link layer protocol of interface to Frame Relay

| Operation                                                     | Command                                        |
|---------------------------------------------------------------|------------------------------------------------|
| Configure the link layer protocol of interface to Frame Relay | <b>link-protocol fr [ ietf   nonstandard ]</b> |

By default, the interface's link layer protocol is PPP.

Note the following:

- The interface's link layer protocol can be configured to Frame Relay only when it operates in the synchronous mode.
- When the interface's link layer protocol is SLIP, the physical attributes of the interface cannot be modified to synchronous mode. At this time, you should first modify the link layer protocol of the interface to PPP and then you may change the interface attribute to synchronous mode.



*The Frame Relay interface can send the packet in either of the Frame Relay formats, while it can recognize and receive packets in both formats. That is, even if the format of Frame Relay of opposite equipment is different from that of the local, the equipment at the two ends can communicate with each other as long as the opposite equipment can recognize the two formats automatically. But when the opposite equipment can not recognize the two formats automatically, the Frame Relays of equipment at the two ends must be set to the same format.*

## 2 Configure Frame Relay Terminal Type

In Frame Relay, the two sides in communication are classified into user side and network side. The user side is called DTE, and the network side is called DCE. The equipment response interface should be configured as DTE or DCE format according to its location in the network. In Frame Relay networks, Network-to-Network Interface (NNI) is used between the Frame Relay switches.

In the interface view, perform the following task to configure the type of Frame Relay interface as DTE, DCE or NNI.

**Table 275** Configure Frame Relay interface type

| Operation                                                   | Command                                      |
|-------------------------------------------------------------|----------------------------------------------|
| Configure Frame Relay interface type                        | <b>fr interface-type { dte   dce   nni }</b> |
| Restore the Frame Relay interface type to the default value | <b>undo fr interface-type</b>                |

The default type of Frame Relay interface is DTE.

Note the following point: If the terminal type of Frame Relay interface is changed to DCE or NNI, **fr switching** should be enabled in the system view.

## 3 Configure Frame Relay LMI Type

The LMI protocol is used to maintain the PVC lists of Frame Relay protocol, including adding PVC records, deleting the records about disconnected PVCs, monitoring the change of PVC status, and verifying the link integrity. The 3Com Router supports three standard LMI protocols: LMI complying with ITU-T Q.933 Appendix A, LMI complying with ANSI T1.617 Appendix D and non-standard LMI.

In the interface view, perform the following task to configure the type of LMI protocol of Frame Relay interface.

**Table 276** Configure Frame Relay LMI protocol type

| Operation                                                       | Command                                                            |
|-----------------------------------------------------------------|--------------------------------------------------------------------|
| Configure Frame Relay LMI protocol type                         | <b>fr lmi type { ansi   nonstandard   q933a } [ bi-direction ]</b> |
| Restore the Frame Relay interface LMI protocol type to default. | <b>undo fr lmi type</b>                                            |

When the Frame Relay interface type is DCE or NNI, the default type of LMI protocol of interface is Q933a. When the Frame Relay interface type is DTE, the default LMI protocol of interface is null.

#### 4 Configure the Related Parameters of Frame Relay LMI Protocol

The procedure of the LMI protocol is as follow:

- DTE sends out a status enquiry message, and the timer T391 starts. T391 is set with the polling interval. In other words, DTE will send a status enquiry message at each interval of T391. Simultaneously, the counter V391 at the DTE side will start. If  $V391 < N391$ , The status enquiry message sent by DTE will only inquire the "link integrity". If  $V391 = N391$ , it will clear all. In this case, besides inquiring the "link integrity", the status enquiry sent by DTE will inquire the statuses of all the PVCs, which is called "Full Status Message Polling".
- Upon receiving the enquiry message, DCE respond to the status enquiry message by sending the status message. Simultaneously, the polling authentication timer T392 at the DCE side starts, and DCE waits for the next status enquiry message. Upon the timeout of T392, if DCE receives no status enquiry messages, it will record this error and add 1 to the number of errors.
- Upon receiving the status response message, DTE knows the link status and PVC status. When DCE responds to the status enquiry message, it should respond the status message of all the PVCs if the PVC status on the network changes or there is PVC added or deleted, irrespective of DTE inquires for the PVC status or not,. Thereby, DTE can know the changes on DCE side, and update the record based on that information.
- If the timer T391 times out, but no status message is received yet at the DTE side to respond to that, this event error will be recorded and 1 will be added to the number of errors.
- If the number of errors in N393 events exceeds N392, DTE or DCE will assume that the path is usable but all the virtual circuits are unusable. N393 represents the total number of observed events, and N392 represents the error threshold.

You can configure the various counters and thresholds of the frame relay LMI protocol, to optimize the running efficiency of equipment at the DTE and DCE sides.

Perform the following configurations in synchronous interface view.

**Table 277** Configure the related parameters of Frame Relay LMI protocol

| Operation                                                                   | Command                                    |
|-----------------------------------------------------------------------------|--------------------------------------------|
| Set the counter on PVC status enquiry messages (N391 DTE)                   | <code>fr lmi n391dte [ n391-value ]</code> |
| Restore the default value of the counter on the PVC status enquiry messages | <code>undo fr lmi-n391dte</code>           |
| Set the LMI error threshold (N392 DCE)                                      | <code>fr lmi n392dce [ n392-value ]</code> |
| Restore the default value of the LMI error threshold                        | <code>undo fr lmi n392dce</code>           |
| Set the LMI error threshold (N392 DTE)                                      | <code>fr lmi n392dte [ n392-value ]</code> |
| Restore the default value of the LMI error threshold                        | <code>undo fr lmi n392dte</code>           |
| Set the LMI event counter (N393 DTE)                                        | <code>fr lmi n393dte [ n393-value ]</code> |
| Restore the default value of the LMI event counter                          | <code>undo fr lmi n393dte</code>           |
| Set the LMI event counter (N393 DCE)                                        | <code>fr lmi n393dce [ n393-value ]</code> |

|                                                                                |                                            |
|--------------------------------------------------------------------------------|--------------------------------------------|
| Restore the default value of the LMI event counter                             | <code>undo fr lmi n393dce</code>           |
| Set the link integrity polling timer at the user side (T391 DTE)               | <code>fr lmi t391dte [ t391-value ]</code> |
| Restore the default value of the link integrity polling timer at the user side | <code>undo fr lmi t391dte</code>           |
| Set the polling timer at the network side (T392 DCE)                           | <code>fr lmi t392dce [ t392-value ]</code> |
| Restore the default value of the polling timer at the network side             | <code>undo fr lmi t392dce</code>           |

The following table describes the value ranges and default values of related parameters of the Frame Relay LMI protocol

**Table 278** Descriptions of related parameters of Frame Relay LMI protocol

| Operation mode | Parameter description                                                                                 | Value range     | Default value |
|----------------|-------------------------------------------------------------------------------------------------------|-----------------|---------------|
| DTE            | Link integrity polling timer (T391)<br>When T391 = 0, it indicates that the LMI protocol is disabled. | 5 to 30 seconds | 10 seconds    |
|                | Counter on the PVC full status message polling requests (N391)                                        | 1 to 255 times  | 6 times       |
|                | Error threshold counter at the user side (N392)                                                       | 1 to 10 times   | 3 times       |
|                | Event counter at the user side (N393)                                                                 | 1 to 10 times   | 4 times       |
| DCE            | Polling authentication timer at the network side (T392)                                               | 5 to 30 seconds | 15 seconds    |
|                | Error threshold counter at the network side (N392)                                                    | 1 to 10 times   | 3 times       |
|                | Event counter at the network side (N393)                                                              | 1 to 10 times   | 4 times       |

In which, the related parameters at the DTE side include:

- T391DTE: The interval of the link integrity polling for the equipment at the DTE side
- N391DTE: DTE equipment will send a status enquiry message at a certain interval (which is determined by T391). The status enquiry messages are divided into two types: link integrity authentication messages and link status enquiry messages. The parameter N391DTE is used to define the sending ratio of these two types of messages. That is:

Number of link integrity authentication messages: Number of link status enquiry messages = N391-1: 1

- N392DTE: The threshold for the errors that can occur in the total number of observed events at the DTE side.
- N393DTE: The total number of observed events at the DTE side.

DTE equipment will send a status enquiry message at a certain interval (which is determined by T391) to inquire the link status. Upon receiving that message, the DCE equipment sends the status response message promptly. If the DTE equipment does not receive the response in the specified time, the error will be recorded. If the number of errors exceeds the threshold, the DTE equipment will regard the physical path and all the virtual circuits as unusable. The parameters N392 and N393 together define the "error threshold". That is, if the number of errors in the N393 status enquiry messages sent by the DTE equipment reaches

N392, the DTE equipment will assume that the number of errors reaches the threshold, and will regard the physical path and all the virtual circuits as unusable.

The parameters at the DCE side include:

- T392DCE: Define the longest duration for the DCE equipment to wait for a status enquiry message. It should be larger than T391.
- N392DCE: The threshold for the errors that can occur in the total number of observed events at the DCE side.
- N393DCE: The total number of observed events at the DCE side.

It should be noted that N392 should be no larger than N393 and T391DTE should be smaller than its peer T392DCE.

## 5 Configure Frame Relay Address Mapping

Frame Relay address mapping means to establish the mapping between the peer protocol address and the local DLCI. Address mapping of Frame Relay can either be configured statically or set up dynamically.

### a Configure Frame Relay static address mapping

Static configuration means the manual setup of the mapping relation between the peer protocol address and local DLCI, and is usually applied when there are few peer hosts or there is a default route.

In interface view, perform the following task to configure the Frame Relay static address mapping.

**Table 279** Configure Frame Relay static address mapping

| Operation                       | Command                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add a static address mapping    | <code>fr map { ip   ipx } protocol-address dlci dlci [ broadcast ] [ nonstandard   ietf ] [ logic-channel channel_number ] [ nocompress   compression vj ] [ compression frf9 ]</code> |
| Delete a static address mapping | <code>undo fr map { ip   ipx } protocol-address dlci dlci</code>                                                                                                                       |

By default, the dynamic inverse arp is enabled on all the interfaces.

After the Frame Relay static address mapping is configured, the dynamic inverse arp will be disabled automatically on the specified DLCI.

### b Configure Frame Relay dynamic inverse arp

Dynamic configuration means the mapping peer protocol address and local DLCI dynamically after running the inverse address resolution protocol (Inverse ARP), which is applicable when the peer router also supports the "inverse address resolution protocol" and network is complex.

In interface view, perform the following task to configure the dynamic inverse arp of Frame Relay.

**Table 280** Configure Frame Relay dynamic address mapping

| Operation                       | Command                                              |
|---------------------------------|------------------------------------------------------|
| Enable dynamic address mapping  | <code>fr inarp [ { ip   ipx } [ dlci ] ]</code>      |
| Disable dynamic address mapping | <code>undo fr inarp [ { ip   ipx } [ dlci ] ]</code> |

By default, the dynamic inverse arp is enabled on the interface.

The map created through the dynamic inverse ARP has broadcast attribute.

## 6 Configure Frame Relay Local Virtual Circuit Number

Perform the following configurations in synchronous serial interface view.

**Table 281** Configure Frame Relay local virtual circuit number

| Operation                                                  | Command                         |
|------------------------------------------------------------|---------------------------------|
| Assign a virtual circuit number to Frame Relay interface   | <b>fr dlci dlci-number</b>      |
| Remove the virtual circuit number of Frame Relay interface | <b>undo fr dlci dlci-number</b> |

After entering the DLCI view through the **fr dlci** command, the user can configure the parameters associated with this virtual circuit, such as Frame Relay class.

The virtual circuit number is valid locally, that is, the virtual circuit numbers on both ends of the link can be the same. Different interfaces can be assigned with the same virtual circuit number, but the virtual circuit number must be unique on one physical interface.

When the Frame Relay interface type is DCE or NNI, the interface (either main interface or sub-interface) should be configured manually with virtual circuits. When the Frame Relay interface type is DTE, for the main interface, the system will determine the virtual circuit automatically according to the opposite equipment; the sub-interface must be configured with virtual circuits manually.

## 7 Configure Frame Relay Sub-Interface

The Frame Relay interface is a kind of NBMA (Non-Broadcast Multi-Access) interface, which supports sub-interfaces. The Frame Relay module has two types of interfaces: main interface and sub-interface. The sub-interface is logical interface and can be used to configure protocol address and virtual circuit. One physical interface can include multiple sub-interfaces, which do not exist physically. However, for the network layer, both the sub-interface and main interface can be used to configure the virtual circuit to connect to remote equipment.

The sub-interfaces of Frame Relay fall into two types: point-to-point sub-interface, used to connect a single remote object and point-to-multipoint sub-interface, used to connect multiple remote objects in the same network segment.

The address mapping relation between the frame-relay sub-interfaces can be configured manually, or dynamically established by using the inverse ARP. For a point-to-point sub-interface, you only need configure one PVC on this sub-interface, since there is only one peer device. For a point-to-multipoint sub-interface, you can configure multiple PVCs. Each PVC can establish the address mapping with its connected peer through running the inverse dynamic ARP. Thereby, different PVCs can reach their peers without confusing. Alternatively, you can respectively establish different static address mapping for these PVCs.

### a Creating Frame Relay Sub-Interface

In the interface view, perform the following task to create a sub-interface.

**Table 282** Create Frame Relay sub-interface

| Operation            | Command                      |
|----------------------|------------------------------|
| Enter interface view | <b>interface type number</b> |

|                                                                   |                                                                                               |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Configure interface link layer protocol to Frame Relay            | <code>link-protocol fr [ ietf   nonstandard ]</code>                                          |
| Create frame-relay sub-interface and enter the sub-interface view | <code>interface type<br/>number.subinterface-number<br/>[multipoint   point-to-point ]</code> |
| Delete the frame-relay sub-interface                              | <code>undo interface type<br/>number.sub-number</code>                                        |

**b** Configure virtual circuit of Frame Relay sub-interface

In interface view, perform the following task to configure the virtual circuit of Frame Relay sub-interface.

**Table 283** Configure virtual circuit of Frame Relay sub-interface

| Operation                   | Command                               |
|-----------------------------|---------------------------------------|
| Configure a virtual circuit | <code>fr dlci dlci-number</code>      |
| Remove a virtual circuit    | <code>undo fr dlci dlci-number</code> |

**c** Configure Sub-Interface PVC and Establish Address Mapping

Since there is only one peer address for point-to-point sub-interface, the peer address is determined when a PVC is configured for the sub-interface. For point-to-multipoint sub-interface, the peer address and local DLCI can be determined by configuring static address mapping or using inverse address resolution protocol.

Establishing static address mapping of Frame Relay sub-interface

**Table 284** Establish static address mapping

| Operation                 | Command                                                                                                                                                                                                    |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Establish address mapping | <code>fr map { ip   ipx }<br/>protocol-address dlci dlci [<br/>broadcast ] [ nonstandard   ietf ]<br/>[ logic-channel channel_number ] [<br/>nocompress   compression vj ] [<br/>compression frf9 ]</code> |
| Delete an address mapping | <code>undo fr map { ip   ipx }<br/>protocol-address dlci dlci</code>                                                                                                                                       |

Applying dynamic address mapping to the sub-interface

**Table 285** Configure Frame Relay dynamic address mapping

| Operation                       | Command                                              |
|---------------------------------|------------------------------------------------------|
| Enable dynamic address mapping  | <code>fr inarp [ { ip   ipx } [ dlci ] ]</code>      |
| Disable dynamic address mapping | <code>undo fr inarp [ { ip   ipx } [ dlci ] ]</code> |

By default, all the sub-interfaces are enabled to use dynamic inverse-arp.

**8** Configure Frame Relay PVC Switching

Router routers can be used as Frame Relay switches to provide the function of Frame Relay PVC switching. There are two ways to configure the Frame Relay switching: configuring the Frame Relay switched route or configuring the Frame Relay switched PVC.

**a** Enable the Frame Relay switching

Perform “Enabling/Disabling Frame Relay PVC switching” in system view, and configure all the other commands in synchronous serial interface view.

**Table 286** Configure the Frame Relay PVC switching

| Operation                                          | Command                                      |
|----------------------------------------------------|----------------------------------------------|
| Enable the Frame Relay to carry out PVC switching  | <b>fr switching</b>                          |
| Disable the Frame Relay to carry out PVC switching | <b>undo fr switching</b>                     |
| Set the Frame Relay interface type                 | <b>fr interface-type { dte   dce   nni }</b> |

By default, Frame Relay PVC switching is disabled.

The configured PVC can take effect only when the type of Frame Relay interface is NNI or DCE.

**b** Configure Frame Relay switched route

Perform the following configurations in synchronous serial interface view.

**Table 287** Configure the Frame Relay local virtual circuit number

| Operation                                      | Command                         |
|------------------------------------------------|---------------------------------|
| Assign a PVC number for Frame Relay interface  | <b>fr dlci dlci-number</b>      |
| Delete the PVC number of Frame Relay interface | <b>undo fr dlci dlci-number</b> |

Perform the following configurations in interface view.

**Table 288** Configure the route for Frame Relay PVC switching

| Operation                                         | Command                                                           |
|---------------------------------------------------|-------------------------------------------------------------------|
| Configure the route for Frame Relay PVC switching | <b>fr dlci-switch in-dlci interface type number dlci out-dlci</b> |
| Delete the route for Frame Relay PVC switching    | <b>undo fr dlci-switch in-dlci</b>                                |

By default, the Frame Relay switched route is not configured.

PVC switching can take effect only when the **fr dlci-switch** command is configured on the two interfaces on the Frame Relay switched routers.

**c** Configure Frame Relay switched PVC

Perform the following configurations in interface view.

**Table 289** Configure Frame Relay local switched PVC number

| Operation                                                                  | Command                         |
|----------------------------------------------------------------------------|---------------------------------|
| Assign a switched PVC number for the main interface or the sub-interface   | <b>fr dlci dlci-number</b>      |
| Delete the switched PVC number for the main interface or the sub-interface | <b>undo fr dlci dlci-number</b> |

Perform the following configurations in system view.

**Table 290** Configure the Frame Relay switched PVC

| Operation                              | Command                                                                               |
|----------------------------------------|---------------------------------------------------------------------------------------|
| Configure the Frame Relay switched PVC | <b>fr switch name interface type number dlci dlci interface type number dlci dlci</b> |
| Delete the Frame Relay switched PVC    | <b>undo fr switch name</b>                                                            |

By default, no Frame Relay switched PVC is created.

After configuring the Frame Relay switched PVC, the user will enter the frame relay switch view to perform the operations of **shutdown** and **undo shutdown** on the switched PVC.



*The differences between configuring a Frame Relay switched route and configuring a Frame Relay switched PVC are listed below:*

1) A Frame Relay switched route can become valid only when it is configured on the two Frame Relay switched interfaces, whereas a Frame Relay switched PVC can become valid as soon as it is configured in system view for once.

2) After the Frame Relay switched PVC is configured, the user will enter the frame relay switch view. At this time, the user can perform the operations of **shutdown** and **undo shutdown** on the switched PVC. However, the user cannot do that on a Frame Relay switched route.

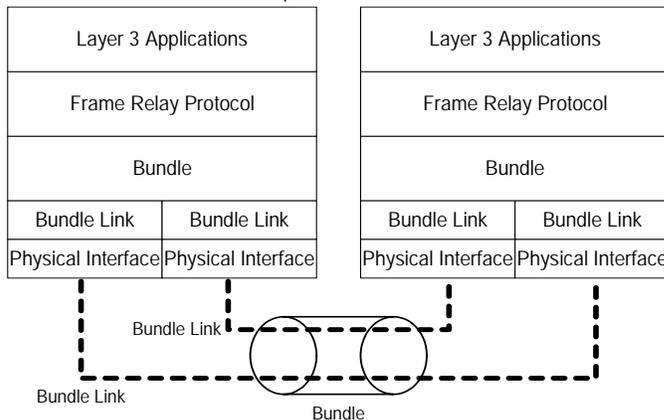
### Configure Multilink Frame Relay (FRF.16)

#### Overview

Multilink Frame Relay can bundle multiple low-rate Frame Relay links to form a Frame Relay with high rate and wide bandwidth. Multilink Frame Relay creates a virtual Frame Relay interface which contains multiple Frame Relay physical interfaces. In this way, the bandwidth of the virtual Frame Relay is equal to the sum of the bandwidth of each Frame Relay physical interface contained in the virtual Frame Relay interface.

The virtual Frame Relay interface is called "Bundle", and the physical interfaces contained in the virtual interface is called "bundle link". As for an actual physical layer, bundle link is equal to an analog data link layer, and bundle manages all the bundle links. As for data link layer, bundle is analog physical layer.

**Figure 80** Illustration of the relationship between bundle and bundle links



On the Router Routers, the virtual Frame Relay interface is called "MFR interface". One MFR interface corresponds to one bundle, and one physical interface corresponds to a bundle link. The management performed on the bundle and bundle link is actually the management to the MFR interface and the physical interface.

After the Frame Relay physical interface is bundle to an MFR interface, the network layer parameters and Frame Relay link layer parameters configured on it

will not take effect. On the MFR interface, you can configure the network layer parameters (e.g., IP address) and Frame Relay parameters (e.g., DLCI). The physical interface bundled on the MFR interface will use the parameters on the MFR interface.

### Configure MFR

The configuration tasks of the MFR are listed as follows:

- Configure a MFR Bundle
- Configure a MFR Bundle Link

#### 1 Configure a MFR bundle

Please perform the following configuration in system view.

**Table 291** Configure a MFR bundle interface (MFR interface)

| Operation                                 | Command                                                                    |
|-------------------------------------------|----------------------------------------------------------------------------|
| Configure or enter a MFR bundle interface | <b>interface mfr number [ .subnumber ] [ multipoint / point-to-point ]</b> |
| Remove a MFR bundle interface             | <b>undo interface mfr number [ .subnumber ]</b>                            |

By default, no MFR bundle interface is configured.

Please perform the following configuration in MFR interface view.

**Table 292** Configure MFR interface parameter

| Operation                                                             | Command                       |
|-----------------------------------------------------------------------|-------------------------------|
| configure bundle identification                                       | <b>mfr bundle-name name</b>   |
| Restore the default bundle identification                             | <b>undo mfr bundle-name</b>   |
| Set the maximum number of the fragments allowed by the MFR interface. | <b>mfr window-size number</b> |

The default bundle identification is "mfr" plus the bundle number, for example, "mfr1".

By default, the maximum number of the fragments allowed by the MFR interface is the same with the number of the physical interfaces bundled to it.

By default, the voice packets are sent on the multiple physical interfaces bundled to the MFR interface by turns.

#### 2 Configure a MFR bundle link

Please perform the following configuration in synchronous serial interface view.

**Table 293** Configure physical interface's link layer protocol to Multilink Frame Relay

| Operation                                                                                                         | Command                                     |
|-------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| Configure physical interface's link layer protocol to Multilink Frame Relay and associate the link with a bundle. | <b>link-protocol fr mfr number [ name ]</b> |

By default, no MFR bundle link is created. To remove the association between the physical interface and the MFR interface, configure the interface's link layer protocol to a none MFR type using the **link-protocol** command.

Please perform the following configuration in synchronous serial interface view.

**Table 294** Configure the parameters of the bundle link interface

| Operation                                                                                                                                  | Command                        |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| configure link identification of the multilink Frame relay bundle link                                                                     | <b>mfr link-name name</b>      |
| Restore the default link identification                                                                                                    | <b>undo mfr link-name</b>      |
| Set the time interval for the bundle link to send Hello messages                                                                           | <b>mfr timer hello seconds</b> |
| Restore the default of the time interval for the bundle link to send Hello messages                                                        | <b>undo mfr timer hello</b>    |
| Set the number of times that the Frame Relay bundle link waits for the acknowledge timer to time out successively                          | <b>mfr retry number</b>        |
| Restore the default value of the number of times that the Frame Relay bundle link waits for the acknowledge timer to time out successively | <b>undo mfr retry</b>          |
| Set the time that the Frame Relay bundle link waits for the remote end to acknowledge the Hello message                                    | <b>mfr timer ack seconds</b>   |
| Restore the default number of the time that the Frame Relay bundle link waits for the remote end to acknowledge the Hello message          | <b>undo mfr timer ack</b>      |

The default link identification is the name of its physical interface.

By default, a bundle link will send out hello message every 10 seconds; it will send a hello message a maximum of 3 times and wait 4 seconds for a hello message acknowledgement.

## Configure Frame Relay Payload Compression (FRF.9)

### Introduction to Frame Relay Payload Compression

Using the Frame Relay payload compression technique to compress Frame Relay packets can effectively save the network bandwidth, and reduce the network load, hence fulfilling the highly efficient data transmission over the Frame Relay networks.

The 3Com Routers adopt FRF.9 standard to implement Frame Relay payload compression. When applied to the Frame Relay lines with relatively low bandwidth, Frame Relay payload compression can achieve significant effect.

### Frame Relay Compression Configuration

Frame Relay interfaces fall into two types: point-to-point interface and multipoint interface. The methods of configuring Frame Relay payload compression are different for these two types of interfaces.

#### 1 Configure Frame Relay payload compression on point-to-point interface

Perform the following configurations in interface view.

**Table 295** Configure Frame Relay compression on point-to-point interface

| Compression                     | Command                         |
|---------------------------------|---------------------------------|
| Enable Frame Relay compression  | <b>fr compression frf9</b>      |
| Disable Frame Relay compression | <b>undo fr compression frf9</b> |

By default, Frame Relay payload compression is disabled.

On the 3Com Router, only the Frame Relay sub-interfaces can be point-to-point interfaces.

#### 2 Configure Frame Relay payload compression on multipoint interface

Perform the following configurations in interface view.

**Table 296** Configure Frame Relay Compression on multipoint interface

| Operation                                                                | Command                                                                              |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Create a Frame Relay map, and enable Frame Relay compression on the DLCI | <code>fr map { ip   ipx }<br/>protocol-address dlci dlci<br/>compression frf9</code> |
| Delete the Frame Relay map, and disable Frame Relay compression          | <code>undo fr map { ip   ipx }<br/>protocol-address dlci dlci</code>                 |

By default, Frame Relay payload compression is disable.

On the 3Com Router, both the Frame Relay main interfaces and sub-interfaces can be multipoint interfaces.

### Enable/Disable TCP/IP Header Compression on Interfaces

Frame Relay supports TCP/IP header compression. Only when the packet format of Frame Relay interface is **nonstandard**, can TCP/IP header compression be executed. TCP/IP header compression can be designated both on the interface and on configuring static address mapping.

Perform the following task in synchronous interface view.

**Table 297** Enable/Disable TCP/IP Header Compression on Interfaces

| Operation                                       | Command                                    |
|-------------------------------------------------|--------------------------------------------|
| Enable TCP/IP Header Compression on Interfaces  | <code>fr compression vj [ passive ]</code> |
| Disable TCP/IP Header Compression on Interfaces | <code>undo fr compression vj</code>        |

By default, interfaces use initiative compression.

### Configure Frame Relay Fragment (FRF.12)

#### 1 Configure Frame Relay Fragment Attributes

When voice and data are transmitted concurrently, transmission of a large data packet will occupy the bandwidth for a relatively long time. This will cause delay and even drop of voice packets behind it, and hence degrade the voice quality. The purpose of configuring Frame Relay fragmentation is to shorten voice delay and ensure real-time voice transmission. After configuring fragmentation, large packets will be fragmented into small data fragments. These smaller and less delay-causing data fragments and the voice packets are interspersed for transmission to ensure an even flow of voice packets into the networks.

**Table 298** Configure Frame Relay Fragment

| Operation                                                         | Command                                                                       |
|-------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Create a Frame Relay class                                        | <code>fr class class-name</code>                                              |
| Delete a Frame Relay class                                        | <code>undo fr class class-name</code>                                         |
| Configure the Frame Relay fragment size                           | <code>fragment fragment-size {<br/>data-level   voice-level }</code>          |
| Disable Frame Relay fragmentation                                 | <code>undo fragment [ fragment-size {<br/>data-level   voice-level } ]</code> |
| Associate a Frame Relay class with a Frame Relay interface or PVC | <code>fr-class class-name</code>                                              |

|                                                                                       |                                       |
|---------------------------------------------------------------------------------------|---------------------------------------|
| Remove the association between a Frame Relay class and a Frame Relay interface or PVC | <code>undo fr-class class-name</code> |
| Enable the Frame Relay traffic shaping                                                | <code>fr traffic-shaping</code>       |
| Disable the Frame Relay traffic shaping                                               | <code>undo fr traffic-shaping</code>  |

## Configure Frame Relay QoS

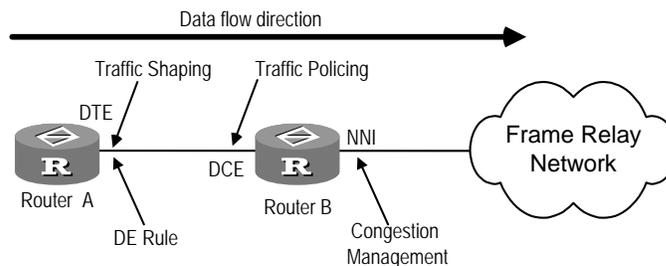
Quality of Service (QoS) is a set of technologies adopted to meet the users' requirements in throughput, delay jitter, delay and packet loss ratio. Briefly speaking, QoS technologies provides network services of different qualities for different requirements.

On a Frame Relay interface, the user can use the general QoS to provide the services, such as traffic policing, traffic shaping, congestion management, and congestion avoidance. For details, please refer to the relative description in the part of QoS.

Furthermore, a Frame Relay network has its own QoS mechanisms, including Frame Relay traffic shaping, Frame Relay traffic policing, Frame Relay congestion management, Frame Relay discard eligibility (DE) rule list and Frame Relay queueing management. According to different requirements, the network service provider can provide various services, such as bandwidth restriction and bandwidth reservation.

Compared with the general QoS, Frame Relay QoS can provide the service of QoS for each PVC on an interface. However, the general QoS can only provide the service of QoS on the whole interface. Therefore, the Frame Relay QoS can provide more flexible quality services for users.

**Figure 81** Frame Relay QoS application

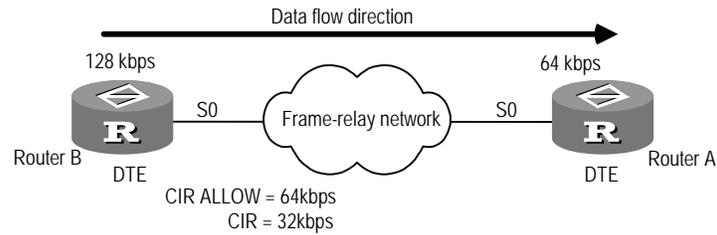


### Frame Relay Traffic Shaping

The Frame Relay traffic shaping can control the normal traffic size and the burst traffic size transmitted from a PVC and enable the Frame Relay PVC to transmit these packets at a relatively average rate.

In a Frame Relay network, the bottleneck will often occur at the boundary of segments if the bandwidths of different segments do not match. As shown in Figure 82, Router B transmits packets to Router A at the rate of 128 kbps whereas the maximum interface rate of Router A is only 64 kbps. In this case, the bottleneck will occur at the place where Router A is connected to the Frame Relay network, and thereby resulting in the congestion that prevents the data from normal transmitting.

**Figure 82** Frame Relay traffic shaping



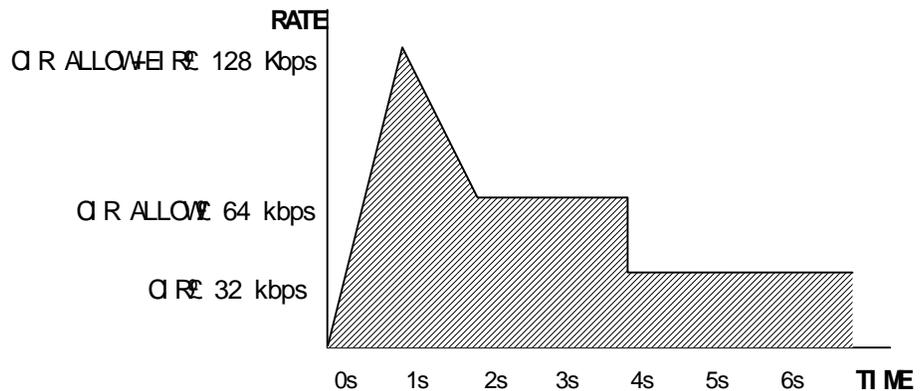
If the Frame Relay traffic shaping is applied on the outgoing interface Serial 0 on Router B, the interface will be able to transmit packets at 64 kbps, a relatively average rate, so as to avoid the network congestion. Even if the congestion occurs to the network, Router B can still transmit packets at 32 kbps.

Frame Relay traffic shaping is applied on the outgoing interface on a router. It can provide for the users the parameters like Committed Information Rate Allowed (CIR ALLOW), Committed Information Rate (CIR), Committed Burst Size (CBS) and Excess Burst Size (EBS).

When the network is in normal, the Frame Relay PVCs can transmit packets at the rate of CIR ALLOW. In this case, the packet traffic transmitted at an interval of Tc is CBS. Furthermore, the Frame Relay traffic shaping allows the PVCs to transmit packets at a rate exceeding CIR ALLOW in case of the burst, and the traffic exceeding the CBS can be EBS at maximum.

When the network congestion occurs, if the Frame Relay switch device has been configured with the function of congestion management, it will notify the router of network congestion. Upon receiving the notification, the router will eventually slow down the transmit rate to the CIR, so as to ease the congestion, then users can transmit data at the rate of CIR. After this, if no notifications of network congestion are received within a certain period of time, the router will eventually raise the transmit rate from the CIR back to the CIR ALLOW.

**Figure 83** Fundamentals of Frame Relay traffic shaping



As shown in Figure 83, the parameters of Frame Relay traffic shaping are respectively set to be: CIR ALLOW= 64 kbps, CIR = 32 kbps, CBS = 64000 bit, EBS = 64000 bit, and interval Tc = CBS / CIR ALLOW = 1s. Within the first interval Tc, the PVC-transmitting burst traffic size equals to CBS+EBS. Beginning from the second Tc, the transmitted traffic size within each interval Tc becomes CBS. At the 3s, the router receives the Frame Relay packet whose backward explicit congestion

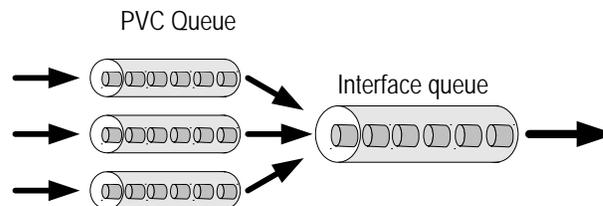
notification (BECN) flag bit is 1, indicating that the congestion has occurred to the network, and the transmit rate of the PVC will be lowered to CIR.

### Frame Relay Queuing Management

To ensure that the packets on the PVCs can be transmitted at an average rate in the process of Frame Relay traffic shaping, a queuing mechanism should be adopted to manage the packets. Generally, except that the Frame Relay interface owns one interface queue, the Frame Relay PVC does not have its own transmit queue. However, after the Frame Relay traffic shaping is enabled on the Frame Relay interface, all the PVCs belonging to this interface will own their independent queues, and all the packets transmitted from the PVCs will enter the Frame Relay PVC queues first.

Besides the Frame Relay PVC queues, the Frame Relay interface also owns an interface queue. In the case that the Frame Relay traffic shaping is not enabled, there will only be the Frame Relay interface queue. After it is enabled, both Frame Relay PVC queues and the Frame Relay interface queue will exist. Their relations are illustrated in Frame Relay queuing.

**Figure 84** Frame Relay queuing



The Frame Relay PVC queueing types include FIFO (First-In First-Out Queueing), PQ (Priority Queueing), CQ (Custom Queueing), and WFQ (Weighted Fair Queueing).

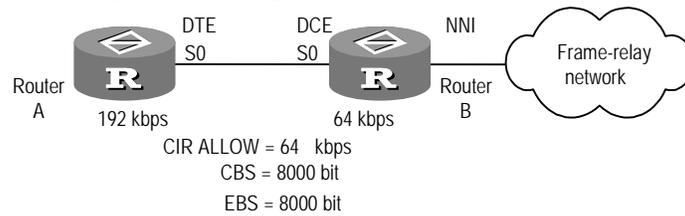
The FIFO, PQ, CQ, WFQ, and PIPQ (PVC Interface Priority Queueing) queues can be used on a Frame Relay interface. Among them, FIFO, PQ, CQ, and WFQ queues are general queues. For the detailed introduction, refer to the part of *QoS*. PIPQ can only be applied on the Frame Relay interface. It is similar to PQ, but aiming at the PVCs on an interface. When the Frame Relay traffic shaping is enabled on an interface, the queueing type on the interface can only be either FIFO or PIPQ.

PIPQ is applied on a Frame Relay interface. There are four types of PIPQ: top, middle, normal and bottom. Their queueing priorities are listed in descending order. The packets on the same PVC can only enter one type of PIPQ queue, and the packets on different PVCs enter different PIPQ queues on the interface, depending on the priorities of the PVCs. The PIPQ transmitting policy is as follows: Based on the queueing priority, transmit the packets in the queue with low priority after those in the queue with high priority are transmitted.

### Frame Relay Traffic Policing

Frame Relay policing monitors the traffic that flows into the network from each PVC, and restricts it in a certain range. If the traffic size on a PVC exceeds the range set by the user, the router will adopt the measures like discarding the packets, so as to protect the network resources and the profit of the operator.

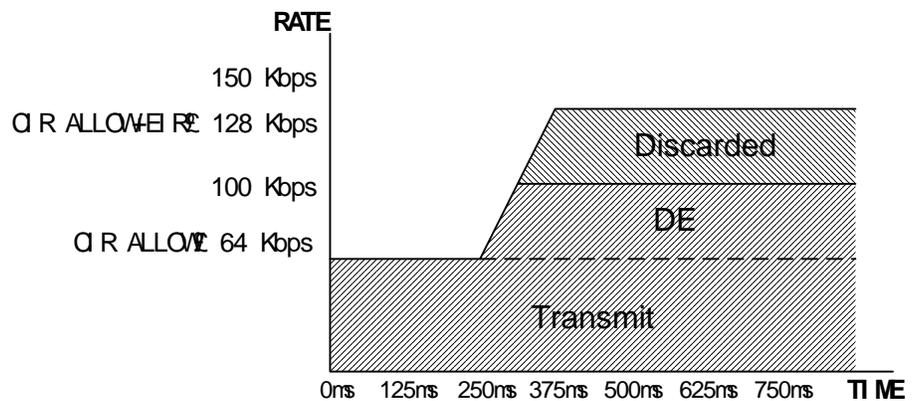
**Figure 85** Frame Relay traffic policing



As shown in the above figure, Router A at the user side transmits packets at 192 kbps to Router B at the switching side. However, Router B only wants to provide the 64 kbps bandwidth for Router A. In this case, you need to configure the Frame Relay traffic policing at the DCE side of Router B.

Frame Relay traffic policing can only be applied on the DCE interface on a router. It can monitor the traffic transmitted from the DTE side. When the traffic size is smaller than CBS, the packets can be normally transmitted, and the router will not process the packets. When the traffic size is larger than CBS and smaller than EBS + CBS, the packets can be normally transmitted. In this case, however, as for those packets in the traffic exceeding CBS, the router will mark the flag bit of DE in the Frame Relay packet headers to 1. When the traffic size is larger than CBS + EBS, the router will transmit the traffic within CBS + EBS, and discard the traffic exceeding CBS + EBS. As for the traffic of EBS which is the size exceeding CBS, the router will mark the flag bit of DE in the Frame Relay packet headers to 1.

**Figure 86** Fundamentals of Frame Relay traffic policing



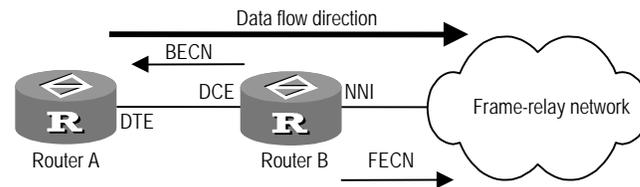
As shown in the above figure, the parameters of Frame Relay traffic policing are respectively set to be: CIR ALLOW = 64 kbps, CBS = 64000 bit, EBS = 64000 bit, and interval  $T_c = CBS / CIR ALLOW = 1s$ . When the interval is in the range of 0 to 2s, DTE will transmit packets to DCE at 64 kbps and DCE will normally forward these packets at 64 kbps. When the interval is in the range of 2 to 4ms, DTE will transmit packets at 100 kbps, and DCE will forward them at 100 kbps. In this case, however, the flag bit of DE in the headers of packets exceeding CBS will be set to 1. After 4 seconds, DTE will transmit the packets to DCE at 150 kbps, and DCE will forward them at 128 kbps. As for the packets exceeding CBS but within CBS + EBS, the flag bit of DE in their headers will be set to 1, and the packets exceeding CBS + EBS will be discarded directly.

### Frame Relay Congestion Management

Frame Relay congestion management can process the Frame Relay packets whenever there is network congestion. It will discard the packets that are marked with the DE flag bit. At the same time, it will notify other devices on the network about the congestion.

Frame Relay congestion management is applied at the output interface on a Frame Relay switched device. If there is no congestion, the router will normally forward the Frame Relay packets without doing any special processing on them. Once there is congestion, the packets that are marked with the DE flag bit will be discarded. As for the forward packets to be forwarded, the router will set the FECN flag bit in the Frame Relay packet headers to 1. As for the backward packets on the same PVC, the router will set the BECN flag bit in the Frame Relay packet headers to 1. If there is no backward packets to be forwarded after a certain period, the router will automatically transmit the Q922A Test Reponse packets with the BECN flag bit 1 to the calling DTE.

**Figure 87** Frame Relay congestion management



### Frame Relay DE rule list

In a Frame Relay network, the packets that are marked with DE flag bit will be first discarded once there is congestion. The DE rule lists are applied on the Frame Relay PVCs on a router, and each of them contains multiple DE rules. If a packet transmitted on a PVC complies with the rules in the DE rule list, its DE flag bit will be set to 1, and the packets like it will be discarded first if the congestion occurs on the network.

### Configure Frame Relay class

The 3Com Router system integrates the QoS on Frame Relay PVCs into Frame Relay class. Thereby, it provides a flexible overall solution to Frame Relay traffic control and quality service. Before configuring the QoS such as Frame Relay traffic shaping, you need to create a Frame Relay class, and configure various QoS parameters on it. Such a Frame Relay class equals to a set of QoS network service solution. Then, the user can associate it with a Frame Relay PVC. It is equivalent to applying a set of QoS scheme to the Frame Relay PVC. Different PVCs can use different Frame Relay classes as well as a single Frame Relay class.

Frame Relay class configuration includes:

- Create a Frame Relay class
  - Associate the Frame Relay class with the Frame Relay interface or a PVC
  - Configure the Frame Relay class parameters
- 1** Create a Frame Relay class

Perform the following configurations in system view.

**Table 299** Create/Delete a Frame Relay class

| Operation                  | Command                         |
|----------------------------|---------------------------------|
| Create a Frame Relay class | <b>fr class class-name</b>      |
| Delete a Frame Relay class | <b>undo fr class class-name</b> |

By default, no Frame Relay class is created.

After creating the Frame Relay class using this command, the user will enter the frame relay class view under which you can configure the parameters like CIR.

## 2 Associate the Frame Relay class with the Frame Relay interface or a PVC

Please configure the association between a Frame Relay class and an interface in interface view, and configure the association between a Frame Relay class and a PVC in DLCI view.

**Table 300** Associate the Frame Relay class with the Frame Relay interface or a PVC

| Operation                                                                             | Command                         |
|---------------------------------------------------------------------------------------|---------------------------------|
| Associate a Frame Relay class with a Frame Relay interface or PVC                     | <b>fr-class class-name</b>      |
| Remove the association between a Frame Relay class and a Frame Relay interface or PVC | <b>undo fr-class class-name</b> |

By default, no Frame Relay class is associated with the Frame Relay interface or the Frame Relay PVC.

When using the command **fr-class**, if the specified Frame Relay class does not exist, this command will first create a Frame Relay class (but not enter the frame relay class view) and then associate it with the current interface or PVCs.

The command **undo fr-class** will remove the association between the specified Frame Relay class and the interface/PVCs without deleting the actual Frame Relay class. In this case, if using the **display current-configuration** command to view the configurations of the router, you can still see the configuration of the Frame Relay class. To delete the Frame Relay class, use the **undo fr class** command.

When a Frame Relay PVC implements QoS, it will search for the corresponding Frame Relay class in the following sequence:

- If there is a Frame Relay class associated with the PVC, use the QoS parameters configured to the Frame Relay class.
- If there is no Frame Relay class associated with the PVC but a Frame Relay class associated with the interface to which the PVC belongs, use the QoS parameters configured to this Frame Relay class.

## 3 Configure the Frame Relay class parameters

In frame relay class view, the user can configure the parameters for the QoS, such as Frame Relay traffic shaping, Frame Relay traffic policing, Frame Relay congestion management, and Frame Relay queueing management. The following sections will cover the parameter settings in detail.

### Configure Frame Relay Traffic Shaping

Frame Relay traffic shaping configuration includes:

- Enable the Frame Relay traffic shaping
- Create a Frame Relay class
- Associate the Frame Relay class with the Frame Relay interface or a PVC

- Configure the parameters of Frame Relay class
- 1 Enable the Frame Relay traffic shaping

Perform the following configurations in synchronous serial interface view.

**Table 301** Enable/Disable the Frame Relay traffic shaping

| Operation                               | Command                        |
|-----------------------------------------|--------------------------------|
| Enable the Frame Relay traffic shaping  | <b>fr traffic-shaping</b>      |
| Disable the Frame Relay traffic shaping | <b>undo fr traffic-shaping</b> |

By default, the Frame Relay traffic shaping is not enabled on the interface.

The function of Frame Relay traffic shaping is applied on the outgoing interfaces on a router. Usually it is applied at the DTE end on a Frame Relay network.

- 2 Create a Frame Relay class

Refer to the previous section “Configure Frame Relay class” for the configuration procedure in detail.

- 3 Associate the Frame Relay class with the Frame Relay interface or a PVC

Refer to the previous section “Configure Frame Relay class” for the configuration procedure in detail.

- 4 Configure the Frame Relay class parameters for Frame Relay traffic shaping

Perform the following configurations in frame relay class view.

**Table 302** Configure the parameters of Frame Relay class

| Operation                                                                 | Command                                               |
|---------------------------------------------------------------------------|-------------------------------------------------------|
| Set the CBS of a Frame Relay PVC                                          | <b>cbs [ outbound ] burst-size</b>                    |
| Restore the CBS of a Frame Relay PVC to the default value                 | <b>undo cbs [ outbound ]</b>                          |
| Set the EBS of a Frame Relay PVC                                          | <b>ebs [ outbound ] excess-burst-size</b>             |
| Restore the EBS of a Frame Relay PVC to the default value                 | <b>undo ebs [ outbound ]</b>                          |
| Set the CIR ALLOW of a Frame Relay PVC                                    | <b>cir allow [ outbound ] rate-limit</b>              |
| Restore the CIR ALLOW of a Frame Relay PVC to the default value           | <b>undo cir allow [ outbound ]</b>                    |
| Set the CIR of a Frame Relay PVC                                          | <b>cir rate-limit</b>                                 |
| Restore the CIR of a Frame Relay PVC to the default value                 | <b>undo cir</b>                                       |
| Enable the adaptive adjustment function of traffic shaping                | <b>traffic-shaping adaptation becn [ percentage ]</b> |
| Disable the adaptive adjustment function of traffic shaping               | <b>undo traffic-shaping adaptation becn</b>           |
| Set the reserved band width of Frame Relay PVC                            | <b>reserved-bandwidth bandwidth-percentage</b>        |
| Restore the reserved band width of a Frame Relay PVC to the default value | <b>undo reserved-bandwidth</b>                        |

The commands **cbs**, **ebs**, and **cir allow** can be used to set the **inbound** and **outbound** parameters. However, only the **outbound** parameters are effective for the Frame Relay traffic shaping.



Numerically, the value of CBS should not be less than CIR ALLOW, otherwise, the large packets may not be sent.

## Configure Frame Relay Traffic Policing

Frame Relay traffic policing configuration includes:

- Enable the Frame Relay traffic policing
- Create a Frame Relay class
- Associate the Frame Relay class with the Frame Relay interface or a PVC

Configure the parameters of Frame Relay class for Frame Relay traffic policing

### 1 Enable the Frame Relay Traffic Policing

Perform the following configurations in synchronous serial interface view.

**Table 303** Enable/Disable the Frame Relay traffic policing

| Operation                                | Command                         |
|------------------------------------------|---------------------------------|
| Enable the Frame Relay traffic policing  | <b>fr traffic-policing</b>      |
| Disable the Frame Relay traffic policing | <b>undo fr traffic-policing</b> |

By default, the Frame Relay traffic policing is not enabled on the interface.

The function of Frame Relay traffic policing is applied on the interface receiving the Frame Relay packets on a router. It can only be applied at the DCE side on a Frame Relay network.

### 2 Create a Frame Relay class

Please refer to the above section “Configure Frame Relay class” for the configuration procedure in detail.

### 3 Associate the Frame Relay class with the Frame Relay interface or a PVC

Please refer to the above section “Configure Frame Relay class” for the configuration procedure in detail.

### 4 Configure the parameters of Frame Relay class for Frame Relay traffic policing

Perform the following configurations in frame relay class view.

**Table 304** Configure the parameters of Frame Relay class

| Operation                                                       | Command                                  |
|-----------------------------------------------------------------|------------------------------------------|
| Set the CBS of a Frame Relay PVC                                | <b>cbs [ inbound ] burst-size</b>        |
| Restore the CBS of a Frame Relay PVC to the default value       | <b>undo cbs [ inbound ]</b>              |
| Set the EBS of a Frame Relay PVC                                | <b>ebs [ inbound ] excess-burst-size</b> |
| Restore the EBS of a Frame Relay PVC to the default value       | <b>undo ebs [ inbound ]</b>              |
| Set the CIR ALLOW of a Frame Relay PVC                          | <b>cir allow [ inbound ] rate-limit</b>  |
| Restore the CIR ALLOW of a Frame Relay PVC to the default value | <b>undo cir allow [ inbound ]</b>        |

The commands **cbs**, **ebs**, and **cir allow** can be used to set the **inbound** and **outbound** parameters on a PVC. However, only the **inbound** parameters are effective for the Frame Relay traffic policing.

## Configure Frame Relay Congestion Management

There are two ways to set the congestion threshold. One is to configure the congestion threshold for a PVC in a specified Frame Relay class, another is to configure the congestion threshold for the overall interface in interface view. The router determines whether there is congestion on the interface according to the ratio that the current queue length on the Frame Relay interface or PVC occupies the total queue length on the interface. If the ratio is greater than the threshold set by the user, the router will assume that there is congestion, and will process the packets with the corresponding methods, such as discarding.

Frame Relay congestion management include the congestion management on the Frame Relay interface and the congestion management on the Frame Relay PVC.

- 1 Configure the congestion management policy on a Frame Relay interface  
Perform the following configurations in synchronous serial interface view.

**Table 305** Configure the congestion management policy on a Frame Relay interface

| Operation                                                                                                           | Command                                             |
|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Enable a Frame Relay interface to discard the packets that are marked with DE flag bit in the case of congestion    | <b>fr congestion-threshold de queue-percentage</b>  |
| Disable the Frame Relay interface to discard the packets that are marked with DE flag bit in the case of congestion | <b>undo fr congestion-threshold de</b>              |
| Enable a Frame Relay interface to process the BECN and FECN flag bits in the case of congestion                     | <b>fr congestion-threshold ecn queue-percentage</b> |
| Disable the Frame Relay interface to process the BECN and FECN flag bits in the case of congestion                  | <b>undo fr congestion-threshold ecn</b>             |

By default, the congestion management is not enabled on a Frame Relay interface. When the congestion management is enabled on a Frame Relay interface, the queueing type on the interface can only be either FIFO or PIFO.

- 2 Configure the congestion management policy on Frame Relay PVC  
Perform the following configurations in frame relay class view.

**Table 306** Configure the congestion management policy on a Frame Relay PVC

| Operation                                                                                                     | Command                                          |
|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Enable a Frame Relay PVC to discard the packets that are marked with DE flag bit in the case of congestion    | <b>congestion-threshold de queue-percentage</b>  |
| Disable the Frame Relay PVC to discard the packets that are marked with DE flag bit in the case of congestion | <b>undo congestion-threshold de</b>              |
| Enable the Frame Relay PVC to process the BECN and FECN bits in the case of congestion                        | <b>congestion-threshold ecn queue-percentage</b> |
| Disable the Frame Relay PVC to process the BECN and FECN bits in the case of congestion                       | <b>undo congestion-threshold ecn</b>             |

By default, the congestion management is not enabled on Frame Relay PVCs. When the congestion management is enabled on a Frame Relay PVC, the queueing type on the PVC can only be FIFO.



*Only when the Frame Relay traffic shaping is enabled on the interface where a PVC is located, can the congestion management take effect on the PVC.*

## Configure Frame Relay DE Rule List

### 1 Configure a DE rule list

Perform the following configurations in system view.

**Table 307** Configure a DE rule list

| Operation                                 | Command                                                                 |
|-------------------------------------------|-------------------------------------------------------------------------|
| Configure an interface-based DE rule list | <b>fr del list-number<br/>inbound-interface type number</b>             |
| Delete the interface-based DE rule        | <b>undo fr del list-number<br/>inbound-interface type number</b>        |
| Configure a protocol-based DE rule list   | <b>fr del list-number protocol<br/>protocol [ characteristic ]</b>      |
| Delete the protocol-based DE rule         | <b>undo fr del list-number protocol<br/>protocol [ characteristic ]</b> |

By default, no DE rule list is defined.

A router can support up to 10 DE rule lists, and each of them can contain up to 100 DE rules.

The commands **fr del inbound-interface** and **fr del protocol** can be used to add multiple rules to a DE rule list. The commands **undo fr del inbound-interface** and **undo fr del protocol** can delete one DE rule each time. To delete a DE rule list, the user should delete all the DE rules in it.

### 2 Apply the DE rule list on a Frame Relay PVC

Perform the following configurations in synchronous serial interface view.

**Table 308** Apply the DE rule list on a Frame Relay PVC

| Operation                                      | Command                                           |
|------------------------------------------------|---------------------------------------------------|
| Apply the DE rule list on a Frame Relay PVC    | <b>fr de del list-number dlci-number</b>          |
| Delete a DE rule list from the Frame Relay PVC | <b>undo fr de del list-number<br/>dlci-number</b> |

By default, no DE rule lists are applied on Frame Relay PVCs.

## Configure Frame Relay Queueing Management

### 1 Configure the Frame Relay PVC queueing

After the Frame Relay traffic shaping is enabled on a Frame Relay interface, each PVC under this interface will own its independent PVC queue. If the function is not enabled on the Frame Relay interface, the PVCs will have no PVC queues.

Perform the following configurations in frame relay class view.

**Table 309** Configure the Frame Relay PVC queueing

| Operation                                                               | Command                             |
|-------------------------------------------------------------------------|-------------------------------------|
| Set the FIFO queue length of a Frame Relay PVC                          | <b>fifo queue-length queue-size</b> |
| Restore the FIFO queue length of a Frame Relay PVC to the default value | <b>undo fifo queue-length</b>       |
| Set the queue type of a Frame Relay PVC to PQ                           | <b>pq pql list-number</b>           |
| Restore the queue type of a Frame Relay PVC to FIFO                     | <b>undo pq pql</b>                  |

|                                                     |                                                                |
|-----------------------------------------------------|----------------------------------------------------------------|
| Set the queue type of a Frame Relay PVC to CQ       | <b>cq cql list-number</b>                                      |
| Restore the queue type of a Frame Relay PVC to FIFO | <b>undo cq cql</b>                                             |
| Set the queue type of a Frame Relay PVC to WFQ      | <b>wfq [ congestive-discard-threshold [ dynamic-queues ] ]</b> |
| Restore the queue type of a Frame Relay PVC to FIFO | <b>undo wfq</b>                                                |

By default, the queue type of a Frame Relay PVC is FIFO.

When the congestion management is enabled on Frame Relay PVCs, the queue type on the interface can only be FIFO.

For the configuration of PQ, CQ and WFQ, refer to the part of *QoS*.

## 2 Configure Frame Relay Interface Queueing

The user can configure four queueing types on a Frame Relay interface: FIFO, PQ, CQ and WFQ. All of them are the queues owned by a general QoS. For their configurations, refer to the part of *QoS*.

Frame Relay interface also supports PVC interface priority queueing (PIPQ). This queueing type can only be applied on a Frame Relay interface. After Frame Relay traffic shaping or Frame Relay congestion management is enabled on a Frame Relay interface, the queueing type on the interface can only be either FIFO or PIPQ.

A PIPQ queue classifies the packets into four categories according to different Frame Relay PVCs.

A PIPQ queue has four sub-queues. They are respectively high-priority queue (**top**), medium-priority queue (**middle**), normal-priority queue (**normal**) and low-priority queue (**bottom**). The priorities are listed in descending order. The packets will be transmitted according to the priority sequence. Specifically, all the packets in the **top** queue will be first transmitted, then the packets in the **middle** queue followed by the packets in the **normal** queue, and finally those in the **bottom** queue. Each Frame Relay PVC on the interface has its own PIPQ priority. Therefore, the packets from this PVC can only enter the corresponding PIPQ queue.

Perform the following configurations respectively in interface view and frame relay class view.

**Table 310** Configure PIPQ

| Operation                                                                                                                         | Command                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Set the queueing type of Frame Relay interface to PIPQ and set the length of each PIPQ queue at the same time (in interface view) | <b>fr pvc-pq [ top-limit middle-limit normal-limit bottom-limit ]</b> |
| Restore the queueing type of Frame Relay interface to FIFO (in interface view)                                                    | <b>undo fr pvc-pq</b>                                                 |
| Set the priority of PIPQ on the Frame Relay PVC (in frame relay class view)                                                       | <b>pvc-pq { top   middle   normal   bottom }</b>                      |
| Restore the priority of PIPQ on the Frame Relay PVC to <b>normal</b> (in frame relay class view)                                  | <b>undo pvc-pq</b>                                                    |

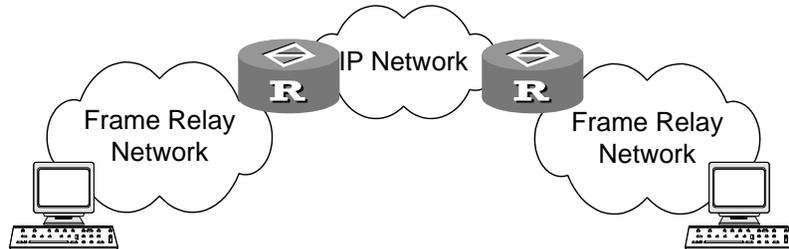
By default, the queueing type of a Frame Relay interface is FIFO.

## Configure Frame Relay over Other Protocols

### Frame Relay over IP

IP networks are used to carry the Frame Relay data to interconnect the Frame Relay networks. In the technique of Frame Relay over IP, a GRE tunnel is established between the Frame Relay networks at both ends of IP, and the Frame Relay data are carried over IP. The application of Frame Relay over IP is illustrated in the following figure:

**Figure 88** Typical application of Frame Relay over IP



### Configure Frame Relay over IP

#### 1 Configure tunnel interface

Create a tunnel interface in all views or enter the tunnel interface view to perform the following configurations.

**Table 311** Configure a tunnel interface

| Operation                                              | Command                                         |
|--------------------------------------------------------|-------------------------------------------------|
| Create a tunnel interface                              | <code>interface tunnel<br/>tunnel-number</code> |
| Specify a source address for the tunnel interface      | <code>source ip-address</code>                  |
| Specify a destination address for the tunnel interface | <code>destination ip-address</code>             |

In addition, the user can make the configurations, such as packet mode, ID keyword, for the tunnel interface. The tunnel interface configuration details will not be covered here. Please read the related chapters in *Operation manual - VPN* for reference.

#### 2 Configure Frame Relay Switching

Enable Frame Relay switching in system view and configure Frame Relay switched routes in serial interface view.

**Table 312** Configure Frame Relay switching

| Operation                              | Command                                                                      |
|----------------------------------------|------------------------------------------------------------------------------|
| Enable Frame Relay switching           | <code>fr switching</code>                                                    |
| Configure a Frame Relay switched route | <code>fr dlci-switch in-dlci<br/>interface tunnel number<br/>out-dlci</code> |

If the specified tunnel interface does not exist when implementing configuration, the system will automatically create a tunnel interface. However, the Frame Relay switched route can take effect only after the source address, destination address, and IP address have been configured for the tunnel interface.

After configuring the Frame Relay route through the `fr dlci-switch interface tunnel` command, two routes will be added to the Frame Relay routing table on the router. One route takes the tunnel interface as the incoming interface and the serial interface as the outgoing interface. On the contrary, the other route takes the serial interface as the incoming interface and the tunnel interface as the outgoing interface.

After the Frame Relay route is configured through the `fr dlci-switch interface tunnel` command, a PVC will be created on the tunnel interface and assigned with a DLCI number *out-dlci*. When implementing configuration, make sure that the same DLCI number (that is, *out-dlci*) should be used on the tunnel interfaces at two ends of the GRE tunnel.

### Frame Relay over ISDN

Nowadays, Frame Relay technique has gained wide applications, in which, most devices are accessed to the Frame Relay networks via leased lines. To shorten the time for users to access Frame Relay networks and lower the cost of leased lines, ISDNs and the related devices can be used to access Frame Relay networks, the so-called Frame Relay over ISDN.

With the Frame Relay over ISDN technique, the cost of a leased line can be shared by the routers, so the overall cost is lowered. The users can access the Frame Relay networks much quicker and with lower cost. At the same time, ISDN can also be taken as a standby for Frame Relay accessing. Therefore, the Frame Relay over ISDN is mainly used in the following two aspects:

- The simplest application is to take Frame Relay over ISDN as the main communications method. That is, all the routers support Frame Relay over ISDN, and the individual routers can directly access the Frame Relay networks (without TA adapters) to communicate.
- Combined with BDR, Frame Relay over ISDN can be taken as the standby communication method for Frame Relay. In such applications, routers support Frame Relay over ISDN. Being the standby for a Frame Relay network, ISDN can be used to re-establish the connections for accessing the Frame Relay network, whenever a Frame Relay accessing line/device fails to work or the Frame Relay network is blocked.

### Frame Relay over ISDN Operation Process and Fundamentals

The following figure shows a typical networking for Frame Relay accessing, in which all the routers support Frame Relay over ISDN:

**Figure 89** Networking of a typical Frame Relay over ISDN application



RouterA, RouterB and RouterC support Frame Relay over ISDN. Being DTE devices, they and RouterD transmit Frame Relay packets over ISDN B channels. RouterD, which works as a DCE device, supports both Frame Relay over ISDN and Frame Relay switching. A simplified working procedure is shown below:

- RouterA (DTE device) originates a call on the BRI interface to the PRI interface on RouterD (DCE device).

- The DCE device identifies the calling number of the incoming call and authenticates the DTE device according to it to determine whether to accept or deny the call.
- If the DTE device passes the authentication, it can establish a B channel to the DCE device for carrying out the Frame Relay communications.



Normally, if a DCE device is connected to multiple DTE devices, calls can only be originated from the DTE side. However, it is not the case for back-to-back connections.



Binding of multiple B channels is not supported. After a call is successfully made, a DTE device and a DCE device can only be connected via a B channel.



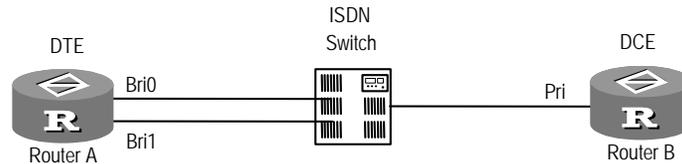
Since a B channel can only be connected to a remote end and cannot have more than one IP addresses, it cannot be configured with multiple DLCIs, nor configured with multiple sub-interfaces.

### Physical Connection Between Frame Relay over ISDN Devices

- Back-to-back connection between DTE and DCE devices

The DTE and DCE devices are connected to ISDN via ISDN (BRI or PRI) interfaces, and both ends can make calls, as shown in the following figure:

**Figure 90** Back-to-back connection between DTE and DCE devices



If legacy BDR is adopted on the ISDN interface used with Frame Relay, the calling party can directly use the configured dial string to make an ISDN call to the remote end, after it finds an available B channel. If dialer profiles are adopted, the calling party will re-configure the selected available B channel with the link layer protocol on the dialer interface, and then use the configured dial string to place an ISDN call to the remote end.

After a physical B channel is set up, Frame Relay LMI (Local Management Interface) and inverse ARP process will start. If an agreement is reached through the negotiation, Frame Relay will be used to carry the network layer data on the B channel.

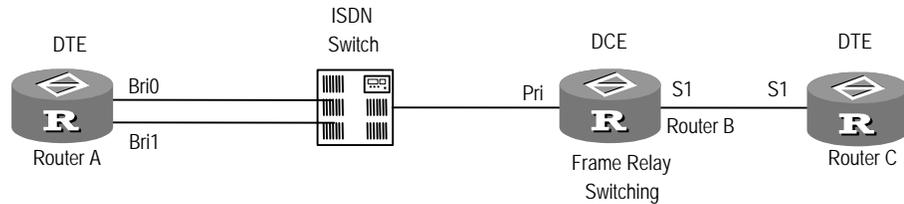


If dialer profiles are adopted, the called party searches for the dialer interface according to the dialing number in the ISDN packet. If the dialer interface is found, the called party will re-configure the selected B channel with the link layer protocol on the dialer interface. If the dialer interface is not found but the **dialer call-in** command has been configured, it will disconnect the call. If the **dialer call-in** command is not configured, PPP will be adopted by default. Therefore, each dialer interface of the called party should be configured with a unique dialing number, and can only receive the calls from that number. This restriction, however, is not placed on the calling parties.

- Frame Relay switching connection between DTE devices

A DCE device provides Frame Relay switching. Its one end is connected to a DTE device via ISDN, and the other end is directly connected to another DTE device, as shown in the following figure:

**Figure 91** Frame Relay switching connection between DTE devices



The DCE device cannot originate a call, since the PVC segment that the DCE device establishes via ISDN can only be activated through dialing. The call can only be originated by the DTE device, which is connected to ISDN. After the call is successfully made, the corresponding PVC segment is established for transmitting the network layer data.

If legacy BDR is adopted on the ISDN interface worked with Frame Relay on the DCE device, the calling party will use the configured dial string to make an ISDN call to the DCE device. If dialer profiles are adopted, the calling party (the DTE device) will re-configure the selected available B channel with the link layer protocol on the dialer interface, and then use the configured dial string to make an ISDN call to the DCE device.

After a physical B channel is set up, Frame Relay LMI and inverse ARP process will start. If an agreement is reached through the negotiation, the corresponding PVC will be established. Then, the DCE device will look for another PVC segment according to the Frame Relay switching configuration and activate the PVC segment. When both PVC segments are in active status, it means that the whole PVC is set up. In this case, Frame Relay can be adopted on the B channel to carry the network layer data.



*Distinguished from legacy BDR, dialer profiles require a called party to search for the dialer interface according to the dialing number in the ISDN packet, and hence obtain the link layer protocol type for the B channel. Then, the called party can dynamically configure the dialer interface or physical ISDN interface and initialize it.*

### Configure Frame Relay over ISDN

Frame Relay over ISDN provides a means for accessing devices from ISDN to a Frame Relay network. Its implementation fully depends on the techniques of Frame Relay and BDR. This section only covers the Frame Relay over ISDN-related commands. For configuration details and commands, refer to the Frame Relay and BDR Configuration in this manual.

#### 1 Related Frame Relay Configuration

Only some simple Frame Relay configurations are covered in this section. For other configurations, refer to the *Link Layer Protocol*.

Perform the following configuration in synchronous serial interface view.

**Table 313** Configure the Frame Relay-related commands

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                                                                |                                                                                                                                                                                  |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure the synchronous serial interface with Frame Relay    | <b>link-protocol fr [ ietf   nonstandard ]</b>                                                                                                                                   |
| Set the Frame Relay interface type                             | <b>fr interface-type { dte   dce   nni }</b>                                                                                                                                     |
| Add a static address map                                       | <b>fr map { ip   ipx } protocol-address dlci dlci [ broadcast ] [ nonstandard   ietf ] [ logic-channel channel_number ] [ nocompress   compression vj ] [ compression frf9 ]</b> |
| Assign a DLCI number for the main interface or a sub-interface | <b>fr dlci dlci-number</b>                                                                                                                                                       |

## 2 Configuration Related to Frame Relay Switching

Only some simple Frame Relay switching configurations are covered in this section. For other configurations, refer to the *Link Layer Protocol*.

Configure the commands **fr switch** and **fr switching** in system view, and perform other configurations in synchronous serial interface view.

**Table 314** Configure the commands related to Frame Relay switching

| Operation                                                    | Command                                                                               |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Enable Frame Relay to implement PVC switching                | <b>fr switching</b>                                                                   |
| Configure a terminal type for a Frame Relay interface        | <b>fr interface-type { dte   dce   nni }</b>                                          |
| Assign DLCI number for the main interface or a sub-interface | <b>fr dlci dlci-number</b>                                                            |
| Configure a Frame Relay switched virtual circuit (SVC)       | <b>fr switch name interface type number dlci dlci interface type number dlci dlci</b> |



*In addition to Frame Relay switching connections between serial interfaces, the **fr switch** command also supports the Frame Relay switching connections between ISDN BRI, ISDN PRI and dialer interfaces.*

## 3 BDR-related Configuration

### ■ Adopt legacy BDR

If legacy BDR is adopted to implement Frame Relay over ISDN, the user can refer to *Dial-up* of this manual for all the configurations except for the link layer protocol on the dialer or physical ISDN interface. The link layer protocol should be configured through the **link-protocol fr** command.

Perform the following configuration in physical ISDN or dialer interface view.

**Table 315** Configure the link layer protocol of the interface

| Operation                                                         | Command                                        |
|-------------------------------------------------------------------|------------------------------------------------|
| Configure the link layer protocol of the interface to Frame Relay | <b>link-protocol fr [ ietf   nonstandard ]</b> |



*The two ends of a BDR call should work with the same link layer protocol.*



*For a physical interface (such as an ISDN BRI or PRI interface), both the D channel and B channel are configured with Frame Relay.*



*In the legacy BDR implementation of Frame Relay over ISDN, a dialer interface and all the ISDN physical interfaces (including BRI and PRI interfaces) attached to it will be configured with Frame Relay.*

- Adopt dialer profiles

In the dialer profiles implementation of Frame Relay over ISDN, the **dialer number** command must be configured, besides using the **link-protocol fr** command to change the link layer protocol on the interface. The configuration is necessary because the negotiation of user name is disabled after the dialer interface is configured with Frame Relay, so the called party will identify different dialer interfaces according to the dial strings of the calling parties. In this case, however, there is no need to configure the **dialer user** command. In addition, the **dialer call-in** command must be configured for the called party to pre-process a dial-in number, thereby to determine whether the user dialing the number should be accessed. For other configurations, refer to the *Dial-up*.

Perform the following configuration in physical ISDN or dialer interface view.

**Table 316** Configure parameters related to dialer profiles

| Operation                                          | Command                                                      |
|----------------------------------------------------|--------------------------------------------------------------|
| Configure a dialer interface with Frame Relay      | <b>link-protocol fr</b> [ <i>ietf</i>   <i>nonstandard</i> ] |
| Enable dialer profiles                             | <b>dialer bundle number</b>                                  |
| Configure the dial string for calling a remote end | <b>dialer number dial-string</b> [ <i>:isdn_subaddress</i> ] |
| Pre-process ISDN dial-in numbers                   | <b>dialer call-in remote-number</b> [ <i>callback</i> ]      |



*The two ends of a BDR call should work with the same link layer protocol.*



*For a dialer interface adopting dialer profiles to implement Frame Relay over ISDN, it should be configured with Frame Relay. In addition, Frame Relay and PPP are probably carried on a B channel for supporting the dynamic configuration on the channel. Therefore, the ISDN physical interface should be configured with PPP. After the dynamic B channel is disconnected, the link layer protocol of the ISDN interface will be automatically restored to PPP (by default, physical interface will inherit the configurations of dialer interface).*



*Multiple **dialer number** is allowed to configure for the calling party, which is the so-called dialer string rotary backup. For the called party, after a dialer interface link layer protocol is configured to Frame Relay, the **dialer numbers** configured on other dialer interfaces cannot be the same **dialer number** configured on it. Otherwise, calls will fail.*

## Display and debug Frame Relay

Please use the **display** and **debugging** commands in all views.

**Table 317** Display and Debug Frame Relay

| Operation                                                                        | Command                                                     |
|----------------------------------------------------------------------------------|-------------------------------------------------------------|
| Display receiving/sending statistics information of Frame Relay LMI type packets | <b>display fr lmi-info</b> [ <i>interface type number</i> ] |
| Display protocol address and Frame Relay address mapping table                   | <b>display fr map-info</b>                                  |

|                                                                                           |                                                                                              |
|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Display Frame Relay data receiving/sending statistics information.                        | <code>display fr statistics [ interface type number ]</code>                                 |
| Display the Frame Relay PVC statistics                                                    | <code>display fr pvc-info [ serial number ] [ dlci dlci-number ]</code>                      |
| Display Frame Relay PVC route table                                                       | <code>display fr dlci-switch</code>                                                          |
| Display Frame Relay switch PVC route table                                                | <code>display fr switch-table</code>                                                         |
| Display Frame Relay protocol status of each interface                                     | <code>display fr interface</code>                                                            |
| Display statistics information of Frame Relay inverse address resolution protocol packets | <code>display fr inarp-info</code>                                                           |
| Display the statistics of MFR bundle and bundle link                                      | <code>display mfr [ interface mfr number   interface serial number ] [ detailed ]</code>     |
| Display the statistics of Frame Relay compression                                         | <code>display fr compression</code>                                                          |
| Display statistics information of MFR interface                                           | <code>display interfaces mfr number</code>                                                   |
| Clear all the automatically established Frame Relay address mappings                      | <code>reset fr inarp-info</code>                                                             |
| Enable all the debugging of Frame Relay                                                   | <code>debugging fr all [ interface type number ]</code>                                      |
| Enable the debugging of Frame Relay annexg                                                | <code>debugging fr annexg [ interface type number ] [ dlci ]</code>                          |
| Enable the debugging of Frame Relay arp                                                   | <code>debugging fr arp [ interface type number ]</code>                                      |
| Enable the debugging of Frame Relay compression                                           | <code>debugging fr compress [ interface type number ]</code>                                 |
| Enable the debugging of Frame Relay congestion                                            | <code>debugging fr congestion [ interface type number ]</code>                               |
| Enable the debugging of Frame Relay DE message                                            | <code>debugging fr de [ interface type number ]</code>                                       |
| Enable the debugging of Frame Relay DLCI queue                                            | <code>debugging fr dlciqueue interface type number dlci dlci-number</code>                   |
| Enable the debugging of Frame Relay event                                                 | <code>debugging fr event [ interface type number ]</code>                                    |
| Enable the debugging of Frame Relay fragment                                              | <code>debugging fr fragment interface type number dlci</code>                                |
| Enable the debugging of Frame Relay lmi                                                   | <code>debugging fr lmi [ interface type number ]</code>                                      |
| Display the debug messages for the MFR bundles and bundle links                           | <code>debugging fr mfr [ control [ interface mfr number   interface serial number ] ]</code> |
| Enable the debugging of Frame Relay packet                                                | <code>debugging fr packet [ interface type number [ dlci ] ] [ hex   detail   all ]</code>   |
| Enable the debugging of Frame Relay PIPQ                                                  | <code>debugging fr pipq [ interface type number ]</code>                                     |
| Enable the debugging of Frame Relay status                                                | <code>debugging fr status [ interface type number [ dlci ] ]</code>                          |
| Enable the debugging of Frame Relay traffic rate                                          | <code>debugging fr transmit-rate [ interface type number ]</code>                            |

## Typical Frame Relay Configuration Example

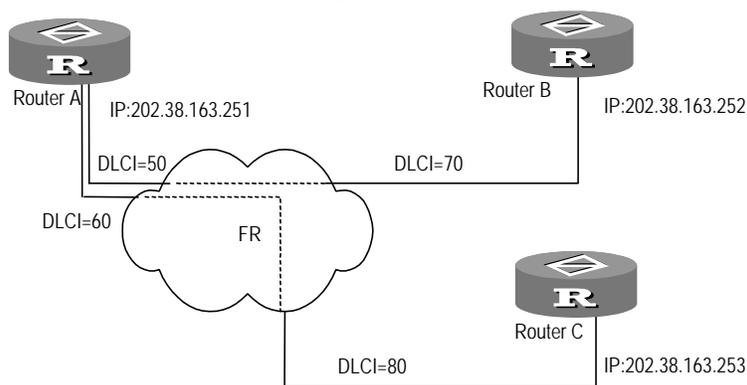
### Interconnect LANs via Frame Relay Network

#### I. Networking Requirement

Interconnect LANs via the public Frame Relay network. The routers work as user equipment in the Frame Relay DTE mode. The routers use static address mapping.

#### II. Networking Diagram

**Figure 92** Interconnect LANs via Frame Relay network



#### III. Configuration Procedure

##### 1 Configure Router A:

###### a Configure interface IP address

```
[Router]interface serial 1
[Router-Serial1]ip address 202.38.163.251 255.255.255.0
```

###### b Configure the link layer protocol of the interface to Frame Relay

```
[Router-Serial1]link-protocol fr
[Router-Serial1]fr interface-type dte
```

###### c Configure static address mapping

```
[Router-Serial1]fr map ip 202.38.163.252 dlci 50
[Router-Serial1]fr map ip 202.38.163.253 dlci 60
```

##### 2 Configure Router B:

###### a Configure interface IP address

```
[Router]interface serial 1
[Router-Serial1] ip address 202.38.163.252 255.255.255.0
```

###### b Configure the link layer protocol of the interface to Frame Relay

```
[Router-Serial1]link-protocol fr
[Router-Serial1]fr interface-type dte
```

###### c Configure static address mapping

```
[Router-Serial1]fr map ip 202.38.163.251 dlci 70
```

##### 3 Configure Router C:

###### a Configure interface IP address

```
[Router]interface serial 1
```

```
[Router-Serial1] ip address 202.38.163.253 255.255.255.0
```

- b** Configure the link layer protocol of the interface to Frame Relay

```
[Router-Serial1] link-protocol fr
[Router-Serial1] fr interface-type dte
```

- c** Configure static address mapping

```
[Router-Serial1] fr map ip 202.38.163.251 dlci 80
```

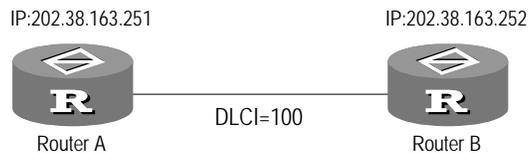
## Interconnect LANs via Private Line

### I. Networking Requirement

Two Routers are directly connected via a serial port. Router A works in the Frame Relay DCE mode, and Router B works in the Frame Relay DTE mode. The router use dynamic address mapping.

### II. Networking Diagram

**Figure 93** Interconnect LANs via private line



### III. Configuration Procedure

- 1** Configure Router A:

- a** Configure interface IP address

```
[Router] interface serial 1
[Router-Serial1] ip address 202.38.163.251 255.255.255.0
```

- b** Configure the link layer protocol of the interface to Frame Relay

```
[Router-Serial1] link-protocol fr
[Router-Serial1] fr interface-type dce
```

- c** Configure local virtual circuit

```
[Router-Serial1] fr dlci 100
```

- 2** Configure Router B:

- a** Configure interface IP address

```
[Router] interface serial 1
[Router-Serial1] ip address 202.38.163.252 255.255.255.0
```

- b** Configure the link layer protocol of the interface to Frame Relay

```
[Router-Serial1] link-protocol fr
[Router-Serial1] fr interface-type dte
```

## Connect Routers through Multilink Frame Relay (FRF.16)

### I. Networking Requirements

RouterA and RouterB are directly connected via the serial ports Serial 0 and Serial1 and through Frame Relay protocol. The two serial ports are bundled together to provide wider bandwidth.

## II. Networking Diagram

Figure 94 MFR bundle networking



## III. Configuration Procedure

### 1 Configure RouterA

#### a Create a MFR interface.

```
[Router]interface mfr 0
[Router-MFR0]ip address 202.38.163.251 255.255.255.0
[Router-MFR0]fr interface-type dte
[Router-MFR0]fr dlci 100
[Router-MFR0]fr map ip 202.38.163.252 dlci 100
```

#### b Bundle Serial 0 and Serial 1 to mfr 0.

```
[Router]interface serial 0
[Router-Serial0]link-protocol fr mfr 0
[Router]interface serial 1
[Router-Serial0]link-protocol fr mfr 0
```

### 2 Configure RouterB

#### a Create a MFR interface.

```
[Router]interface mfr 0
[Router-MFR0]ip address 202.38.163.252 255.255.255.0
[Router-MFR0]fr interface-type dte
[Router-MFR0]fr dlci 100
[Router-MFR0]fr map ip 202.38.163.251 dlci 100
```

#### b Bundle Serial 0 and Serial 1 to mfr 0.

```
[Router]interface serial 0
[Router-Serial0]link-protocol fr mfr 0
[Router]interface serial 1
[Router-Serial0]link-protocol fr mfr 0
```

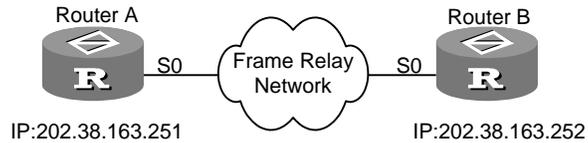
## Frame Relay Compress Typical Configuration Example (FRF.9)

### I. Networking Requirements

Router A and Router B are connected via a Frame Relay network. To improve the efficiency of data transmission, Frame Relay payload compression is used between them.

## II. Networking Diagram

**Figure 95** networking diagram of Frame Relay over IP



## III. Configuration Procedure

### 1 Configure Router A

```
[Router]interface serial 0
[Router-Serial0]ip address 202.38.163.251 255.255.255.0
[Router-Serial0]fr interface-type dte
[Router-Serial0]fr dlci 100
[Router-Serial0]fr map ip 202.38.163.252 dlci 100 compression frf9
```

### 2 Configure Router B

You can configure Router B in the same way as that of Router A, so its configuration will not be mentioned here.

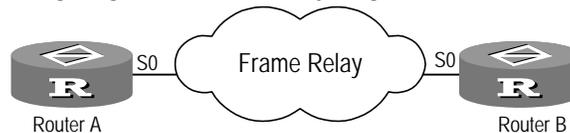
## Typical Frame Relay Fragment Example (FRF.12)

## I. Networking Requirements

RouterA and Router B connect with Frame Relay Network. and enable Frame Relay Fragment between them.

## II. Networking Diagram

**Figure 96** networking diagram of Frame Relay Fragment



## III. Configuration Procedure

### 1 Configure RouterA

```
[Router]interface serial0
[Router-Serial0]link-protocol fr
[Router-Serial0]ip address 10.1.1.2 255.0.0.0
[Router-Serial0] fr dlci 16
[Router-fr-dlci-16]fr-class frts
[Router]fr class frts
[Router-fr-class-frts]cir allow 64000
[Router-fr-class-frts]cbs 64000
[Router-fr-class-frts]cir 64000
[Router-fr-class-frts]fragment 80 data-level
```

### 2 Configure RouterB

```
[Router]interface serial0
[Router-Serial0]link-protocol fr
[Router-Serial0]ip address 10.1.1.1 255.0.0.0
[Router-Serial0]fr dlci 16
[Router-fr-dlci-16]fr-class frts
[Router]fr class frts
```

```
[Router-fr-class-frts]cir allow 64000 64000
[Router-fr-class-frts]cbs 64000
[Router-fr-class-frts]cir 64000
[Router-fr-class-frts]fragment 80 data-level
```

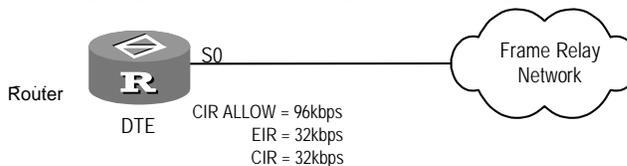
### Configuration Example of Frame Relay Traffic Shaping

#### I. Configuration Requirements

The Router is connected to the Frame Relay network via the interface Serial 0. It is required that the average transmit rate of the router should be 96 kbps, the maximum transmit rate should be 128 kbps, and the minimum transmit rate should be 32 kbps, and at the same time, the router should own the function of adaptive traffic adjustment. In addition, PQ is required to be adopted to ensure that all the IP packets from the segment 10.0.0.0 will pass first.

#### II. Networking Diagram

Figure 97 Networking diagram of Frame Relay traffic shaping



#### III. Configuration Procedure

- 1 Define priority queue Group 1, and request all the IP packets from the segment 10.0.0.0 can pass first.

```
[Router]acl 1
[Router-acl-1]rule normal permit source 10.0.0.0 0.0.0.0
[Router]qos pql 1 protocol ip acl 1 queue top
```

- 2 Create a Frame Relay class and configure the parameters of Frame Relay traffic shaping.

```
[Router]fr class 96k
[Router-fr-class-96k]cir allow 96000
[Router-fr-class-96k]cir 32000
[Router-fr-class-96k]cbs 96000
[Router-fr-class-96k]ebs 32000
[Router-fr-class-96k]traffic-shaping adaptation becn
[Router-fr-class-96k]pq pql 1
```

- 3 Configure the interface Serial 0 and enable the Frame Relay traffic shaping.

```
[Router]interface serial 0
[Router-Serial0]link-protocol fr
[Router-Serial0]ip address 1.1.1.1 255.255.255.0
[Router-Serial0]fr traffic-shaping
```

- 4 Create a Frame Relay PVC and associate the Frame Relay class with it.

```
[Router-Serial0]fr dlci 16
[Router-fr-dlci-16]fr-class 96K
```

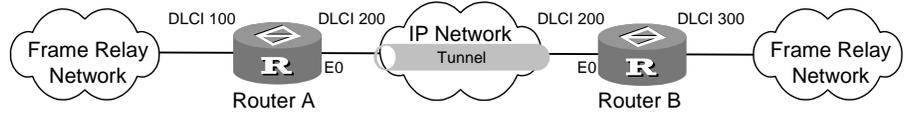
### Typical Frame Relay over IP Configuration Example

#### I. Networking Requirements

Two Frame Relay networks are interconnected via RouterA and RouterB, which are connected via an IP network. Enable Frame Relay over IP on the two routers to interconnect these two Frame Relay networks over the IP network.

## II. Networking Diagram

Figure 98 Networking diagram of Frame Relay over IP



## III. Configuration Procedure

### 1 Configure RouterA

#### a Configure the Frame Relay interface Serial0

```
[Router]interface serial 0
[Router-Serial0]link-protocol fr
[Router-Serial0]fr interface-type dce
[Router-Serial0]fr dlci 100
```

#### b Configure IP interface Ethernet0

```
[Router]interface ethernet 0
[Router-Ethernet0]ip address 10.110.50.1 255.255.255.0
```

#### c Configure tunnel interface

```
[Router]interface tunnel 1
[Router-Tunnel1]source 10.110.50.1
[Router-Tunnel1]destination 10.110.50.2
```

#### d Configure Frame Relay over IP

```
[Router]interface serial 0
[Router-Serial0]fr dlci-switch 100 interface tunnel 1 dlci 200
```

### 2 Configure RouterB

#### a Configure the Frame Relay interface Serial0.

```
[Router]interface serial 0
[Router-Serial0]link-protocol fr
[Router-Serial0]fr interface-type dce
[Router-Serial0]fr dlci 300
```

#### b Configure IP interface Ethernet0

```
[Router]interface ethernet 0
[Router-Ethernet0]ip address 10.110.50.2 255.255.255.0
```

#### c Configure tunnel interface

```
[Router]interface tunnel 1
[Router-Tunnel1]source 10.110.50.2
[Router-Tunnel1]destination 10.110.50.1
```

#### d Configure Frame Relay over IP

```
[Router]interface serial 0
[Router-Serial0]fr dlci-switch 300 interface tunnel 1 dlci 200
```

## Back-to-back Connection through Frame Relay over ISDN

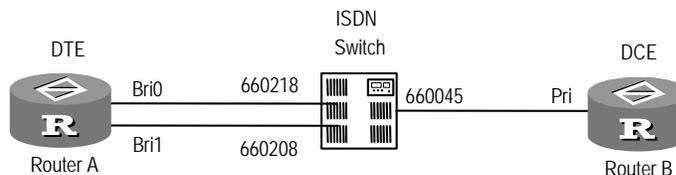
### I. Networking Requirements

RouterA (DTE) and RouterB (DCE) are connected via ISDN. RouterA adopts legacy BDR to make calls while RouterB adopts dialer profiles. To establish a PVC, the call must be originated from RouterA.

On RouterA, two BRI interfaces, Bri0 and Bri1, are available. Bri0 is assigned with the ISDN number 660218, the IP address 110.0.0.1 and the DLCI number 100. Bri1 is assigned with the ISDN number 660208, the IP address 120.0.0.1 and the DLCI number 200. On RouterB, one PRI interface is available for providing services for two dialer interfaces. This PRI interface is assigned with the ISDN number 660045, the IP addresses 110.0.0.2 and 120.0.0.2, and the DLCI numbers 100 and 200.

## II. Networking Diagram

**Figure 99** Networking for the back-to-back connection between DTE and DCE



## III. Configuration Procedure

### 1 Configure RouterA

#### a Configure the BDR parameters on the interface Bri0

```
[Router]dialer-rule 1 ip permit
[Router]interface bri 0
[Router-Bri0]link-protocol fr
[Router-Bri0]ip address 110.0.0.1 255.255.255.0
[Router-Bri0]dialer enable-legacy
[Router-Bri0]dialer-group 1
[Router-Bri0]dialer number 660045
```

#### b Configure the Frame Relay parameters on Bri0.

```
[Router-Bri0]fr map ip 110.0.0.2 dlci 100
[Router-Bri0]fr dlci 100
```

For configuring the BDR and Frame Relay parameters on Bri1, refer to the configuration on Bri0. The user only needs to change the IP address to 120.0.0.1, DLCI number to 200, and address mapping to static address mapping.

### 2 Configure RouterB

#### a Configure BDR and Frame Relay parameters on the PRI interface.

```
[Router]dialer-rule 1 ip permit
[Router]fr switching
[Router]controller e1 0
[Router-E1-0]pri-set
[Router]interface dialer 0
[Router-Dialer0]ip address 110.0.0.2 255.255.255.0
[Router-Dialer0]dialer bundle 10
[Router-Dialer0]dialer-group 1
[Router-Dialer0]dialer number 660218
[Router-Dialer0]dialer call-in 660218
[Router-Dialer0]link-protocol fr
[Router-Dialer0]fr interface-type dce
[Router-Dialer0]fr dlci 100
[Router]interface serial 2:15
[Router-Serial2:15]undo dialer enable-legacy
[Router-Serial2:15]dialer bundle-member 10
```

```
[Router-Serial2:15] dialer bundle-member 20
```

For configuring the BDR and Frame Relay parameters on Dialer1, refer to the configuration on Dialer0. The user only needs to change the IP address to 120.0.0.2, DLCI number to 200, and configure to receive the incoming calls from the number 660208 and assign Dialer1 to Dialer Bundle 20.

## Frame Relay Switching Connection through Frame Relay over ISDN

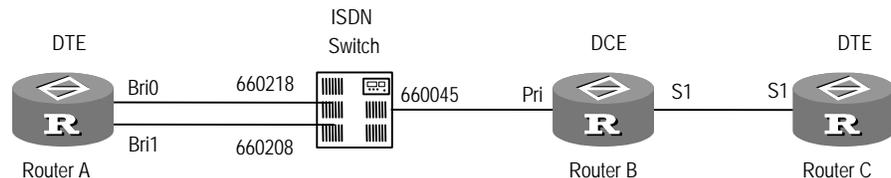
### I. Networking Requirements

RouterB (DCE) is connected to the ISDN interface on RouterA (DTE) via ISDN at one side and RouterC (DTE) via the serial interface at another side. With the Frame Relay switching function of DCE, routers can interwork across ISDN. RouterA adopts legacy BDR to make calls while RouterB adopts dialer profiles. To establish a PVC, the call must be originated from RouterA.

On RouterA, two BRI interfaces, Bri0 and Bri1, are available. Bri0 is assigned with the ISDN number 660218, the IP address 110.0.0.1 and the DLCI number 100. Bri1 is assigned with the ISDN number 660208, the IP address 120.0.0.1 and the DLCI number 200. On RouterB, one PRI interface is available for providing services for two dialer interfaces. This PRI interface is assigned with the ISDN number 660045, and the DLCI numbers 100 and 200 respectively for these two dialer interfaces. At the same time, RouterB is connected to RouterC via a serial interface, which is assigned with the DLCI numbers 300 and 400. The serial interface on RouterC is available with 2 sub-interfaces, which are respectively assigned with the IP addresses 110.0.0.2 and 120.0.0.2, and DLCI numbers 300 and 400.

### II. Networking Diagram

**Figure 100** Networking for the Frame Relay switching connection between DTE devices



### III. Configuration Procedure

#### 1 Configure RouterA

- a** Configure the BDR-related parameters on Bri0.

```
[Router] dialer-rule 1 ip permit
[Router] interface bri 0
[Router-Bri0] link-protocol fr
[Router-Bri0] ip address 110.0.0.1 255.255.255.0
[Router-Bri0] dialer enable-legacy
[Router-Bri0] dialer-group 1
[Router-Bri0] dialer number 660045
```

- b** Configure the Frame Relay-related parameters on Bri0.

```
[Router-Bri0] fr map ip 110.0.0.2 dlci 100
[Router-Bri0] fr dlci 100
```

For configuring the BDR and Frame Relay parameters on Bri1, refer to the configuration on Bri0. The user only needs to change the IP address to 120.0.0.1, DLCI number to 200, and address mapping to static address mapping.

## 2 Configure RouterB

- a Configure the BDR and Frame Relay parameters on the PRI interface.

```
[Router]dialer-rule 1 ip permit
[Router]fr switching
[Router]controller e1 0
[Router-E1-0]pri-set
[Router]interface dialer 0
[Router-Dialer0]ip address 110.0.0.2 255.255.255.0
[Router-Dialer0]dialer bundle 10
[Router-Dialer0]dialer-group 1
[Router-Dialer0]dialer number 660218
[Router-Dialer0]dialer call-in 660218
[Router-Dialer0]link-protocol fr
[Router-Dialer0]fr interface-type dce
[Router-Dialer0]fr dlci 100
[Router]interface serial 2:15
[Router-Serial2:15]undo dialer enable-legacy
[Router-Serial2:15]dialer bundle-member 10
[Router-Serial2:15]dialer bundle-member 20
```

For configuring the BDR and Frame Relay parameters on Dialer1, refer to the configuration on Dialer0. The user only needs to change the IP address to 120.0.0.2, DLCI number to 200, and configure to receive the incoming calls from the number 660208 and assign Dialer1 to Dialer Bundle 20.

- b Configure the Frame Relay switching parameters on Serial1.

```
[Router-Serial1]link-protocol fr
[Router-Serial1]fr interface-type dce
[Router]interface serial 1.1
[Router-Serial1.1]ip address 130.0.0.1 255.255.255.0
[Router-Serial1.1]fr dlci 300
[Router]interface serial 1.2
[Router-Serial1.2]ip address 140.0.0.1 255.255.255.0
[Router-Serial1.2]fr dlci 400
```

- c Configure Frame Relay SVCs.

```
[Router]fr switch myconnect1 interface dialer 0 dlci 100 interface
serial 1 dlci 300
[Router]fr switch myconnect2 interface dialer 1 dlci 200 interface
serial 1 dlci 400
```

## 3 Configure RouterC

- a Configure IP addresses and DLCI numbers for the serial interface and sub-interfaces.

```
[Router]interface serial 1
[Router-Serial1] link-protocol fr
[Router]interface serial 1.1
[Router-Serial1.1]ip address 130.0.0.2 255.255.255.0
[Router-Serial1.1]fr dlci 300
[Router]interface serial 1.2
[Router-Serial1.2]ip address 140.0.0.2 255.255.255.0
[Router-Serial1.2]fr dlci 400
```

---

## Fault Diagnosis and Troubleshooting of Frame Relay

### Fault 1: the physical layer in DOWN status.

Troubleshooting:

- Check whether the physical line is normal.
- Check whether the opposite equipment runs normally.

### Fault 2: the physical layer is already UP, but the link layer protocol is DOWN.

Troubleshooting:

- Check whether both local equipment and opposite equipment have been configured with Frame Relay protocol.
- If two sets of equipment are directly connected, check the local equipment and opposite equipment to see whether one end is configured as Frame Relay DTE interface and the other end as Frame Relay DCE interface.
- Turn on the monitoring switch for the Frame Relay LMI packet to see whether the Status Enquiry packets correspond to the Status packet. If not, it indicates the physical layer data is not receiving or sending correctly. Check the physical layer. Command `debugging fr lmi-info` is used to turn on the monitoring switch for Frame Relay LMI information.

### Fault 3: link layer protocol is UP, but cannot Ping through the peer.

Troubleshooting:

- Check whether the link layer protocols of the equipment at both ends are UP.
- Check whether the equipment at both ends have configured (or created) correct address mapping for the peer.
- Check the route table to see whether there is a route to the peer.

### Fault 4: After the Frame Relay traffic shaping is enabled on the Frame Relay interface, the small-sized packets can be pinged, but the large-sized packets cannot.

Troubleshooting:

- Configuring a too small committed burst size (CBS) will probably cause this phenomenon. In common conditions, CBS cannot be less than 12000 bits. If it is configured too small, the large packets will probably fail to be transmitted.
- Check the configurations of the Frame Relay class associated with the Frame Relay interface or the PVCs, and use the `fr cbs` command to make the CBS larger.

### Fault 4: Frame Relay data cannot be transmitted across ISDN.

Troubleshooting:

- Check whether BDR has been correctly configured. Read the section of troubleshooting in *Dial-up*.
- Use the `debugging dialer event` command to enable BDR event debugging. If "BDR: Bind failed with more than one profile" is displayed, it means that the `dialer number` command has been configured repeatedly at the receiving end. In this case, make sure that this command is uniquely configured at the receiving end.

- Check whether the Frame Relay configurations at both ends are correct. Read the section of troubleshooting in *Link Layer Protocol*.

# 18

## CONFIGURING HDLC

This chapter contains information on the following topics:

- Configure HDLC
- Display and Debug HDLC

### Configure HDLC

HDLC (High Data Link Control) is a bit-oriented link layer protocol. Its most prominent feature is that it can transparently transmit any kind of bit flow without the restriction that the data must be character set. Protocols of standard HDLC protocol group operate upon the synchronous serial lines, e.g., DDN. The address field of HDLC is 8 bits, its control field is 8 bits, and the protocol field is 16 bits, which are used to represent all kinds of control information of HDLC protocol and to mark whether they are data. The 3Com Router supports the HDLC protocol and can connect with HDLC protocol of other popular devices. HDLC configuration includes:

- Configure the link layer protocol of the interface to HDLC
- 1 Configure the Link Layer Protocol of the Interface to HDLC

In synchronous interface view, perform the following task.

**Table 318** Configure the link layer protocol of the interface to HDLC

| Operation                                                  | Command                   |
|------------------------------------------------------------|---------------------------|
| Configure the link layer protocol of the interface to HDLC | <b>link-protocol hdlc</b> |

By default, the link layer protocol of the interface is PPP.



*Only when the interface operates in the synchronous mode, can the link layer protocol be configured to HDLC.*



*When the interface link layer protocol is SLIP, its physical attribute cannot be changed to synchronous mode. At this time, you should first change the link layer protocol of the interface to PPP before you change the interface attribute to synchronous mode.*

### Display and Debug HDLC

**Table 319** Display and debug HDLC

| Operation                                 | Command                                               |
|-------------------------------------------|-------------------------------------------------------|
| Enable all the debugging of HDLC protocol | <b>debugging hdlc all [ interface type number ]</b>   |
| Enable HDLC event debugging               | <b>debugging hdlc event [ interface type number ]</b> |

|                              |                                                                     |
|------------------------------|---------------------------------------------------------------------|
| Enable HDLC packet debugging | <code>debugging hdlc packet [ interface <i>type number</i> ]</code> |
|------------------------------|---------------------------------------------------------------------|

# 19

## CONFIGURING BRIDGE

This chapter contains information on the following topics:

- Bridge Overview
- Configure Bridge's Routing Function
- Display and Debug Bridge
- Typical Bridge Configuration

---

### Bridge Overview

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 in the networks widely dispersed, using 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 networks 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 the communication in mixed Token Ring and Ethernet environments.

The transparent bridging supported by the 3Com Router series has the following features:

- Conforms to the IEEE 802.1d standards and supports the STP and bridging functions specified in IEEE 802.1d.
- Supports bridging on the links of PPP and HDLC.
- Supports bridging on X.25 links.

- Supports bridging on the Frame Relay links.
- Supports bridging on the sub-interfaces of VLAN.
- Supports bridging on BDR and dialing standby.
- Supports binding of multiple ports and load sharing.
- Support both routing and bridging function for specified protocol.
- Support filtering Ethernet frames according to the MAC address or Ethernet frame format.
- Provides command configuration and management functions.
- Provides functions of logging, alarming and debugging.

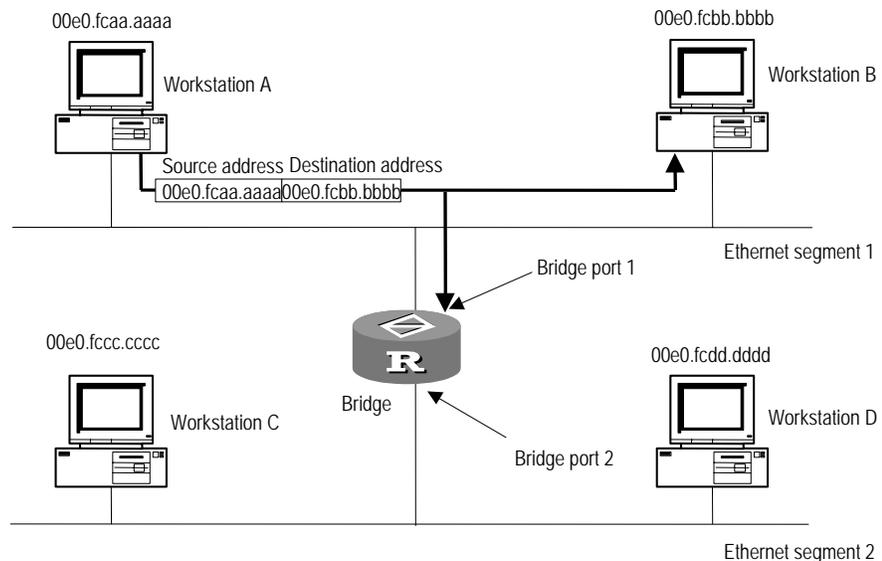
### Main Functions of Bridging

#### Obtain address table

Bridging implements forwarding in accordance with the bridging table comprised of MAC addresses and interfaces. A bridge should obtain the correlation between MAC addresses and ports. When the bridge connects with a LAN segment, it will detect all the Ethernet frames on this segment. Once the Ethernet frame sent from a node 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.

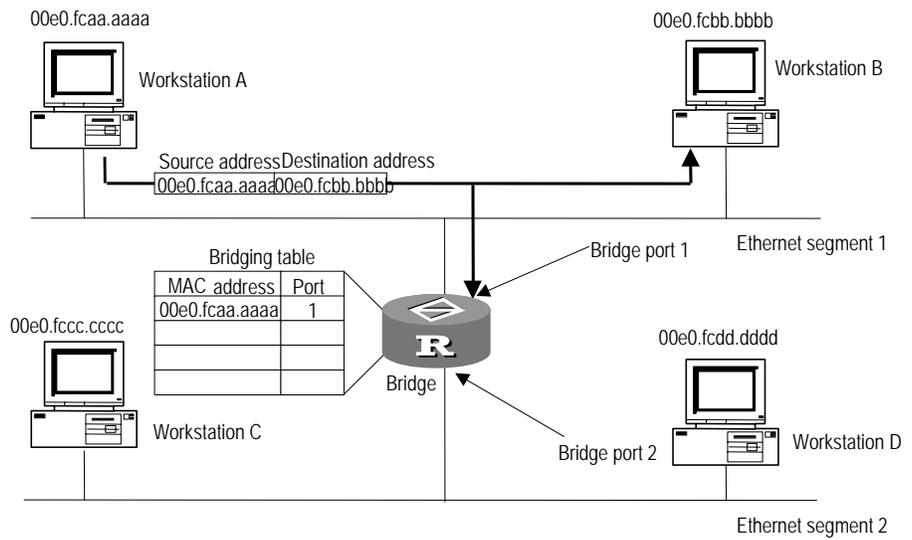
As shown in the following figure, four workstations A, B, C and D are distributed in two LANs: Ethernet segment 1 connected with Bridge port 1 and Ethernet segment 2 connected with Bridge port 2. At a certain moment, when Workstation A transmits an Ethernet frame to Workstation B, both the bridge and Workstation B will receive this frame.

**Figure 101** Workstation A transmits information to workstation B on the Ethernet segment 1



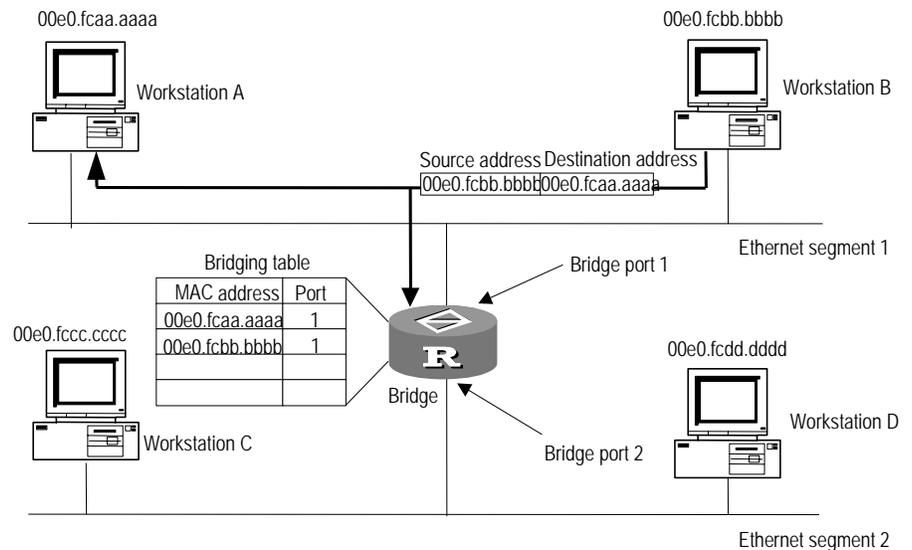
Upon receiving the Ethernet frame, the bridge learns that Workstation A is connected with Bridge port 1 since the frame received is from Port 1. As a result, the correlation between the MAC address of Workstation A and Bridge port 1 will be added to the bridging table, as shown in the following figure:

**Figure 102** Bridge learns that Workstation A is connected with Port 1



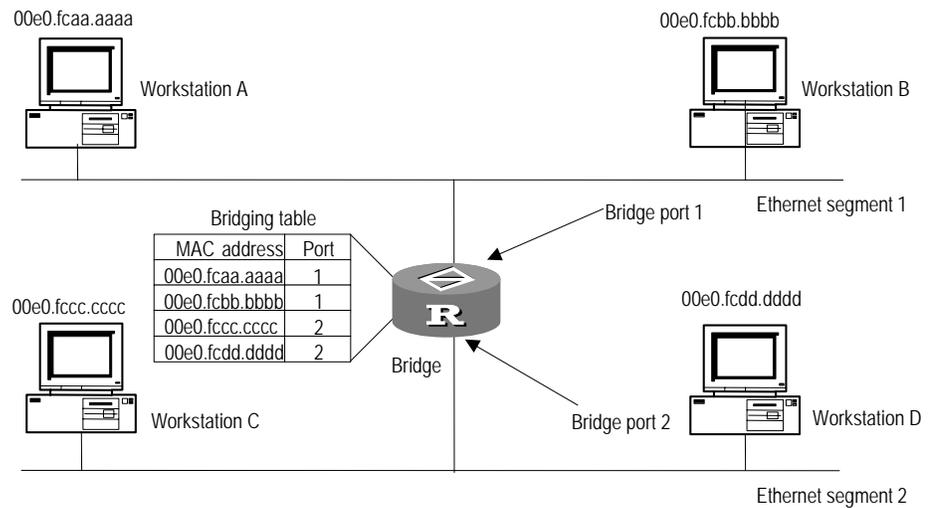
Once Workstation B responds to Workstation A, the bridge can detect the responding Ethernet frame from Workstation B and learn that Workstation B is also connected to Bridge port 1 because the frame is detected on port 1 too. As a result, the correlation between the MAC address of Workstation B and Bridge port 1 is added to the bridging table too, as shown in the following figure:

**Figure 103** 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:

**Figure 104** Final bridging address table

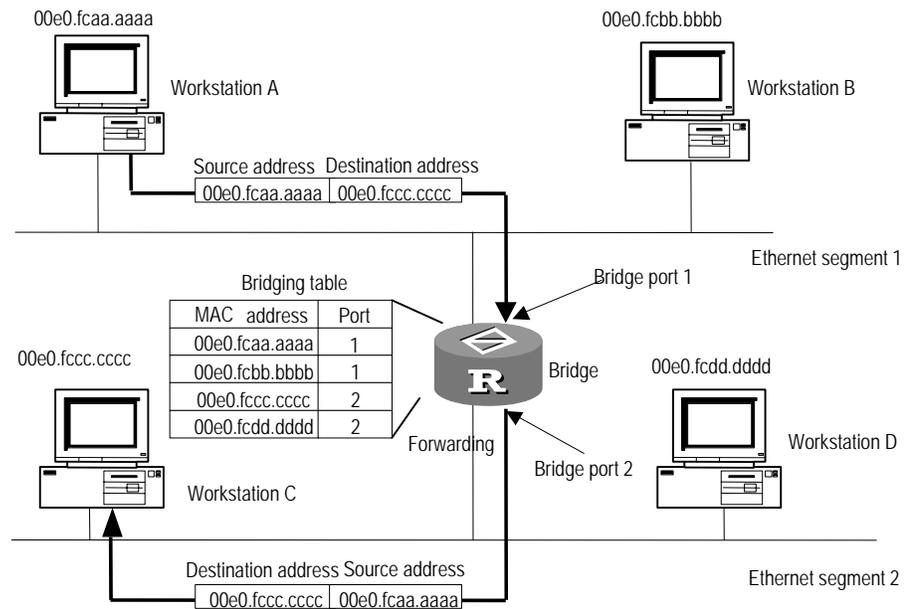


**Forward and Filter**

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.

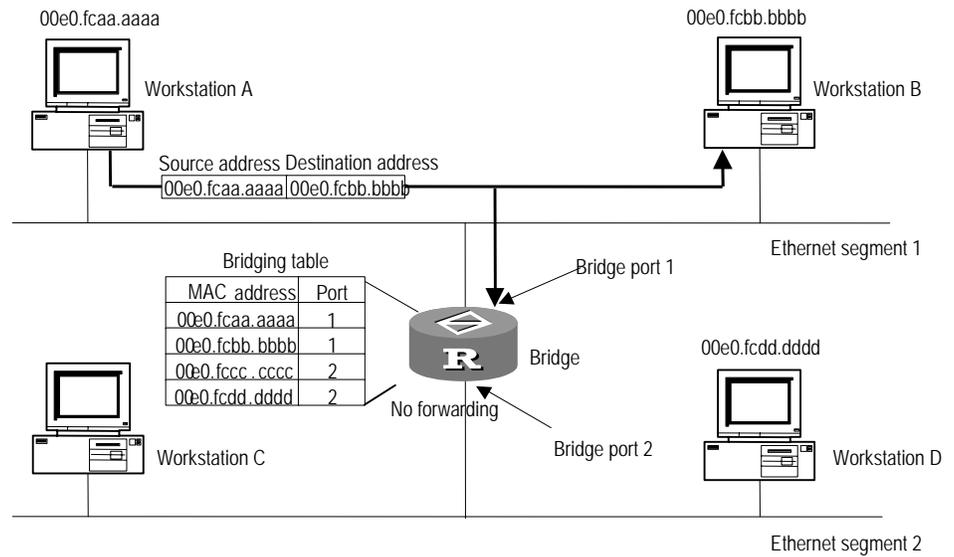
**Figure 105** Forward



Note that the bridge will forward the broadcast or multicast frames received on one port to the other ports.

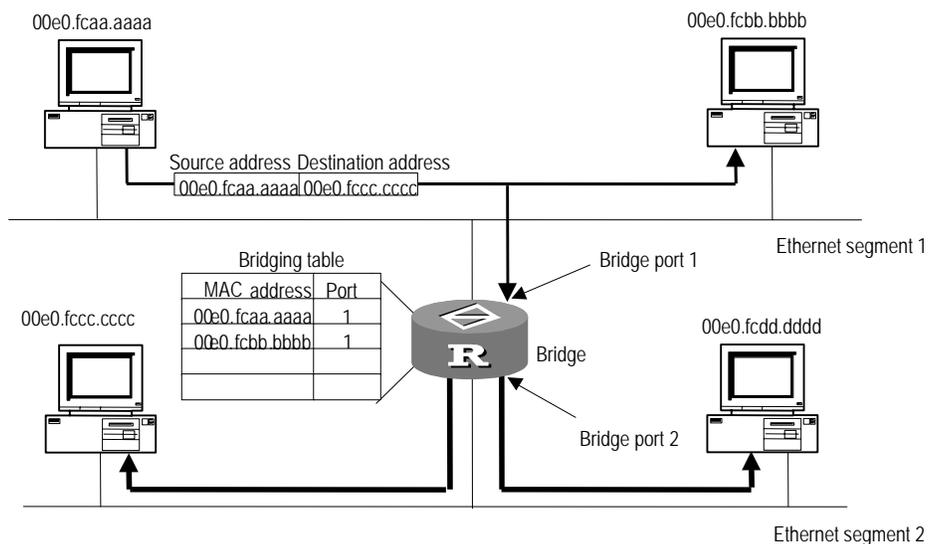
Given that Workstation A sends an Ethernet frame to Workstation B, the bridge will filter this frame rather than forwarding it, since Workstation B and Workstation A are located on the same physical network segment.

**Figure 106** 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:

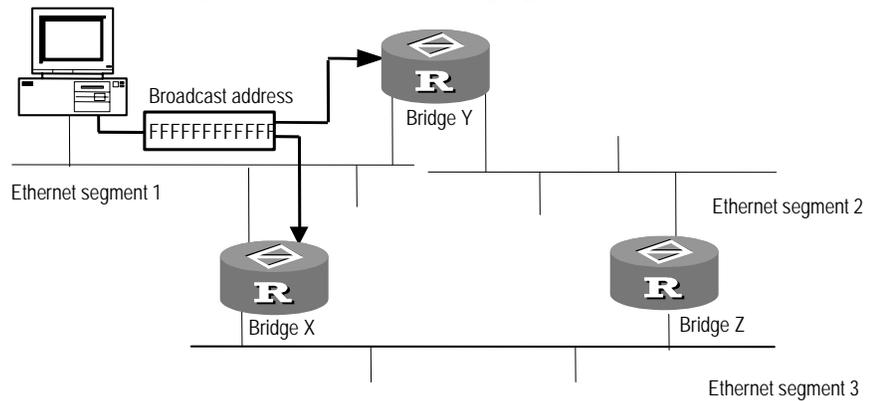
**Figure 107** No matched MAC address is found in the bridging table



### Eliminating loop

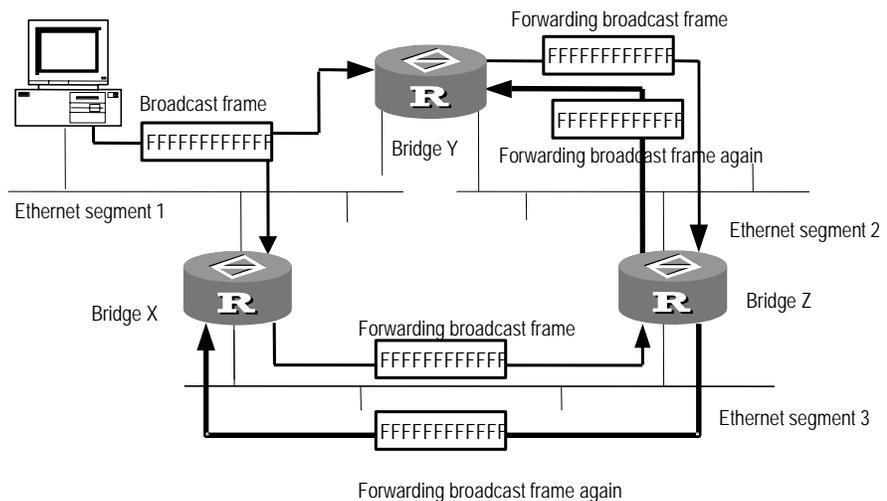
As shown in the following figure, both bridges X and Y are connected with Ethernet segment 1. Once detecting a broadcasting frame, both bridges will send it to all ports except the source port on which the frame is detected. That is, both bridges X and Y will forward this broadcast frame.

**Figure 108** 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. Like this, the frame is repeatedly forwarded over the network, which is called bridging loop.

**Figure 109** 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.

**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.

STP transmits a type 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:

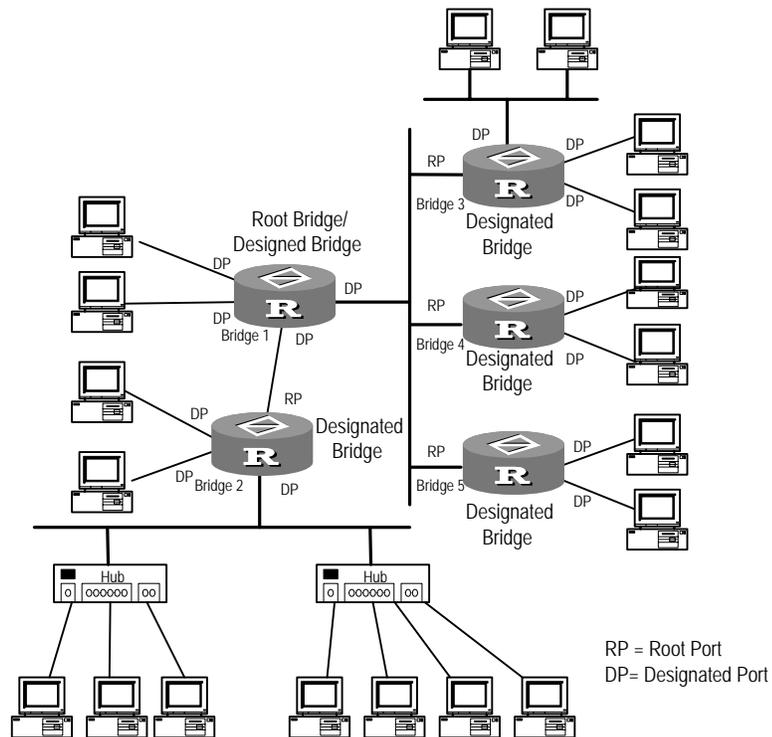
- Root Identifier: Consists of the Bridge Priority and the MAC address of the root bridge.
- Root Path Cost: Path cost from the individual leaf nodes to the root bridge.
- Bridge Identifier: Consists of the Bridge priority and the MAC address of the current bridge.
- Port Identifier: Consists of the Port Priority and the Port Number.
- Message Age of BPDU
- Max Age of BPDU
- Hello Time of BPDU
- Forward Delay of port state transition

### **Spanning Tree Topology**

- 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 110** Spanning tree topology

### BPDU Forwarding Mechanism

Upon the initiation of the network, all the bridges assume themselves as the root bridge. The designated interface of the bridge regularly sends its BPDU once a Hello Time. If it is the root port 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 forward 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.

### 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 routed protocols and the bridging protocols 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.

For the 3Com Router series, if the bridging function is not enabled, all the IP packets will be routed through IP. If it is enabled, the packets in the bridge-set will be bridge forwarded.

**Link-set** When there are multiple parallel links between two bridge devices, and the corresponding link ports are all added to the bridge set, the spanning tree protocol can be used to avoid bridge loop, and can ensure that only one link is available to transmit data. Other corresponding link ports are all in congestion state. This can guarantee normal bridging between two bridge devices on the cost of wasting link bandwidth. The link set can guarantee the bridging function and save the link bandwidth. The solution is, adding multiple parallel links to a link set. Each corresponding link port can still independently take part in the spanning tree calculation, which guarantees the bridging function. During data forwarding, each link in the link set can share loads, thus utilizing all link bandwidths.

---

## Configure Bridge's Routing Function

Bridge configuration includes:

- Enable/Disable bridging functions
- Configure bridge-set
- Add ports to a bridge-set
- Configure bridging address table
- Configure parameters related to STP
- Create ACLs of bridge
- Apply ACLs on Ports
- Configure routing function
- Configure link-set
- Configure bridging over Frame Relay
- Configure bridging over BDR
- Configure bridging over LAPB
- Configure bridging over PPP
- Configure bridging over HDLC
- Configure bridging over VLAN

### 1 Enable/Disable Bridging Functions

Perform the following configuration in system view.

**Table 320** Enable/Disable bridging functions

| Operation                  | Command                   |
|----------------------------|---------------------------|
| Enable bridging functions  | <b>bridge enable</b>      |
| Disable bridging functions | <b>undo bridge enable</b> |

By default, disable bridging functions.

## 2 Configure Bridge-Set

Each bridge set is independent, and packets can not be transmitted between the ports belonging to different bridge sets. That is, the packets received via one bridge set port can only be sent via the ports of the same bridge set. One physical interface can only be added to one bridge set.

The bridges support several STP versions and these versions are not compatible. Sometimes, different STP versions may result in bridge looping.

The 3Com Router series only support the STP defined in IEEE.

Perform the following configuration in system view.

**Table 321** Specify the STP version supported by the bridge-set

| Operation                                           | Command                                       |
|-----------------------------------------------------|-----------------------------------------------|
| Specify the STP version supported by the bridge-set | <b>bridge <i>bridge-set</i> stp ieee</b>      |
| Delete the STP version supported by the bridge-set  | <b>undo bridge <i>bridge-set</i> stp ieee</b> |

By default, the bridge-set supports the STP version ieee.

## 3 Add Ports to a Bridge-Set

One interface on the router cannot be added to more than one bridge set.

Perform the following configuration in interface view.

**Table 322** Add ports to a bridge-set

| Operation                      | Command                                  |
|--------------------------------|------------------------------------------|
| Add ports to a bridge-set      | <b>bridge-set <i>bridge-set</i></b>      |
| Remove ports from a bridge-set | <b>undo bridge-set <i>bridge-set</i></b> |

By default, the port is not added to any bridge-set.

## 4 Configure Bridging Address Table

Bridging address table records the correlation between the destination MAC addresses and the ports. According to it, a bridge implements forwarding.

### a Configure static address table 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 interface view.

**Table 323** Configure static address table entries

| Operation                              | Command                                                                                                                     |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Configure static address table entries | <b>bridge <i>bridge-set</i> mac-address <i>mac-address</i> { permit   deny } [ <i>interface-type interface-number</i> ]</b> |
| Delete static address table entries    | <b>undo bridge <i>bridge-set</i> mac-address <i>mac-address</i></b>                                                         |

By default, dynamic address table is adopted to forward frames.

### b Enable/Disable forwarding by using dynamic address table

Perform the following configuration in system view.

**Table 324** Enable/Disable forwarding by using dynamic address table

| Operation                                          | Command                                |
|----------------------------------------------------|----------------------------------------|
| Enable forwarding using the dynamic address table  | <b>bridge bridge-set learning</b>      |
| Disable forwarding using the dynamic address table | <b>undo bridge bridge-set learning</b> |

By default, the dynamic address table is used to forward frames.

**c** Configure the aging time of dynamic address table

The aging time of dynamic address table refers to the time that an entry can remain in the address table before it is deleted. The aging time is controlled by the aging timer. Upon the expiration of the timer, the entry will be deleted from the bridge address table.

Perform the following configuration in system view.

**Table 325** Configure the aging time of dynamic address table

| Operation                                                            | Command                          |
|----------------------------------------------------------------------|----------------------------------|
| Configure the aging time of dynamic address table                    | <b>bridge aging-time seconds</b> |
| Restore the aging time of dynamic address table to the default value | <b>undo bridge aging-time</b>    |

By default, the aging time of dynamic address table is 300 seconds. The aging time is in the range of 10 to 1000000 seconds.

**5** Configure Parameters Related to STP

**a** Disable/Enable STP on ports

Only when STP is enabled on the ports can all the configured parameters related to STP take effect.

Perform the following configuration in interface view.

**Table 326** Disable/Enable STP on ports

| Operation            | Command                                       |
|----------------------|-----------------------------------------------|
| Disable STP on ports | <b>bridge-set bridge-set stp disable</b>      |
| Enable STP on ports  | <b>undo bridge-set bridge-set stp disable</b> |

By default, STP is enabled on all ports.

**b** Configure the bridge priority

Bridge Identifier is comprised of the bridge priority and the MAC address of the bridge. The bridge with smallest Bridge Identifier will be elected as the root bridge of the whole spanning tree. If the priorities of all the bridges in the network are the same, the bridge with the smallest MAC address will be elected as the root bridge. In the case that the STP is enabled, changing the priority of a bridge will cause the recompilation of the spanning tree.

Perform the following configuration in system view.

**Table 327** Configure the bridge priority

| Operation                                        | Command                          |
|--------------------------------------------------|----------------------------------|
| Configure the bridge priority                    | <b>bridge stp priority value</b> |
| Restore the default value of the bridge priority | <b>undo bridge stp priority</b>  |

By default, the bridge priority is 32768. It is valued in the range of 0 to 65535.

**c** Configure the path cost of bridge port

The path cost of the port is related to its link speed. The higher the link speed is, the lower the path cost should be configured. If the port is configured with the default path cost, STP will automatically detect the current link speed of the port and accordingly compute the path cost on the port.

Perform the following configuration in interface view.

**Table 328** Configure the path cost of bridge port

| Operation                                                     | Command                                             |
|---------------------------------------------------------------|-----------------------------------------------------|
| Configure the path cost of bridge port                        | <b>bridge set bridge-set stp port pathcost cost</b> |
| Restore the path cost on the bridge port to the default value | <b>undo bridge-set bridge-set stp port pathcost</b> |

By default, the path cost of Ethernet port is 100, and the path cost of serial interface is 647. It is valued in the range 1 to 65535.

**d** Configure the bridge port priority

In the case that path costs of the ports are the same, the port with lower ID is more likely to become the designated port. The port ID is comprised of Port Priority and Port Number. The smaller the port priority, the smaller the bridge port ID will be. Changing the bridge port priority will cause recomputation of the spanning tree. If all the bridge ports adopt the same priority, the smaller the port number is, the smaller the port ID will be.

Perform the following configuration in interface view.

**Table 329** Configure the bridge port priority

| Operation                                             | Command                                              |
|-------------------------------------------------------|------------------------------------------------------|
| Configure the bridge port priority                    | <b>bridge-set bridge-set stp port priority value</b> |
| Restore the default value of the bridge port priority | <b>undo bridge-set bridge-set stp priority</b>       |

By default, the bridge port priority is 128. It is in the range of 0 to 255.

**e** Configure the interval for sending BPDUs

The Hello Time timer is used to control the interval to send BPDUs. Whenever a port enables the STP, it enables the Hello Time timer. Appropriate Hello Time ensures that the bridge can detect the link fault in the network promptly without consuming too many network resources.

Perform the following configuration in system view.

**Table 330** Configure the interval for sending BPDUs

| Operation                                         | Command                                      |
|---------------------------------------------------|----------------------------------------------|
| Configure Hello Time timer                        | <b>bridge stp timer hello <i>seconds</i></b> |
| Restore the default value of the Hello Time timer | <b>undo bridge stp timer hello</b>           |

By default, the value of Hello Time timer is 2 seconds. It is in the range of 1 to 10 seconds.

When configuring the Hello Time timer, it should be noted that:

- In the spanning tree, all the bridges use the time value of Hello Time timer of the root bridge, and their own configurations take no effect.
- Too long a Hello Time will cause the bridge to recompute the spanning tree because it considers the packet dropping of the link as link fault, whereas too short a Hello Time will cause it to send BPDUs frequently and thus exacerbate the bridge CPU load. It is recommended that users use the default value.

**f** Configure the forward delay for the port status transition

Link faults may cause the network to recompute the spanning tree topology. However, the recomputed new BPDU cannot be propagated throughout the network right away. If the newly elected root port and the designated port begin to forward data immediately, a temporary loop may be incurred. 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 forward 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. The forward delay timer is thus used to control the interval for the system waiting to enter the Forwarding state.

Perform the following configuration in system view.

**Table 331** Configure the forward delay for the port status transition

| Operation                                            | Command                                              |
|------------------------------------------------------|------------------------------------------------------|
| Configure the forward delay timer                    | <b>bridge stp timer forward-delay <i>seconds</i></b> |
| Restore the default value of the forward delay timer | <b>undo bridge stp timer forward-delay</b>           |

By default, the value of the forward delay timer is 15 seconds. It is in the range of 4 to 200 seconds.

When configuring the forward delay timer, note that:

- No matter what its individual configuration might be, all the bridges in the spanning tree should use the time value of the forward delay timer of the root bridge.
- If the forward delay is configured too short, temporary redundant paths may be introduced. If the forward delay is configured too long, however, the restoring of network connection may take a long time because the STP cannot converge to a stable state for a long period. It is recommended that users use the default value.

**g** Configure the Max Age of BPDU

The Max Age is the parameter used to judge whether the BPDUs are “timeout”. Users can configure it according to the actual network conditions. When a port enables the STP, the Max Age timer begins to time. If no BPDU is received in the specified period, it will assume that the link has failed and the STP will recompute the minimum spanning tree.

Perform the following configuration in system view.

**Table 332** Configure the Max age of BPDU

| Operation                                      | Command                                  |
|------------------------------------------------|------------------------------------------|
| Configure a time value for the Max Age timer   | <b>bridge stp max-age <i>seconds</i></b> |
| Restore the default value of the Max Age timer | <b>undo bridge stp max-age</b>           |

By default, the value of the Max Age timer is 20 seconds. It is in the range of 6 to 40 seconds.

When configuring the Max Age timer, it should be noted that:

- Spanning tree should use the value of the Max Age timer of the root bridge.
- Too short a Max Age will result in frequent recompilations of spanning tree and mistaking the network delay for link fault. On the other hand, too long a Max Age may make the bridge unable to detect link fault promptly and reduce the network self-sensing ability. It is recommended that users use the default value.

## 6 Create ACLs of Bridge

### a Create an ACL based on MAC Ethernet addresses

Perform the following configuration in system view.

**Table 333** Create an ACL based on MAC Ethernet addresses

| Operation                                     | Command                                                                            |
|-----------------------------------------------|------------------------------------------------------------------------------------|
| Create an ACL based on MAC Ethernet addresses | <b>acl <i>acl-number</i> { permit   deny }<br/><i>mac-address mac-wildcard</i></b> |
| Delete an ACL based on MAC Ethernet addresses | <b>undo acl <i>acl--number</i></b>                                                 |

By default, no ACL based on MAC Ethernet addresses is created.

When creating an ACL based on MAC Ethernet addresses, value the *access-list-number* in the range of 700 to 799. *mac-address* is an MAC Ethernet address in the format of xx-xx-xx-xx-xx-xx, which is used to match the source address of a packet. *Mac-wildcard* is the wildcard of the MAC Ethernet address.

### b Create ACLs based on varied Ethernet encapsulation formats

Perform the following configuration in system view.

**Table 334** Create ACLs based on varied Ethernet encapsulation formats

| Operation                                                  | Command                                                                           |
|------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Create ACLs based on varied Ethernet encapsulation formats | <b>acl <i>acl-number</i> { permit   deny }<br/><i>type-code type-wildcard</i></b> |
| Delete ACLs based on varied Ethernet encapsulation formats | <b>undo acl <i>acl- number</i></b>                                                |

By default, no ACL based on varied Ethernet encapsulation formats is created.

When creating an ACL based on Ethernet type code (Ethernet-II, SNAP or LSAP), you can specify *acl-number* in the range of 200 to 299. *type-code* is a 16-bit hexadecimal number written with a leading "0x", corresponding to the type-code field in the Ethernet-II or SNAP frames. *type-wildcard* is a 16-bit hexadecimal number written with a leading "0x" and used to specify the shielded bits.

When creating an ACL, note that:

- The rules will be compared in the order in which they are configured.
- If no rule is matched, Ethernet frames should still be permitted to pass.
- The number of created rules cannot exceed 200.

## 7 Apply ACLs on Ports

Perform the following configuration in interface view.

### a Apply ACLs based on MAC addresses on ports

**Table 335** Apply ACLs based on MAC addresses on ports

| Operation                                                                              | Command                                                     |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Apply ACLs based on MAC addresses in the input direction of ports                      | <b>bridge-set bridge-set source-mac acl acl-number</b>      |
| Remove the application of ACLs based on MAC addresses in the input direction of ports  | <b>undo bridge-set bridge-set source-mac acl acl-number</b> |
| Apply ACLs based on MAC addresses in the output direction of ports                     | <b>bridge-set bridge-set dest-mac acl acl-number</b>        |
| Remove the application of ACLs based on MAC addresses in the output direction of ports | <b>undo bridge-set bridge-set dest-mac acl acl-number</b>   |

By default, no ACL is applied on the port.

### b Apply an ACL encapsulated in the form of IEEE 802.2 on the port

**Table 336** Apply an ACL encapsulated in the form of IEEE 802.2 on the port

| Operation                                                                                               | Command                                                        |
|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Apply an ACL encapsulated in the form of IEEE 802.2 to the input side of the port                       | <b>bridge-set bridge-set inbound-lsap acl acl-number</b>       |
| Remove the application of the ACL encapsulated in the form of IEEE 802.2 to the input side of the port  | <b>undo bridge-set bridge-set inbound-lsap acl acl-number</b>  |
| Apply the ACL encapsulated in the form of IEEE 802.2 to the output side of the port                     | <b>bridge-set bridge-set outbound-lsap acl acl-number</b>      |
| Remove the application of the ACL encapsulated in the form of IEEE 802.2 to the output side of the port | <b>undo bridge-set bridge-set outbound-lsap acl acl-number</b> |

By default, no ACL is applied on the port.

### c Apply an ACL encapsulated in the form of Ethernet-II/Ethernet-SNAP on the port

**Table 337** Apply an ACL encapsulated in the form of IEEE 802.2 on the port

| Operation                                                                                           | Command                                                  |
|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Apply an ACL encapsulated in the form of Ethernet-II or Ethernet-SNAP to the input side of the port | <b>bridge-set bridge-set inbound-type acl acl-number</b> |

|                                                                                                                           |                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Remove the application of the ACL encapsulated in the form of Ethernet-II or Ethernet-SNAP to the input side of the port  | <b>undo bridge-set <i>bridge-set</i><br/>inbound-type acl <i>acl-number</i></b>  |
| Apply an ACL encapsulated in the form of Ethernet-II or Ethernet-SNAP to the output side of the port                      | <b>bridge-set <i>bridge-set</i><br/>outbound-type acl <i>acl-number</i></b>      |
| Remove the application of the ACL encapsulated in the form of Ethernet-II or Ethernet-SNAP to the output side of the port | <b>undo bridge-set <i>bridge-set</i><br/>outbound-type acl <i>acl-number</i></b> |

By default, no ACL is applied on the port.

When applying an ACL on the port, note that:

- Add the port to a bridge-set first, then apply the ACL on that port.
- If ACLs of the same type are applied to the same port, the latest ACL applied will replace the previous ones.

## 8 Configure Routing Function

### a Enable routing function

For the data of a specified protocol, they will be bridged if the communication is carried out between the bridge ports. If the communication with a network outside the bridge-set is needed, the data can be routed. If the bridge's routing is not enabled yet, the data of all the protocols can only be bridged. Once the bridge's routing is enabled, you can specify both bridging and routing for the packets of a particular protocol. You can flexibly switch over between them through configuring the command.

Perform the following configuration in system view.

**Table 338** Enable/Disable bridge's routing

| Operation                         | Command                           |
|-----------------------------------|-----------------------------------|
| Enable bridge's routing function  | <b>bridge routing-enable</b>      |
| Disable bridge's routing function | <b>undo bridge routing-enable</b> |

By default, bridge's routing function is disabled.

### b Create bridge-template interface

Bridge-template interface exists on the router, it does not support bridging, but it represents the whole bridge-set corresponding to the routed interface on the router. Bridge-template interface uses the same number of the bridge-set represented by it. All kinds of network layer attributes can be configured on the bridge-template interface. Each bridge-set can have only one bridge-template interface.

Perform the following configuration in system view.

**Table 339** Configure a bridge-template interface

| Operation                                                                                      | Command                                                |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Create a bridge-template interface to connect the specified bridge-set to the routing network. | <b>interface bridge-template<br/><i>bridge-set</i></b> |

### c Configure bridge set to route or bridge the network layer protocol

Perform the following configuration in system view.

**Table 340** Configure bridge set to route or bridge the network layer protocol

| Operation                                                   | Command                                             |
|-------------------------------------------------------------|-----------------------------------------------------|
| Enable the bridge set to route the network layer protocol   | <b>bridge bridge-set routing { ip   ipx }</b>       |
| Disable the bridge set to route the network layer protocol  | <b>undo bridge bridge-set routing { ip   ipx }</b>  |
| Enable the bridge set to bridge the network layer protocol  | <b>bridge bridge-set bridging { ip   ipx }</b>      |
| Disable the bridge set to bridge the network layer protocol | <b>undo bridge bridge-set bridging { ip   ipx }</b> |

By default, the bridging is enabled, the routing is disabled.

You can execute the **display bridge bridge-set bridge-template** command to view the configuration of routing and bridging on each interface.

## 9 Configure Link-Set

### a Define a link-set

The link set can bundle multiple parallel links between two bridges, thus sharing loads among multiple links and enhancing link bandwidth utilization ratio when there is no bridge loop.

Perform the following configuration in interface view.

**Table 341** Define a link-set

| Operation                    | Command                                        |
|------------------------------|------------------------------------------------|
| Assign a port to a link-set. | <b>bridge-set bridge-set link-set link-set</b> |

### b Share load by source MAC address

Perform the following configuration in system view.

**Table 342** Share load by source MAC address

| Operation                                                            | Command                                                |
|----------------------------------------------------------------------|--------------------------------------------------------|
| Bind the ports to a link-set to share the load by source MAC address | <b>bridgebridge-set link-set link-set origin</b>       |
| Disable the load sharing by source address                           | <b>undo bridge bridge-set link-set link-set origin</b> |

By default, the load is shared by packets instead of source MAC address. However, the load will be shared by source MAC address, if it is configured.

Executing the **display bridge bridge-set link-set** command can display the configuration of the link-set on each bridge as well as whether it is sharing the load.

## 10 Configure Bridging over Frame Relay

When establishing a bridge, mapping between the bridge address and DLCI address should be specified.

Perform the following configuration in interface view.

**Table 343** Map the bridge address to DLCI

| Operation                                               | Command                             |
|---------------------------------------------------------|-------------------------------------|
| Configure a Frame Relay mapping forwarded to the bridge | <b>fr map bridge dlc1 broadcast</b> |

**11** Configure Bridging over BDR

Perform the following configuration in system view.

**a** Define a dialer list**Table 344** Define a dialer list

| Operation             | Command                                                      |
|-----------------------|--------------------------------------------------------------|
| Define a dialer list. | <b>dialer-rule dialer-group<br/>bridge { permit   deny }</b> |

**b** Configure the bridge interface

Perform the following configuration in interface view.

**Table 345** Configuration on the interface

| Operation                             | Command                                         |
|---------------------------------------|-------------------------------------------------|
| Add the interface to the dialer-group | <b>dialer-group dialer-group</b>                |
| Map the bridge address to BDR         | <b>dialer route bridge broadcast<br/>string</b> |

**12** Configure Bridging over LAPB

Perform the following configuration in interface view.

**Table 346** Configure the link layer protocol of the interface to LAPB

| Operation                                                  | Command                                                        |
|------------------------------------------------------------|----------------------------------------------------------------|
| Configure the link layer protocol of the interface to LAPB | <b>link-protocol lapb [ dte   dce ]<br/>[ multi-protocol ]</b> |

**13** Configure Bridging over PPP

Perform the following configuration in interface view.

**Table 347** Configure the link layer protocol of the interface to PPP

| Operation                                                 | Command                  |
|-----------------------------------------------------------|--------------------------|
| Configure the link layer protocol of the interface to PPP | <b>link-protocol ppp</b> |

**14** Configure Bridging over HDLC

Perform the following configuration in interface view.

**Table 348** Configure the link layer protocol of the interface to HDLC

| Operation                                                  | Command                   |
|------------------------------------------------------------|---------------------------|
| Configure the link layer protocol of the interface to HDLC | <b>link-protocol hdlc</b> |

**15** Configure Bridging over VLAN

Perform the following configuration in interface view.

**Table 349** Configure bridge on VLAN

| Operation                                             | Command                             |
|-------------------------------------------------------|-------------------------------------|
| Configure the bridge-set on the sub-interface of VLAN | <b>bridge-set <i>bridge-set</i></b> |

## Display and Debug Bridge

Perform the **reset**, **display** and **debugging** commands in all views.

**Table 350** Display and debug bridge

| Operation                                                                               | Command                                                        |
|-----------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Clear the statistics of access list rules                                               | <b>reset acl counters [ <i>acl-number</i> ]</b>                |
| Clear the entries of all the bridge-sets or specified groups in the forwarding database | <b>reset bridge [ <i>bridge-set</i> ]</b>                      |
| Clear the statistics of Spanning Tree                                                   | <b>reset stp statistics</b>                                    |
| Clear the traffic statistics of bridge-set on the interface                             | <b>reset bridge traffic</b>                                    |
| Display the states of all the bridge-sets                                               | <b>display bridge-set [ <i>bridge-set</i> ]</b>                |
| Display the information in the bridge forwarding database                               | <b>display bridge information</b>                              |
| Display the state and statistics of STP                                                 | <b>display bridge spanning-tree</b>                            |
| Display the static data of bridge-set traffic on a port                                 | <b>display bridge traffic</b>                                  |
| Display the routing and bridging configuration on each interface                        | <b>display bridge <i>bridge-set</i> <i>bridge-template</i></b> |
| Display link set configuration of the specified bridge set.                             | <b>display bridge<i>bridge-set</i> link-set</b>                |
| Enable bridge-set debugging                                                             | <b>debugging bridge</b>                                        |
| Enable the spanning-tree protocol debugging                                             | <b>debugging stp { error   event   packet }</b>                |

## Typical Bridge Configuration

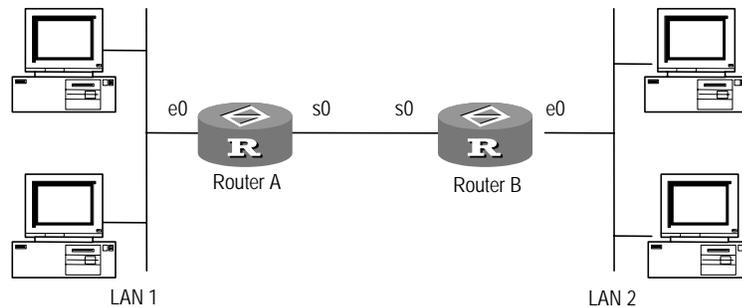
### Transparent Bridging Multiple LANs

#### I. Networking Requirements

Suppose that 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. It is required to build the transparent bridge between these two LANs.

## II. Networking Diagram

**Figure 111** Networking of building transparent bridges between multiple Ethernet segments



## III. Configuration Procedure

### 1 Configure Router A

```
[Router]bridge enable
[Router]bridge 1 stp ieee
[Router]bridge 1 learning
[Router]bridge aging-time 300
[Router]interface ethernet 0
[Router-Ethernet0]bridge-set 1
[Router-Ethernet0]bridge-set stp disable
[Router-Ethernet0]interface serial 0
[Router-Serial0]link-protocol ppp
[Router-Serial0]bridge-set 1
[Router-Serial0]bridge-set 1 stp disable
```

### 2 Configure Router B

```
[Router]bridge enable
[Router]bridge 1 stp ieee
[Router]bridge 1 learning
[Router]bridge aging-time 300
[Router]interface ethernet 0
[Router-Ethernet0]bridge-set 1
[Router-Ethernet0]bridge-set 1 stp disable
[Router-Ethernet0]interface Serial 0
[Router-Serial0]link-protocol ppp
[Router-Serial0]bridge-set 1
[Router-Serial0]bridge-set 1 stp disable
```

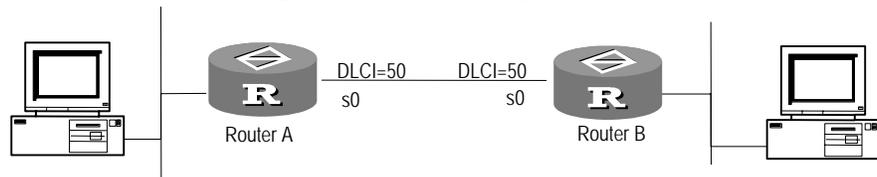
## Transparent Bridging over Frame Relay

### I. Networking Requirements

Two routers are directly connected via serial interfaces. Implement transparent bridging over the Frame Relay.

### II. Networking Diagram

Figure 112 Transparent bridge over the Frame Relay



### III. Configuration Procedure

#### 1 Configure Router A

```
[Router]fr switching
[Router]bridge enable
[Router]bridge 1 stp ieee
[Router]interface serial 0
[Router-Serial0]link-protocol fr
[Router-Serial0]fr interface-type dce
[Router-Serial0]fr dlci 50
[Router-Serial0]bridge-set 1
[Router-Serial0]fr map bridge 50 broadcast
[Router-Serial0]interface ethernet 0
[Router-Ethernet0]bridge-set 1
[Router-Ethernet0]bridge-set 1 stp disable
```

#### 2 Configure Router B

```
[Router]fr switching
[Router]bridge enable
[Router]bridge 1 stp ieee
[Router]interface serial 0
[Router-Serial0]link-protocol fr
[Router-Serial0]fr interface-type dte
[Router-Serial0]fr dlci 50
[Router-Serial0]bridge-set 1
[Router-Serial0]fr map bridge 60 broadcast
[Router-Serial0]interface ethernet 0
[Router-Ethernet0]bridge-set 1
[Router-Ethernet0]bridge-set stp disable
```

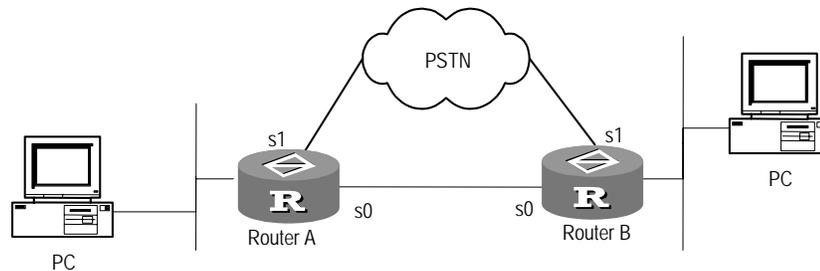
## Transparent Bridging for Synchronous Dial-in Standby

### I. Networking Requirements

Configure transparent bridging for synchronous dial-in standby on two routers. Thereby, transparent bridging can be implemented by enabling synchronous dial-in in case that the serial interfaces through which the routers are directly connected are failed.

### II. Networking Diagram

**Figure 113** Networking of transparent bridging for synchronous dial-in standby



### III. Configuration Procedure

#### 1 Configure Router A

```
[Router]bridge enable
[Router]bridge stp timer forward-delay 4
[Router]bridge 1 stp ieee
[Router]dialer-rule 1 bridge permit
[Router]interface serial 1
[Router-Serial1]link-protocol ppp
[Router-Serial1]dialer enable-legacy
[Router-Serial1]dialer-group 1
[Router-Serial1]dialer route bridge broadcast 660074
[Router-Serial1]bridge-set 1
[Router-Serial1]interface serial 0
[Router-Serial0]standby interface Serial 1
[Router-Serial0]bridge-set 1
[Router-Serial0]interface ethernet0
[Router-Ethernet0]bridge-set 1
[Router-Ethernet0]bridge-set 1 stp disable
```

#### 2 Configure Router B

```
[Router]bridge enable
[Router]bridge stp timer forward-delay 4
[Router]bridge 1 stp ieee
[Router]dialer-rule 1 bridge permit
[Router]interface serial 1
[Router-Serial1]link-protocol ppp
[Router-Serial1]dialer enable-legacy
[Router-Serial1]dialer-group 1
[Router-Serial1]dialer number
[Router-Serial1]bridge-set 1
[Router-Serial1]interface serial 0
[Router-Serial0]bridge-set 1
[Router-Serial0]interface ethernet0
[Router-Ethernet0]bridge-set 1
[Router-Ethernet0]bridge-set 1 stp disable
```

## Transparent Bridging for Asynchronous Dial-in Standby

### I. Networking Requirements

Configure transparent bridging for asynchronous dial-in standby on two routers. Thereby, transparent bridging can be implemented by enabling asynchronous dial-in in case that the serial interfaces through which the routers are directly connected are failed.

### II. Networking Diagram

Please refer to Figure 113.

### III. Configuration Procedure

#### 1 Configure Router A

```
[Router]bridge enable
[Router]bridge stp timer forward-delay 4
[Router]bridge 1 stp ieee
[Router]dialer-rule 1 bridge permit
[Router]interface serial 1
[Router-Serial1]link-protocol ppp
[Router-Serial1]physical-mode async
[Router-Serial1]modem
[Router-Serial1]async mode protocol
[Router-Serial1]dialer enable-legacy
[Router-Serial1]dialer-group 1
[Router-Serial1]dialer route bridge broadcast 660074
[Router-Serial1]bridge-set 1
[Router-Serial1]interface serial 0
[Router-Serial0]standby interface Serial 1
[Router-Serial0]bridge-set 1
[Router-Serial0]interface ethernet0
[Router-Ethernet0]bridge-set 1
[Router-Ethernet0]bridge-set 1 stp disable
```

#### 2 Configure Router B

```
[Router]bridge enable
[Router]bridge stp timer forward-delay 4
[Router]bridge 1 stp ieee
[Router]dialer-rule 1 bridge permit
[Router]interface serial 1
[Router-Serial1]link-protocol ppp
[Router-Serial1]physical-mode async
[Router-Serial1]modem
[Router-Serial1]async mode protocol
[Router-Serial1]dialer enable-legacy
[Router-Serial1]dialer-group 1
[Router-Serial1]dialer number
[Router-Serial1]bridge-set 1
[Router-Serial1]interface serial 0
[Router-Serial0]bridge-set 1
[Router-Serial0]interface ethernet0
[Router-Ethernet0]bridge-set 1
[Router-Ethernet0]bridge-set 1 stp disable
```

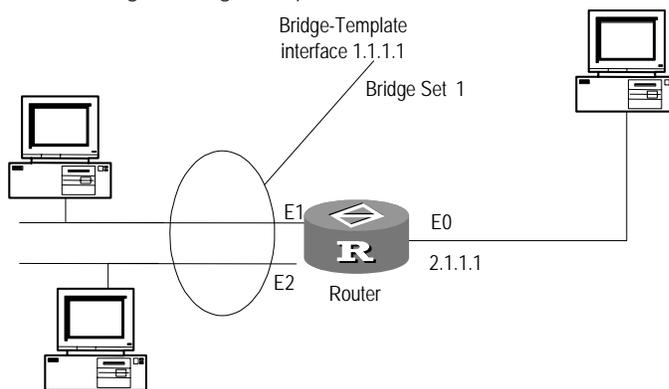
## Bridge-Template interface

### I. Networking Requirements

Configure a router so that routing can be carried out on each interface in the bridge-set.

### II. Networking Diagram

**Figure 114** Networking of bridge-template interface



### III. Configuration Procedure

```
[Router]bridge enable
[Router]bridge routing-enable
[Router]bridge 1 stp ieee
[Router]interface ethernet1
[Router-Ethernet1]bridge-set 1
[Router-Ethernet1]interface ethernet2
[Router-Ethernet2]bridge-set 1
[Router-Ethernet2]interface bridge-template 1
[Router-Bridge-Template1]ip address 1.1.1.1 255.255.0.0
[Router-Bridge-Template1]interface ethernet0
[Router-Ethernet0]ip address 2.1.1.1 255.255.0.0
```

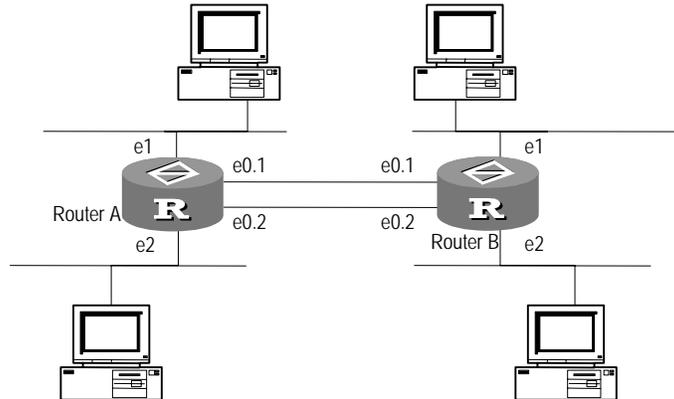
## Bridging on Sub-Interfaces

### I. Networking Requirements

Two routers are connected via a network cable. Enabling bridging on the Ethernet sub-interfaces so that the two bridges established via the routers can be interconnected.

### II. Networking Diagram

Figure 115 Networking for bridging on sub-interfaces



### III. Configuration Procedure

#### 1 Configure Router A

```
[Router]bridge enable
[Router]bridge 1 stp ieee
[Router]bridge 2 stp ieee
[Router]interface ethernet 1
[Router-Ethernet1]bridge-set 1
[Router-Ethernet1]interface ethernet 2
[Router-Ethernet2]bridge-set 2
[Router-Ethernet2]interface ethernet 0.1
[Router-Ethernet0.1]vlan-type dot1q vid 1
[Router-Ethernet0.1]bridge-set 1
[Router-Ethernet0.1]interface ethernet 0.2
[Router-Ethernet0.2]vlan-type dot1q vid 2
[Router-Ethernet0.2]bridge-set 2
```

#### 2 Configure Router B

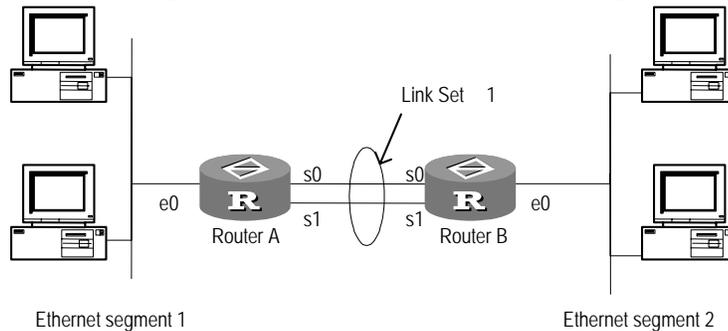
```
[Router]bridge enable
[Router]bridge 1 stp ieee
[Router]bridge 2 stp ieee
[Router]interface ethernet 1
[Router-Ethernet1]bridge-set 1
[Router-Ethernet1]interface ethernet 2
[Router-Ethernet2]bridge-set 2
[Router-Ethernet2]interface ethernet 0.1
[Router-Ethernet0.1]vlan-type dot1q vid 1
[Router-Ethernet0.1]bridge-set 1
[Router-Ethernet0.1]interface ethernet 0.2
[Router-Ethernet0.2]vlan-type dot1q vid 2
[Router-Ethernet0.2]bridge-set 2
```

## Link-Set Configuration I. Networking Requirements

Bind multiple parallel links between bridges into a link-set so that the links can share the load when bridging the traffic.

## II. Networking Diagram

**Figure 116** Networking of use link-set to implement port binding



## III. Configuration Procedure

### 1 Configure Router A

```
[Router]bridge enable
[Router]bridge 1 stp ieee
[Router]interface ethernet 0
[Router-Ethernet0]bridge-set 1
[Router-Ethernet0]interface serial0
[Router-Serial0]bridge-set 1
[Router-Serial0]bridge-set 1 link-set 1
[Router-Serial0]interface serial1
[Router-Serial1] bridge-set 1
[Router-Serial1] bridge-set 1 link-set 1
```

### 2 Configure Router B

```
[Router]bridge enable
[Router]bridge 1 stp ieee
[Router]interface ethernet 0
[Router-Ethernet0]bridge-set 1
[Router-Ethernet0]interface serial0
[Router-Serial0]bridge-set 1
[Router-Serial0]bridge-set 1 link-set 1
[Router-Serial0]interface serial1
[Router-Serial1]bridge-set 1
[Router-Serial1]bridge-set 1 link-set 1
```

# V

## NETWORK PROTOCOL

- Chapter 20    Configuring IP Address
- Chapter 21    Configuring IP Application
- Chapter 22    Configuring IP Performance
- Chapter 23    Configuring IP Count
- Chapter 24    Configuring IPX
- Chapter 25    Configuring DLSw



# 20

## CONFIGURING IP ADDRESS

This chapter contains information on the following topics:

- IP Address Overview
- Troubleshooting IP Address Configuration
- Map between WAN Interface IP Address and Link Layer Protocol Address

---

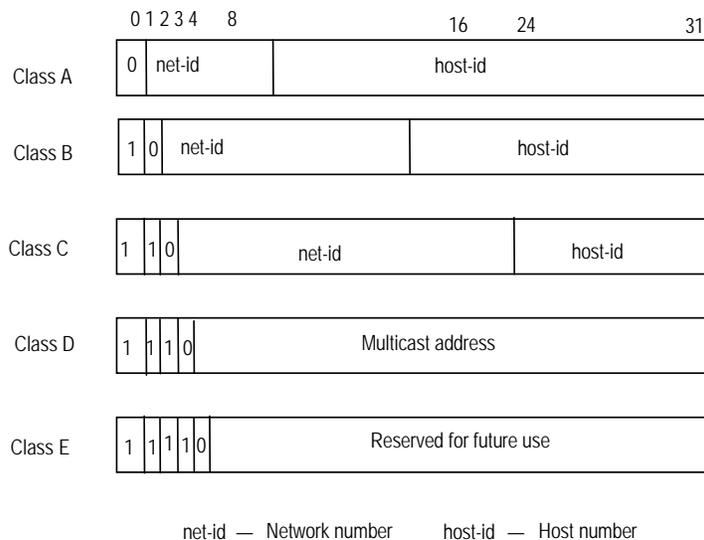
### IP Address Overview

IP address is a unique 32-bit address assigned to a host connected to Internet. Usually it is composed of two parts: network ID and host ID. Its structure enables convenient addressing on Internet. IP address is assigned by Network Information Center (NIC) of American National Defense Data Network.

For easy IP address management and convenient networking, IP address of Internet is divided into five classes. An IP address consists of the following 3 fields:

- Type field (also called type bit), used to distinguish the type of IP address.
- Network ID field (net-id).
- Host ID field (host-id).

**Figure 117** 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, IP addresses are mostly of 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 a user can use are listed in the following table.

**Table 351** IP address classes and ranges

| Network class | IP network range          | Description                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A             | 1.0.0.0 ~ 126.0.0.0       | <p>Network IDs with all the digits being 0 or all the digits being 1 are reserved for special use.</p> <p>Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing.</p> <p>Host ID with all the digits being 1 indicates the broadcast address, i.e. broadcast to all hosts on the network.</p> <p>Network ID 127 is used for self-loop interface.</p> |
| B             | 128.1.0.0 ~ 191.254.0.0   | <p>Network IDs with all the digits being 0 or all the digits being 1 are reserved for special use.</p> <p>Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing.</p> <p>Host ID with all the digits being 1 indicates the broadcast address, i.e. broadcast to all hosts on the network.</p>                                                        |
| C             | 192.0.1.0 ~ 223.255.254.0 | <p>Network IDs with all the digits being 0 or all the digits being 1 are reserved for special use.</p> <p>Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing.</p> <p>Host ID with all the digits being 1 indicates the broadcast address, i.e. broadcast to all hosts on the network.</p>                                                        |
| D             | None                      | <p>Addresses of class D are multicast addresses.</p> <p>Host ID with all the digits being 1 indicates the broadcast address, i.e. broadcast to all hosts on the network.</p>                                                                                                                                                                                                                                            |
| E             | None                      | 255.255.255.255 is used as the whole network's broadcast address, and the other addresses are reserved for future use.                                                                                                                                                                                                                                                                                                  |

Important features of IP address:

Some IP addresses are not in a hierarchical structure, which is different from the structure of telephone number. In other words, these IP addresses cannot reflect any geographical information about the host position.

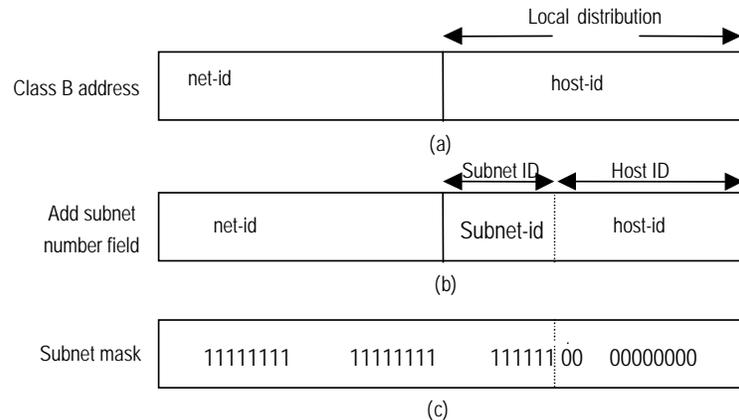
- When a host is connected to two networks at the same time (such as the host used as a router), it must have two corresponding IP addresses with different net-ids. Such host is called multihomed host.
- According to Internet concept, several LANs connected via transceiver or bridges are still in the same network, so these LANs have the same net-id.
- In terms of IP address, all networks which are assigned with net-ids are equal (no matter whether it is a small LAN or a big WAN).

Since 1985, only the net-id of IP address is assigned, while the following 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 and uniquely. If there are many enterprise hosts widely scattered, the host IDs may be further divided into internal sub-nets to facilitate management. Please 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 message 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 "1s" and a string of continuous "0s". The 1s corresponds to the network ID field and the sub-net number field, while the 0s correspond to the host ID field.

**Figure 118** 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 host IDs. But after a 6-bit-long sub-net field is classified, there may be at most 62 sub-nets (excluding sub-nets whose numbers are purely 1s or purely 0s). Each sub-net has 10bit host ID, i.e. each sub-net has 1022 host IDs at most. Totally, there are  $62 \times 1022 = 63364$  host IDs which is less than the sum before sub-net classification.

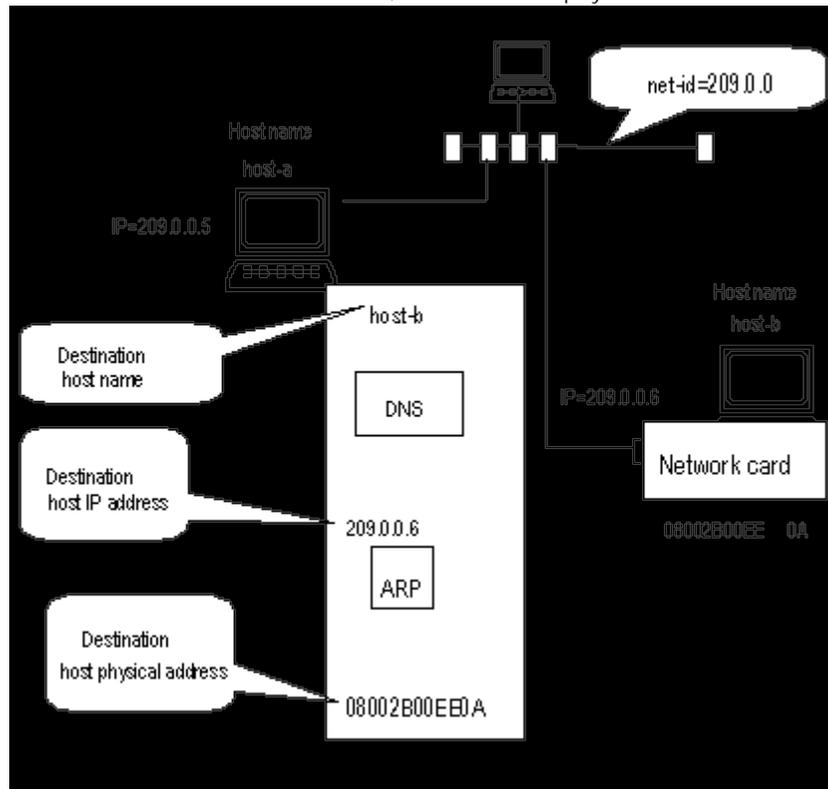
If there is no sub-net division in an enterprise, then its sub-net mask is the default value and the length of "1" indicates the net-id length. Therefore, for IP addresses of classes A, B and C, the default values of corresponding sub-net mask are 255.0.0.0, 255.255.0.0 and 255.255.255.0 respectively.

A router connecting multiple sub-nets 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 messages 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 relation between host name, IP address and physical address.

**Figure 119** Relation between host name, IP address and physical address



**Configure IP Address** **Configure IP Address for an Interface**

Use a mask to label the network ID contained in an IP address. Example: the IP address of an Ethernet interface of a router is 129.9.30.42, and the mask is 255.255.0.0. To obtain the network ID a logical and operation is performed between the IP address and the mask. Thus the above router's Ethernet interface will be 129.0.0.0

Each interface of a router can have several IP addresses, among which one is the master IP address and the others are slave IP addresses. Any two IP addresses of a router cannot be in the same network segment.

Perform the following configuration in interface view.

**1** Configure master IP address of an interface

For each interface of a router, multiple IP addresses can be configured, among which one is the master IP address and the rest are slave IP addresses. Two IP addresses of one router can never be configured within the same network segment.

**Table 352** Configure master IP address of an interface

| Operation                                   | Command                                                        |
|---------------------------------------------|----------------------------------------------------------------|
| Configure master IP address of an interface | <code>ip address ip-address { mask   mask-length }</code>      |
| Delete IP address of an interface           | <code>undo ip address ip-address { mask   mask-length }</code> |

By default, the interface has no master IP address.

When configuring the master IP address for an interface, note:

- An interface can only have one master IP address.
- When deleting the IP address of the interface, if no IP address and mask is specified, all the IP addresses (including all slave IP addresses) will be deleted from the interface.
- One router can be configured with up to 200 IP addresses at most.
- Only the Loopback interface can be configured with 32-bit mask and other interfaces can only be configured with 30-bit mask at most.

## 2 Configure slave IP address of an interface

Besides the master IP address, at most 4 slave IP addresses can be configured on an interface. The purpose of assigning slave IP addresses is to have the same interface located in different sub-nets, so as to create network routes with the same interface as the output port, and set up connection via the same interface to multiple sub-nets.

**Table 353** Configure slave IP address of an interface

| Operation                                  | Command                                                                |
|--------------------------------------------|------------------------------------------------------------------------|
| Configure slave IP address of an interface | <code>ip address ip-address { mask   mask-length } sub</code>          |
| Delete slave IP address of an interface    | <code>undo ip address ip-address { mask   mask-length } [ sub ]</code> |

By default, the interface has no slave IP address.

When configuring slave IP addresses for an interface, please note:

- Slave IP addresses cannot be on the same network segment with each other and they cannot be on the same network segment with the master IP address. Otherwise, the system will prompt:
- IP address configured now conflicts with others.
- If the interface is not configured with the master IP address, the first configured IP address will become the master IP address automatically.
- When there are slave IP addresses on the interface, the master IP address cannot be deleted. Otherwise, the system will prompt:

Must delete secondary before deleting primary.

## 3 Set negotiable attribute of an IP address for an interface

When an interface is encapsulated with PPP, but not configured with IP address while the peer has been configured with IP address, the user can configure negotiable attribute of IP address on the interface on the local router. (To configure `ip address ppp-negotiate` command on the local router, and to configure `remote address` on the peer router) In this case, the local router can accept the IP address originated from PPP negotiation and allocated by the peer router. Such configuration is mainly used to obtain IP address allocated by ISP when accessing the Internet via ISP.

**Table 354** Set negotiable attribute of IP address for an interface

| Operation                                                   | Command                                                     |
|-------------------------------------------------------------|-------------------------------------------------------------|
| Set PPP negotiable attribute of IP address for an interface | <b>ip address ppp-negotiate</b>                             |
| Cancel negotiable attribute of IP address for an interface  | <b>undo ip address ppp-negotiate</b>                        |
| Assign IP address for the peer interface                    | <b>remote address { ip-address / pool [ pool-number ] }</b> |
| Cancel IP address for the peer interface                    | <b>undo remote address</b>                                  |

By default, the interface has no negotiating IP address.

Note the following:

- 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 is DOWN, the IP address originated from negotiation will be deleted.
- If the interface has an 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.

### Configure IP Address Unnumbered for an Interface

#### Introduction to IP address unnumbered

Borrowing IP address will save IP address resources. If an interface has no IP address, it can neither generate any route nor forward any message. "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 master 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**.

Note the following:

- The borrower can not be an Ethernet interface
- The address of the lending interface cannot be lent by the borrowed interface.
- The lending interface can lend its address to multiple interfaces.

Because the borrowing interface has no IP address of its own, and can not route, two routes need to be configured manually to connect routers.

IP address unnumbered configuration includes:

- Activate/deactivate IP address unnumbered.
- 1 Activate/deactivate IP address unnumbered
- Perform the following task in the interface view,

**Table 355** Configure IP address unnumbered

| Operation                        | Command                                                                          |
|----------------------------------|----------------------------------------------------------------------------------|
| Activate IP address unnumbered   | <b>ip address unnumbered</b><br><b>interface-type</b><br><b>interface-number</b> |
| Deactivate IP address unnumbered | <b>undo ip address unnumbered</b>                                                |

By default, the interface has no IP address.

## 2 Display IP address unnumbered

**Table 356** Display IP address unnumbered

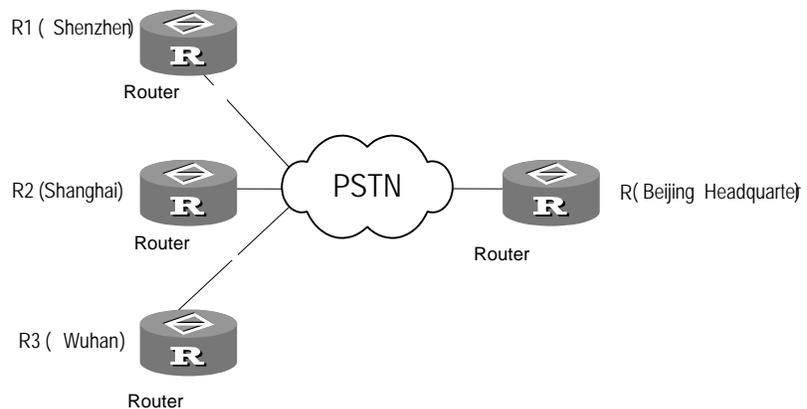
| Operation                                             | Command                                 |
|-------------------------------------------------------|-----------------------------------------|
| Display information of interface borrowing IP address | <b>display interfaces [type number]</b> |
| Display the current configuration information.        | <b>display current-configuration</b>    |

## Configuration Example

### I. Configuration Requirements

Suppose the headquarters of a company is in Beijing, with subsidiary offices in Shenzhen and Shanghai and one office in Wuhan. R is the headquarters router, which connects the subsidiaries and office routers R1, R2 and R3 via PSTN. The four routers R, R1, R2 and R3 all have its serial port for dialing and one Ethernet interface to connect with local network.

### II. Networking Diagram

**Figure 120** Networking diagram of IP address unnumbered configuration

### III. Configuration Procedure

#### 1 Configure headquarters router R

```
[Router-Ethernet0] ip address 172.16.10.1 255.255.255.0
```

##### a Borrow IP address of Ethernet interface 0:

```
[Router-Serial0] ip address unnumbered Ethernet0
[Router-Serial0] link-protocol ppp
```

##### b Configure routing to Ethernet segment of Shenzhen router R1:

```
[Router] ip route-static 172.16.20.0 255.255.255.0 172.16.20.1
```

##### c Configure the interface routing to Shenzhen router R1 serial port

```
[Router] ip route-static 172.16.20.1 255.255.255.255 serial0
```

**2** Configure router R1 of Shenzhen subsidiary:

```
[Router-Ethernet0] ip address 172.16.20.1 255.255.255.0
```

**a** Borrow IP address of Ethernet

```
[Router-Serial0] ip address unnumbered Ethernet0
[Router-Serial0] link-protocol ppp
```

**b** Configure routing to Ethernet segment on Beijing router R, this routing is default routing

```
[Router] ip route-static 0.0.0.0 0.0.0.0 172.16.10.1
```

**c** Configure interface routing to serial port of Beijing router R

```
[Router] ip route-static 172.16.10.1 255.255.255.255 serial0
```

Two static routing must be configured on Beijing headquarters router R to ensure access to Ethernet host of Shenzhen router R1.

The first static routing is to Ethernet segment of R1: the next hop is the IP address of serial port of R1 (or an unnumbered IP address)

```
ip route-static 172.16.20.1 255.255.255.0 172.16.20.1
```

The second static route is an interface route to the serial port of R1, and the next hop is the serial port of R

```
ip route-static 172.16.20.1 255.255.255.255 serial 0
```

After the two routes are added, router R will be able to forward the IP message to R1 correctly

Similarly, two static routes must be configured on R1 to access the Ethernet segment of router R. The first static routing is to Ethernet segment of R: the next hop is the IP address of serial port of R (or an unnumbered IP address)

```
ip route-static 0.0.0.0 0.0.0.0 172.16.10.1
```

The second static route is an interface route to the serial port of R, and the next hop is the serial port of R1.

```
ip route-static 172.16.10.1 255.255.255.255 serial0
```

The configuration of R2 and R3 is similar to that of R1.

---

## 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 master 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 port 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, turn on the arp debugging switch on the router, and check if the router can correctly send and receive arp messages. If it can send but

cannot receive the arp message, then possibly the error is on the Ethernet physical layer.

**Fault 2: When the interface is encapsulated with PPP or Frame Relay, the link layer protocol status does not change to UP.**

Troubleshooting: check whether the IP address of this interface is in the same network segment as the opposite side.

**Fault 3: After the interface borrows an IP address, the link layer protocol status will turn to UP, but it can not ping through itself, and other ports can not ping through this borrowed IP address either.**

Troubleshooting: Check whether the lender port is UP. Only when the port protocol of the lender is UP, will the address be added to the route table and pinged through by other ports.

---

### 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 a dialup interface (such as an asynchronous serial port or ISDN interface), mapping between IP address and dialing serial port is maintained by the command **dialer route ip**.
- 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 tables, which are essential for the normal working of the router. For details, refer to related chapters in *Link Layer Protocol*.



# 21

## CONFIGURING IP APPLICATION

This chapter contains information on the following topics:

- Configure Address Resolution Protocol (ARP)
- Configure Domain Name Resolution (DNS)
- VLAN Configuration
- DHCP Server Configuration
- Configure DHCP Relay
- Configure Network Address Translation (NAT)

---

### Configure Address Resolution Protocol (ARP)

ARP is mainly used for resolution from IP address to Ethernet MAC address. Normally, dynamic ARP is used to resolve the mapping relation from the IP address to the Ethernet MAC address. The resolution is completed automatically. At present, the number of dynamic ARP mapping table items supported by the 3Com Router series is up to 2000.

To configure ARP, carry out the following steps:

#### 1 Manually add/delete static ARP mapping table item

In some special cases, for example, the LAN gateway is assigned with a fixed IP address and bound to a specific network adapter, so that packets to this IP address can only go out via this gateway. While filtering illegal IP addresses if they are bound to a non-existing MAC address, it is necessary for user to configure mapping items in the static ARP table manually.

In the system view, configure the following commands.

**Table 357** Define a static ARP mapping

| Operation                                     | Command                                      |
|-----------------------------------------------|----------------------------------------------|
| Manually add static ARP mapping table item    | <b>arp static ip-address<br/>mac-address</b> |
| Manually delete static ARP mapping table item | <b>undo arp static ip-address</b>            |

#### 2 Manually add/delete dynamic ARP mapping table item

In the system view, configure the following commands.

**Table 358** Define a static ARP mapping

| Operation                                      | Command                                       |
|------------------------------------------------|-----------------------------------------------|
| Manually add dynamic ARP mapping table item    | <b>arp dynamic ip-address<br/>mac-address</b> |
| Manually delete dynamic ARP mapping table item | <b>undo arp dynamic ip-address</b>            |

By default, the system executes static ARP mapping.

Static ARP mapping items are valid as long as the router works normally, but dynamic ARP mapping items are valid for only 20 minutes.

**Display and Debug ARP**

**Table 359** Display and Debug ARP

| Operation                          | Command                                             |
|------------------------------------|-----------------------------------------------------|
| Display ARP mapping table          | <code>display arp [ verbose [ ip-address ] ]</code> |
| Clear dynamic ARP information      | <code>reset arp-cache</code>                        |
| Turn on ARP commission information | <code>debugging arp</code>                          |

**Configure Domain Name Resolution (DNS)**

The TCP/IP Extranet not only provides an IP address to locate a device, but also designs a specific character-string host naming mechanism. This system uses a layered naming mode, designating a meaningful name for a device on the Internet. There is a domain name resolution server on the network to associate the domain name to the corresponding IP address. As a result, the user can use the easy-to-remember, meaningful domain name instead of the complex IP address.

Domain name resolution includes dynamic resolution and static resolution, which can supplement each other. In the resolution of a domain name, first use static resolution. If it fails, then use dynamic resolution. Some common domain names can be put into static domain name resolution table, which greatly increases the efficiency of domain name resolution.

s domain name resolution requests. The server firstly resolves the domain name inside its own database, and submits it to superior domain name resolution server if the domain name is not within local domain, till the resolution is completed. The result can either be an IP address, or a non-existing domain name, which will be fed back to the user.

Static resolution sets relationships between domain names and IP addresses manually. When a client requires an IP address corresponding to a domain name, it searches the static domain name resolution table for this designated domain name to get the corresponding IP address

**Configure Static Domain Name Resolution**

Static domain name resolution is conducted through static domain name resolution table, similar to the host file under Windows 95/98 operating system. The router can obtain the IP addresses of common domain names by checking this table. Meanwhile, it is easier for the user to remember host names than the highly abstract IP address to access the corresponding device.

Domain name resolution configuration include:

- Add/delete static domain name resolution table item
- 1 Add/delete static domain name resolution table item

Perform the following task in system view.

**Table 360** Add/delete static domain name resolution table item

| Operation                                    | Command                                     |
|----------------------------------------------|---------------------------------------------|
| Add static domain name resolution table item | <code>ip host domain-name ip-address</code> |

|                                                 |                                                  |
|-------------------------------------------------|--------------------------------------------------|
| Delete static domain name resolution table item | <code>undo ip host domain-name ip-address</code> |
|-------------------------------------------------|--------------------------------------------------|

By default, the system has no static domain name resolution mapping.

Pay attention that when adding a domain name mapping, if the same hostname has been input twice, the current configuration will overwrite the previous one. A static domain name resolution table can maintain a maximum of 50 mapping relationships between domain names and IP addresses.

**Display and Debug Domain Name Resolution**

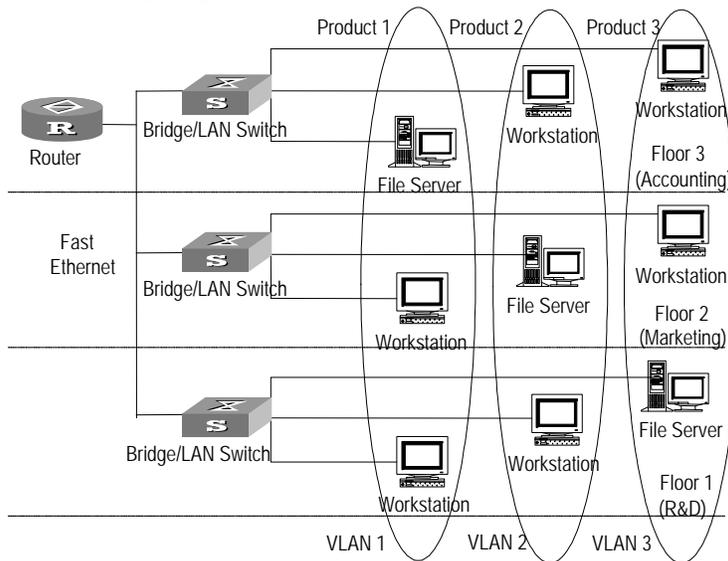
**Table 361** Display and Debug domain name resolution

| Operation                                        | Command                      |
|--------------------------------------------------|------------------------------|
| Display static domain name resolution table item | <code>display ip host</code> |

**VLAN Configuration**

To facilitate the mobility of computers in the network and save bandwidth, we can create VLAN in LAN Switch to meet various requirements. After creating VLAN in LAN Switch port, data communication can be easily implemented within the same VLAN. However, the different VLANs are isolated from each other, so it is necessary to transmit packet between different VLAN in the same way as transmitting it between different LAN segments. The forwarding function between VLANs on the 3Com Router series is implemented by Ethernet interface and it supports IP and IPX packet. In order to save port resources, several subinterfaces can be encapsulated on one Ethernet interface and every subinterface acts as an independent Ethernet interface. Therefore, a physical Ethernet interface can implement data forwarding between several VLANs as shown in the figure below.

**Figure 121** Networking diagram mode of VLAN



In accordance with the IEEE 802.1Q, to implement the VLAN functionality of the 3Com Router series, a 4-byte VLAN tag is placed between the source/destination MAC address of the original Ethernet frame header and the Type field to mark the VLAN message. The format of VLAN tag is shown as below.

**Figure 122** Format of VLAN tag

|                               |   |   |   |        |   |   |   |                              |   |   |   |        |   |   |   |          |   |         |   |   |   |   |   |   |   |   |   |   |   |   |   |
|-------------------------------|---|---|---|--------|---|---|---|------------------------------|---|---|---|--------|---|---|---|----------|---|---------|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Byte 1                        |   |   |   | Byte 2 |   |   |   | Byte 3                       |   |   |   | Byte 4 |   |   |   |          |   |         |   |   |   |   |   |   |   |   |   |   |   |   |   |
| TPID(Tag Protocol Identifier) |   |   |   |        |   |   |   | TCI(Tag Control Information) |   |   |   |        |   |   |   |          |   |         |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 1                             | 0 | 0 | 0 | 0      | 0 | 0 | 1 | 0                            | 0 | 0 | 0 | 0      | 0 | 0 | 0 | Priority | * | VLAN ID |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 7                             | 6 | 5 | 4 | 3      | 2 | 1 | 0 | 7                            | 6 | 5 | 4 | 3      | 2 | 1 | 0 | 7        | 6 | 5       | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

TPID (Tag Protocol Identifier) field has two bytes. When its value is 0X8100, it means the Ethernet frame header contains VLAN tag. The third and fourth byte are TCI (Tag Control Information) fields, with the higher three bits being user priority field, the fourth being the instruction of standard encapsulation format and the other 12 bits being VLAN IDs whose value ranges from 0 to 4094 (the value must begin with 1 on routers).

**Configure VLAN** VLAN Configuration includes:

- Create Ethernet subinterface.
- Specify the VLAN to which Ethernet subinterface belongs.
- Configure IP address of Ethernet subinterface.

**1** Create Ethernet subinterface

Among the VLAN configuration tasks of the 3Com Router series, Ethernet subinterface should first be created and then other functions are to be configured. After deleting Ethernet subinterface, the original interface parameters will be invalidated.

Please implement the following configuration under the system view.

**Table 362** Create Ethernet subinterface

| Operation                                                         | Command                                                                       |
|-------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Create Ethernet subinterface and enter Ethernet subinterface view | <b>interface ethernet</b><br><b>interface-number.subinterface-number</b>      |
| Delete specified Ethernet subinterface                            | <b>undo interface ethernet</b><br><b>interface-number.subinterface-number</b> |

By default, Ethernet subinterface is not created.

**2** Specify the VLAN on which Ethernet subinterface is located

In order to enable a certain Ethernet subinterface to receive and transmit VLAN message, it is necessary to specify to which VLAN the subinterface belongs, i.e., to specify the ID number of the VLAN.

Please implement the following configuration under Ethernet subinterface view.

**Table 363** Specify the VLAN on which Ethernet subinterface is located

| Operation                                                               | Command                            |
|-------------------------------------------------------------------------|------------------------------------|
| Specify the VLAN on which Ethernet subinterface is located              | <b>vlan-type dot1q vid vlan-id</b> |
| Remove the specification for the belonging of the Ethernet subinterface | <b>undo vlan-type</b>              |

By default, Ethernet subinterface does not specify VLAN ID.

It must be noted that if VLAN ID is not specified for the created Ethernet subinterface, the Ethernet subinterface can only carry IPX data, but cannot configure IP address to carry IP data.

**3** Configure IP address of Ethernet subinterface

In as Ethernet interface is connected with a LAN Switch port. As the Ethernet subinterface of every specified VLAN ID can act as an independent gateway, this subinterface and other Ethernet subinterface in the same VLAN ID should belong to the same subnet segment.

Please implement the following configuration under Ethernet subinterface view.

**Table 364** Configure IP address of Ethernet subinterface

| Operation                                     | Command                               |
|-----------------------------------------------|---------------------------------------|
| Configure IP address of Ethernet subinterface | <b>ip address ip-address mask</b>     |
| Delete IP address of Ethernet subinterface    | <b>undo ip address [ ip-address ]</b> |

By default, no IP address is defined.

Ethernet subinterface acts as a gateway in VLAN and so the subnet number of its IP address must be correct. The default gateway of LAN Switch ports that belong to the same VLAN should be set as the IP address of this subinterface. Besides, the IP address of Ethernet subinterface can be set only when this subinterface has finished the configuration of VLAN ID.

**Display and Debug VLAN**

**Table 365** Display and Debug VLAN

| Operation                                                   | Command                   |
|-------------------------------------------------------------|---------------------------|
| Display the relevant information of all the configured VLAN | <b>display vlan</b>       |
| Enable the debugging of the Ethernet                        | <b>debugging ethernet</b> |

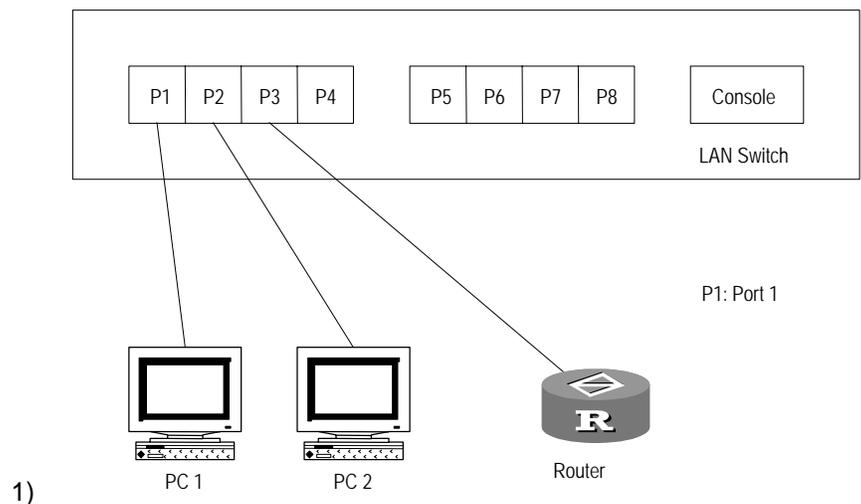
**Typical VLAN Configuration Example**

**I. Networking Requirements**

Two PCs respectively belongs to two VLANs and a router is used to implement data forwarding between two different VLANs.

**II. Networking Diagram**

**Figure 123** Networking diagram for configuring VLAN forwarding



**III. Configuration Procedure**

- 1) Configure the 3Com Routers:
  - a) Create and enter the view of Ethernet subinterface Ethernet0.1

```
[Router] interface ethernet 0.1
```

**b** Specify 3 as the ID number of the VLAN on which the subinterface is located.

```
[Router-Ethernet0.1] vlan-type dot1q vid 3
```

**c** Configure IP address for the subinterface.

```
[Router-Ethernet0.1] ip address 3.3.3.8 255.255.255.224
```

**d** Create and enter the view of Ethernet subinterface Ethernet0.2.

```
[Router] interface ethernet 0.2
```

**e** Specify 4 as the ID number of the VLAN on which the subinterface is located.

```
[Router-Ethernet0.2] vlan-type dot1q vid 4
```

**f** Configure IP address for the subinterface.

```
[Router-Ethernet0.2] ip address 3.3.3.55 255.255.255.224
```

## 2 Configure LAN Switch:

**a** Configure the port information of LAN Switch

```
Port :
Port1 : default Vlan id : 3 port type: untagged
Port2 : default Vlan id : 4 port type: untagged
Port3 : default Vlan id : 0 port type: tagged
```

**b** Configure VLAN information of LAN Switch.

```
Vlan :
Unknown Vlan :Discard
Vlan index : 0
Vlan id : 003
Including ports:
Port 1 : 'YES'
Port 2 : 'NO'
Port 3 : 'YES'
Unknown Vlan :Discard
Vlan index : 1
Vlan id : 004
Including ports:
Port 1 : 'NO'
Port 2 : 'YES'
Port 3 : 'YES'
```

## Fault Diagnosis and Troubleshooting of VLAN

**Fault: Ping the IP address of the Ethernet subinterface in the same VLAN from a PC, but fails.**

Troubleshooting: The steps below can be taken.

- Use **display interface ethernet 0.1** command or **display interface ethernet 0.2** command to ensure that the physical interface of this subinterface and the protocol are both in state Up. If the configuration is correct, whereas the physical interface and the protocol are both in state of Down, please check whether the network cable is correctly connected or not.
- If the physical interface of this subinterface and the protocol are both in state of Up, and the Ping operation still fails, please check whether the LAN Switch configuration is correct. It must be ensured that the default VLAN id of ports connected with router Ethernet interface differs from that of ports connected with PC and the type of all ports must be tagged. However, the type of all ports

connected with PC must be set as “untagged” for the reason that PC cannot identify data packet marked with VLAN tag.

### **Fault: Ping Two PCs, but fails to ping them through.**

Troubleshooting: The steps below can be taken.

- First, ping the IP address of Ethernet subinterface in the same VLAN from a PC. If the ping fails, solve the problem according to the method described in fault one.
- If one PC can ping through the IP address of Ethernet subinterface in the same VLAN, but fails to ping through another PC, please use the command **route print** in MS-DOS of the two PCs to see if the route to peer PC is available. If not, please add the relevant route.

## **DHCP Server Configuration**

### **Background of the DHCP development**

As the scale of networks grows and their complexities increase, network configurations become more and more complex. The original BOOTP protocol for static host configuration cannot satisfy the demands of users, especially on the occasions when computers are always on the move (e.g., using laptops or wireless network) and the number of actual computers exceeds that of the available IP addresses. To facilitate users to improve utilization ratio of resources and to support diskless networking mechanisms, the DHCP (Dynamic Host Configuration Protocol) based on BOOTP was developed. Similar to the BOOTP protocol, DHCP works in client-server mode. With this protocol, a DHCP client can dynamically request configuration information from a DHCP server, including important parameters such as assigned IP addresses, subnet masks and default gateways, etc. DHCP server can also conveniently configure this information dynamically for DHCP clients.

### **DHCP vs BOOTP**

- Both BOOTP and DHCP adopt the client/server communication mode. A client applies to the server for configurations (including the configurations of important parameters such as allocated IP address, subnetmask, and the default gateway). Then, the server will return the corresponding configuration information according to the policies. Both types of packets are encapsulated with the UDP packets. Furthermore, their structures are almost the same.
- BOOTP is running in a relatively static (every host is connected by a permanent network) environment. Hence, administrators should configure special BOOTP parameter files for each host and then, these files will stay the same for a relatively long time.
- DHCP extends the BOOTP from two aspects: DHCP enables computers to obtain all the needed configuration information by using one message and it allows computers to rapidly and dynamically obtain IP addresses so to avoid statically specifying addresses for each host by BOOTP.

### **IP address allocation policy provided by DHCP**

Different hosts have different application requirements. For example, some servers perhaps need to use the fixed IP addresses for a long time, some hosts need to use certain IP addresses dynamically allocated for a long period of time and some individuals can arbitrarily use the allocated temporary IP addresses. A

DHCP server can provide three types of IP address allocation policies according to the different requirements:

- Allocate addresses manually: Administrators configure special IP addresses for a small number of particular hosts such as the service server WWW.
- Allocate addresses automatically: Allocate permanent IP addresses for some hosts connected to the network for the first time and the addresses will be allocated to the hosts for a long period of time.
- Allocate addresses dynamically: Allocate some addresses to client hosts by means of “leasing”. In this case, the expiry date is limited and clients should re-apply for new addresses upon the expiry. Most of clients are offered such dynamic addresses.

### Occasions in which DHCP server is applied

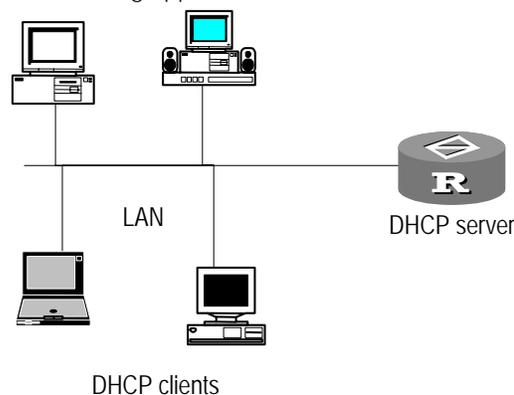
DHCP service is usually used to implement the allocation of IP addresses in the following occasions:

- Network scale is relatively large, manual configuration will consume an enormous working volume and at the same time, it is difficult to centralize the management of the overall network.
- Hosts on the network are more than the IP addresses supported by this network. That is, a fixed IP address cannot be allocated to each host. For example, Internet accessing operators are in this situation. Numerous users must dynamically obtain their own IP addresses through the DHCP service and the number of simultaneous users is limited to a certain degree.
- There are only a few hosts with their own fixed IP addresses on the network (for example, various server hosts need fixed IP addresses) while most hosts have no requirement for fixed IP addresses.

### Fundamentals of DHCP Server

Normally, a typical DHCP application network comprises of a DHCP server and numerous client computers such as PCs and portable computers, as shown in the following figure:

**Figure 124** Typical networking application of DHCP server



To obtain a legal dynamic IP address (the processes of obtaining an auto-allocated address and a manually allocated address are similar), a DHCP client should interact different information with the server in different stages. Normally, there are three types of modes:

- DHCP client logs into the network for the first time

If it is the first time for a DHCP client to log in to the network, it will establish a connection with the DHCP server through four stages:

- Discovering stage. This is the stage when the DHCP client searches the DHCP servers. The DHCP client broadcasts a DHCP\_Discover message to search the DHCP servers, and every host installed with the TCP/IP suite on the network will receive this type of broadcast message but only the DHCP servers respond to it.
- Offering stage. This is the stage when the DHCP servers offer IP addresses. Upon receiving the client DHCP\_Discover message, the DHCP servers select an unallocated IP address from the IP address pools for the DHCP client, and send the DHCP\_Offer message containing leased IP address and other settings to the DHCP client.
- Selecting stage. This is the stage when the DHCP client selects the IP address offered by a certain DHCP server. If multiple DHCP servers send the DHCP\_Offer messages to it, the DHCP client will accept only the first received DHCP\_Offer message. Then, it will respond with a DHCP\_Request message by means of broadcasting. This message requests the selected DHCP server for an IP address.
- Acknowledgement stage. This is the stage when the DHCP server acknowledges the offered IP address. Upon receiving the DHCP\_Request message from the DHCP client, the DHCP server sends back a DHCP\_ACK message containing the offered IP address and other settings to the DHCP client, advising that the offered IP address can be used. Then, the DHCP client will bind its TCP/IP suite with the network card. Except the server selected by the DHCP client, other DHCP servers will use their unallocated IP addresses for the applications of other clients for IP addresses.
- DHCP client logs into the network again:
  - Once the DHCP client logs into the network correctly, it merely needs to send the DHCP\_Request message containing the IP address allocated previously (there is no need to send a DHCP\_Discover message once again).
  - Upon receiving the DHCP\_Request message, the DHCP server will allow the DHCP client to continue to use the original IP address and will return the DHCP\_ACK message.
  - If the IP address can not be allocated to the DHCP client again (in this case, the IP address has been allocated to another DHCP client), the DHCP server will return a DHCP\_NAK message. When the DHCP client receives the DHCP\_NAK message, it needs to send a DHCP\_Discover message to request a new IP address.

In addition, you can use the `ipconfig /release_all` command in the command line on the user PC (that is, the DHCP client) to release the IP address. In this case, the user PC sends a DHCP\_Release message to the DHCP server. Then, you can use the `ipconfig /renew_all` command on the user PC to apply for a new IP address. In this case, the user PC sends a DHCP\_Discover message to the DHCP server.

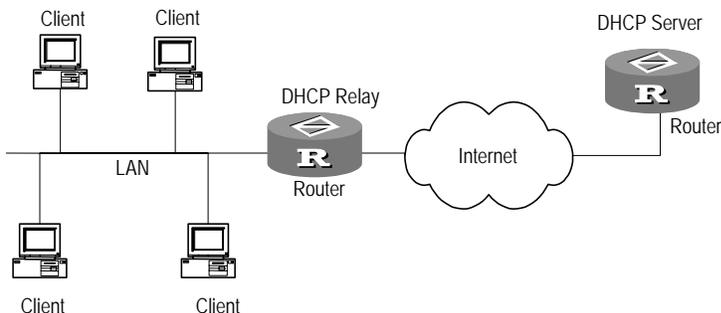
- DHCP client extends the valid period for leasing the IP address:
  - The dynamic IP address of the DHCP client allocated by the DHCP server usually has a certain valid leasing period. Upon the expiry, the DHCP server

will take back the IP address. If the DHCP client wants to continue to use this address, it should renew the IP leasing contract such as extending the leasing contract of the IP address.

- In practice, the DHCP client will automatically send the message for renewing the IP leasing contract to the DHCP server when the DHCP client starts up or half of the valid period of the IP leasing contract has expired. To renew the IP leasing contract, the DHCP client will send a DHCP\_Discover message to the DHCP server. If the IP address is valid, the DHCP server will send back a DHCP\_ACK message to notify the DHCP client that it has obtained a new IP leasing contract. In addition, the `ipconfig /renew` command can be used on the user PC (that is, the DHCP client) to renew its IP leasing contract.
- Priority sequence in which the DHCP server allocates IP address to the client  
The DHCP server will select an IP address for a client in the following order:
  - a IP address in the DHCP Server database, which is statically bound with the MAC address of the client.
  - b IP address that was used by the client.
  - c Address in the requested IP address option contained in the DHCP\_Discover message sent by the client.
  - d IP address that is first found when searching for the IP addresses available for allocation in the DHCP address pool in sequence.
  - e Report the error, if no IP address is available for allocation after going through the above steps.
- Applications of DHCP Server

In practice, to improve the serving efficiency of DHCP servers, a DHCP server will probably be used to serve the clients beyond the LAN. Normally, routers have been added with the function of DHCP relay proxy (that is, providing the across-segment transmission of DHCP packets). Clients in the LAN can communicate with the DHCP servers in other subnetworks through the DHCP relay proxy and finally obtain legal IP addresses.

**Figure 125** Integrated networking application of DHCP server and DHCP relay



Normally, DHCP relay proxy can either be a host or a router as long as the service program of DHCP relay proxy is enabled.

### DHCP Server Configuration

- DHCP server configuration includes:
- Enable/Disable the DHCP service
  - Create a DHCP address pool

- Configure the range of a DHCP address pool
  - Configure the IP addresses that do not participate in auto-allocation in the DHCP address pool
  - Configure the lease valid period of the IP addresses in a DHCP address pool
  - Configure the IP address of the outgoing gateway router at the DHCP client
  - Configure the domain name of the DHCP client
  - Configure the IP address of the DNS server used by the DHCP client
  - Configure the IP address of the NetBIOS server used by the DHCP client
  - Set the type of NetBIOS node for DHCP client
  - Configure the maximum number of ping packets sent by the DHCP server and the maximum time waiting for response
  - Configure the user-defined options
- 1 Enable/disable the DHCP Service

Before performing the DHCP configurations, DHCP service should be enabled first. Only after the DHCP service is enabled, other related DHCP configurations can take effect.

Perform the following configurations in system view.

**Table 366** Enable/disable the DHCP service

| Operation                | Command                 |
|--------------------------|-------------------------|
| Enable the DHCP service  | <b>dhcp enable</b>      |
| Disable the DHCP service | <b>undo dhcp enable</b> |

By default, the DHCP service is disabled.

2 Create a DHCP address pool

To allocate the IP addresses, the user needs to create an address pool on the DHCP server. When the client requests an IP address, the DHCP server will choose an appropriate address pool according to a certain algorithm, it will select an idle IP address from this address pool, and transmit it together with other parameters (e.g. DNS server address, the lease period of the address and so on) to the client. Each DHCP server can be configured with 1 and more address pools. Up to 50 address pools are supported.

An address pool in the DHCP server is organized in the form of a "tree" structure. The root is the address of the natural segment, branches are the subnet addresses of the segment, and the leaf nodes are the manually binding client addresses. In this tree structure, the inheritance of configurations is fulfilled. In other words, subnets (son nodes) inherit the configuration of the natural segment (father node), and like that, the clients (grandson nodes) inherit the configuration parameters of the subnets (son nodes). Therefore, as for some general parameters, such as domain name, the user just needs to perform the configuration on the father node or the son nodes.

Perform the following configurations in system view.

**Table 367** Create a DHCP address pool or entering the DHCP address pool view

| Operation                                                      | Command                              |
|----------------------------------------------------------------|--------------------------------------|
| Create a DHCP address pool or enter the DHCP address pool view | <b>dhcp server ip-pool pool-name</b> |

|                          |                                                 |
|--------------------------|-------------------------------------------------|
| Disable the DHCP service | <code>undo dhcp server ip-pool pool-name</code> |
|--------------------------|-------------------------------------------------|

By default, no DHCP address pool is created.

### 3 Configure the range of a DHCP address pool

#### a Configure the static binding address allocated to the client

Some special clients (e.g., WWW server) need to be bound with fixed IP addresses, that is, to bind a certain client MAC address with a certain IP address. When the client with this MAC address applies for a DHCP address, the server will find the corresponding fixed IP address according to the client MAC address, and allocate it for the client. You can assume that a statically binding address is a special DHCP address pool that contains only one address.

Perform the following configurations in DHCP address pool view.

**Table 368** Configure the statically binding IP address and MAC address

| Operation                                         | Command                                                         |
|---------------------------------------------------|-----------------------------------------------------------------|
| Configure a statically binding IP address         | <code>static-bind ip-address ip-address [ mask netmask ]</code> |
| Delete the statically binding IP address          | <code>undo static-bind ip-address</code>                        |
| Configure a statically binding client MAC address | <code>static-bind mac-address mac-address</code>                |
| Delete a statically binding client MAC address    | <code>undo static-bind mac-address</code>                       |

By default, no binding of DHCP client IP address and MAC address is configured. For the binding client MAC address, the default type is **ethernet**.



*The command `static-bind ip-address` must be used together with the `static-bind mac-address` command. None of them have the superposition function, that is, the latest configuration will replace the previous one.*



*The command `network` and the commands `static-bind ip-address` and `static-bind mac-address` are conflicting. In other words, a DHCP address pool can be used either to configure statically binding addresses or the dynamic addresses, but not both.*

#### b Configure the dynamic IP addresses allocated to clients

For the addresses dynamically allocated to the clients (including the permanent dynamic addresses and those dynamic addresses with a limited lease period), it is necessary to configure the range of the address pool. Only one address segment can be configured in one address pool, and the mask can be used to set the address range.

Perform the following configurations in DHCP address pool view.

**Table 369** Configure the range of the dynamically allocated IP addresses

| Operation                                                     | Command                                          |
|---------------------------------------------------------------|--------------------------------------------------|
| Configure the range of the IP addresses allocated dynamically | <code>network ip-address [ mask netmask ]</code> |
| Delete the range of the IP addresses allocated dynamically    | <code>undo network</code>                        |

By default, no DHCP address pool is configured, that is, there are no allocable addresses.



The command **network** cannot be superimposed, that is, the latest configuration will overwrite the previous one.



The command **network** and the commands **static-bind ip-address** and **static-bind mac-address** are conflicting. In other words, for the same DHCP address pool, configure either dynamically binding address or the dynamic address, but not both.

#### 4 Configure the IP Addresses in the DHCP Address Pool not participating in Auto-allocation

As for a network or subnetwork, some IP addresses may have been used by some servers or particular hosts, like WWW server, gateway and FTP server. The DHCP server should exclude these addresses to ensure the normal operation of the network when allocating addresses. Otherwise, there will be the possibility that one address is allocated to two hosts, and hence causes the IP address allocation conflict.

By default, no IP address that does not participate in the auto-allocation is configured. As for some IP addresses that do not participate in the allocation, use the **dhcp server forbidden-ip** command to avoid their allocations.

Perform the following configurations in system view.

**Table 370** Configure the IP addresses in an address pool that do not participate in auto-allocation

| Operation                                                                                      | Command                                                                   |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Configure the IP addresses in a DHCP address pool that will not participate in auto-allocation | <b>dhcp server forbidden-ip<br/>low-ipaddress [ high-ipaddress ]</b>      |
| Delete the IP addresses in a DHCP address pool that do not participate in auto-allocation      | <b>undo dhcp server forbidden-ip<br/>low-ipaddress [ high-ipaddress ]</b> |

By default, IP addresses that do not participate in auto-allocation are not configured. That is, all the addresses are assumed to participate in auto-allocation.



This command can be superimposed. That is, the latest and the original configurations will take effect simultaneously. When using the **undo dhcp server forbidden-ip** command to delete the address-excluding setting, make sure that the parameters are totally consistent with those originally configured. That is, do not delete only some addresses originally configured.

#### 5 Configure IP Address Leasing Valid Period for DHCP Address Pool

According to various purposes of client hosts, a DHCP server can specify different valid periods of address leasing for different address pools and thus enhance the application flexibility. All the addresses in the same DHCP address pool own the same valid period. Address leasing valid period can not be inherited.

Perform the following configurations in DHCP address pool view.

**Table 371** Configure IP address leasing valid period for DHCP address pool

| Operation                                                                                                               | Command                                                                        |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Configure the leasing valid period of the dynamically allocated IP address for a DHCP address pool                      | <b>expired { day day [ hour<br/>hour [ minute minute ] ]  <br/>unlimited }</b> |
| Restore the leasing valid period of the dynamically allocated IP address for the DHCP address pool to the default value | <b>undo expired</b>                                                            |

By default, the valid leasing period of IP address is 1 day.

## 6 Configure the IP Address of Egress Gateway Router for DHCP Clients

When a DHCP client accesses a server (or host) beyond the local subnetwork, all the data must be sent and received via the egress gateway for the local network. Only a maximum of 8 egress gateway addresses can be configured in each DHCP address pool.

Perform the following configurations in DHCP address pool view.

**Table 372** Configure the gateway router address of client

| Operation                                           | Command                                                                           |
|-----------------------------------------------------|-----------------------------------------------------------------------------------|
| Configure the egress gateway address of DHCP client | <b>gateway-list</b> <i>ipaddress1</i> [ <i>ipaddress2</i> ... <i>ipaddress8</i> ] |
| Delete the egress gateway address of DHCP client    | <b>undo gateway-list</b> { <i>ip-address</i>   <b>all</b> }                       |

By default, the egress gateway address of DHCP client is not configured.



*When specifying multiple egress gateway addresses, you need to continuously configure up to two addresses in the **gateway-list** command, instead of using this command repeatedly. That is because the new egress gateway address will replace the previous one other than superimposing it.*

## 7 Configure Domain Name of DHCP Client

In DHCP servers, the domain names used by the corresponding clients can be specified respectively for each address pool.

Perform the following configurations in DHCP address pool view.

**Table 373** Configure the domain names of DHCP clients

| Operation                                            | Command                              |
|------------------------------------------------------|--------------------------------------|
| Configure the domain name allocated to a DHCP client | <b>domain-name</b> <i>domainname</i> |
| Delete the domain name allocated to a DHCP client    | <b>undo domain-name</b>              |

By default, the domain names allocated to DHCP clients are not configured.

## 8 Configure IP Address of DNS Used by DHCP Clients

When a computer accesses the Internet through the domain name, the domain name should be resolved to IP addresses. To access the DHCP client to the Internet, a DHCP server specifies the DNS address for the client when allocating the IP address to it. Each DHCP address pool can be configured with up to a maximum of 8 DNS addresses.

Perform the following configurations in DHCP address pool view.

**Table 374** Configure the DNS addresses in a DHCP address pool

| Operation                                             | Command                                                                       |
|-------------------------------------------------------|-------------------------------------------------------------------------------|
| Configure the addresses of DNSes for the DHCP clients | <b>dns-list</b> <i>ipaddress1</i> [ <i>ipaddress2</i> ... <i>ipaddress8</i> ] |
| Delete the IP addresses of DNSes for the DHCP clients | <b>undo dns-list</b> { <i>ip-address</i>   <b>all</b> }                       |

By default, the IP address of DNS is not configured.



*When specifying multiple DNS's, you need to continuously configure up to two addresses in the **dns-list** command, instead of using this command repeatedly.*

*That is because the new DNS address will replace the previous one rather than superimpose it.*

## 9 Configure IP Address of NetBIOS Server Used by DHCP Clients

Clients can communicate through the NetBIOS protocol. As for the clients installed with the Microsoft operating system, WINS (Windows Internet Naming Service) Server will provide the hostname-to-IP-address resolution mechanism for the hosts adopting the NetBIOS protocol. Therefore, WINS setting is necessary for most Windows network clients. Each DHCP address pool can be configured with up to a maximum of 8 NetBIOS addresses.

Perform the following configurations in DHCP address pool view.

**Table 375** Configure the address of NetBIOS server used by DHCP clients

| Operation                                                    | Command                                                            |
|--------------------------------------------------------------|--------------------------------------------------------------------|
| Configure the address of NetBIOS server used by DHCP clients | <code>nbns-list ip-address1 [ ip-address2 ... ip-address8 ]</code> |
| Delete the address of NetBIOS server used by DHCP clients    | <code>undo nbns-list { ip-address   all }</code>                   |

By default, the IP address of NetBIOS server is not configured.



*When specifying multiple NetBIOS servers, you need to continuously configure up to two addresses in the `nbns-list` command, instead of using this command repeatedly. That is because the new NetBIOS server address will replace the previous one other than superimpose it.*

## 10 Set the type of NetBIOS node for DHCP client

When DHCP clients use the NetBIOS protocol to communicate on WANs, the mapping relations should be established between host names and IP addresses. There are four types of NetBIOS nodes for obtaining mapping relations:

- **b-node**: Obtain the mapping between them by means of broadcast.
- **p-node**: Obtain the mapping relation by means of communicating with a NetBIOS server.
- **m-node**: p-node owning part of the broadcasting features.
- **h-node**: b-node owning the “peer-to-peer” communicating mechanism.

Perform the following configurations in DHCP address pool view.

**Table 376** Set the type of NetBIOS node for DHCP client

| Operation                                                             | Command                                                         |
|-----------------------------------------------------------------------|-----------------------------------------------------------------|
| Set the type of NetBIOS node for DHCP client                          | <code>netbios-type { b-node   h-node   m-node   p-node }</code> |
| Restore the type of NetBIOS node for DHCP client to the default value | <code>undo netbios-type</code>                                  |

By default, clients adopt **h-node**.

## 11 Configure Maximum Number of ping Packets Sent by the DHCP Server and the Longest Time Waiting for Response

Before allocating an IP address to a client, the DHCP server should detect this IP address. That is, checking whether there is response through pinging the host with this address. If no response is received after the longest time waiting for a response, re-send ping packets to this address until reaching the maximum number of ping packets allowed to be sent. If still no response is received, you can

assume that the IP address in this segment is not in use. Only when it is not in use can the IP address be allocated to the specified client.

Perform the following configurations in system view.

**Table 377** Configure maximum number of ping packets sent by DHCP server & time for response

| Operation                                                                                                         | Command                                                |
|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Configure the maximum number of ping packets sent by the DHCP server                                              | <code>dhcp server ping { packets number }</code>       |
| Restore the maximum number of ping packets sent by the DHCP server to the default value                           | <code>undo dhcp server ping packets</code>             |
| Configure the longest time waiting for response after ping packets are sent by the DHCP server                    | <code>dhcp server ping { timeout milliseconds }</code> |
| Restore the longest time waiting for response after ping packets are sent by the DHCP server to the default value | <code>undo dhcp server ping timeout</code>             |

By default, the number of ping packets being sent is 2 and the time waiting for ping response packets is 500ms.

## 12 Configure self-defined options

As DHCP continuously develops, you can support these new options/development by adding add them to the attribute tables of the DHCP servers by means of the self-defined options.

Perform the following configurations in DHCP address pool view.

**Table 378** Configure DHCP self-defined options

| Operation                            | Command                                                                                                    |
|--------------------------------------|------------------------------------------------------------------------------------------------------------|
| Configure DHCP self-defined options  | <code>option code { ascii ascii-string   hex hex-string [ hex-string... ]   ip-address ip-address }</code> |
| Delete the DHCP self-defined options | <code>undo option code</code>                                                                              |

## Display and Debug DHCP Server

Use `reset`, `debugging` and `display` command in All views.

**Table 379** Display and Debug DHCP servers

| Operation                                                                   | Command                                                              |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------|
| Display the address binding information of DHCP                             | <code>display dhcp server ip-in-use [ ip-address ]</code>            |
| Reset all the address binding information of DHCP                           | <code>reset dhcp server ip-in-use { all   ip-address }</code>        |
| Display the statistic information of address conflicts of DHCP              | <code>display dhcp server conflict [ ip-address ]</code>             |
| Reset all the statistics of address conflicts of DHCP                       | <code>reset dhcp server conflict { all   ip-address }</code>         |
| Display the statistics of DHCP server                                       | <code>display dhcp server statistics</code>                          |
| Reset all the statistics of DHCP server                                     | <code>reset dhcp server statistics</code>                            |
| Display the information of the available addresses in the DHCP address pool | <code>display dhcp server expired</code>                             |
| Display the information of the tree structure in the DHCP address pool      | <code>display dhcp server tree</code>                                |
| Enable the DHCP server debugging                                            | <code>debugging dhcp server { events   packet   ip-relation }</code> |

## Typical DHCP Server Configuration Example

The common DHCP networking methods can be classified into two categories: One is that the DHCP server and the clients reside on the same subnetwork and they directly carry out the interaction of DHCP. Another one is that the DHCP server and the clients reside on different subnetworks and they must implement the allocation of IP addresses through the DHCP relay proxy. In both these cases, the DHCP configurations are the same.

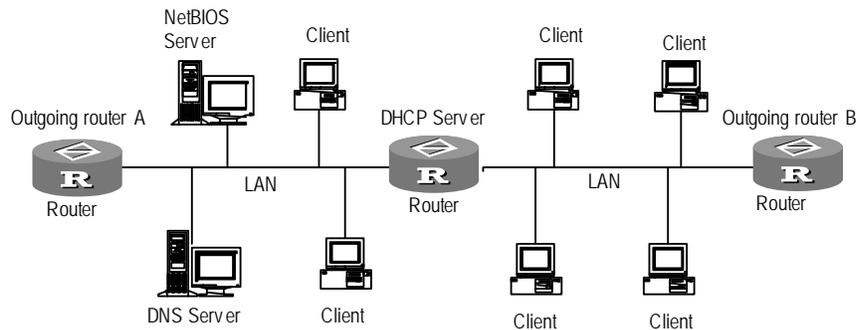
### I. Networking Requirements

DHCP server allocates IP addresses dynamically for the clients in the same segment, the address pool segment 10.1.1.0 is divided into two segments: 10.1.1.0 (the mask is 255.255.255.128) and 10.1.1.128 (the mask is 255.255.255.128). The two Ethernet interfaces of the DHCP server are 10.1.1.1 (the mask is 255.255.255.128) and 10.1.1.129 (the mask is 255.255.255.128) respectively.

In the segment 10.1.1.0, the address lease period is 10 days and 12 hours, the domain name is 3com.com. The DNS address is 10.1.1.2, without NetBIOS address, and the outgoing router address is 10.1.1.126. In the segment 10.1.1.128, the address lease period is 5 days, the DNS address is 10.1.1.2, the NetBIOS address is 10.1.1.4, and the outgoing router address is 10.1.1.254.

### II. Networking Diagram

**Figure 126** DHCP server and clients reside in the same network



### III. Configuration Procedures

- 1 Enable the DHCP service.
 

```
[Router] dhcp enable
```
- 2 Configure the IP addresses (DNS address, NetBIOS address and outgoing gateway address) that do not participate in auto-allocation.
 

```
[Router] dhcp server forbidden-ip 10.1.1.2
[Router] dhcp server forbidden-ip 10.1.1.4
[Router] dhcp server forbidden-ip 10.1.1.254
```
- 3 Configure the common attributes (pool address range, domain name, DNS address) of DHCP address 0.
 

```
[Router] dhcp server ip-pool 0
[Router-dhcp0] network 10.1.1.0 mask 255.255.255.0
[Router-dhcp0] domain-name 3com.com
[Router-dhcp0] dns-list 10.1.1.2
```

- 4 Configure the attributes (address pool range, outgoing gateway and address lease period) in DHCP pool 1.

```
[Router] dhcp server ip-pool 1
[Router-dhcp1] network 10.1.1.0 mask 255.255.255.128
[Router-dhcp1] gateway-list 10.1.1.126
[Router-dhcp1] expired day 10 hour 12
```

- 5 Configure the attributes (address pool range, outgoing gateway, NetBIOS address, and address lease period) in DHCP pool 2.

```
[Router] dhcp server ip-pool 2
[Router-dhcp2] network 10.10.1.128 mask 255.255.255.128
[Router-dhcp2] expired day 5
[Router-dhcp2] nbns-list 10.1.1.4
[Router-dhcp2] gateway-list 10.1.1.254
```

### Troubleshooting **Fault: Dynamic IP address allocation conflict occurs at the client.**

Solution: Following these steps to solve this problem.

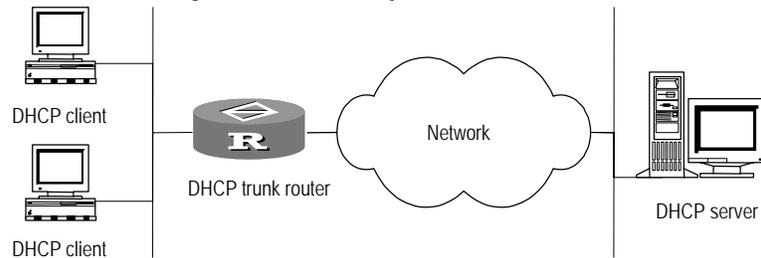
- 1 First of all, determine whether there is a host with this IP address on the network. You can perform the ping operation with relative long timeout to check the connectivity of this IP address.
- 2 If a host with this IP address exists, you need to use the command **dhcp server forbidden-ip** to configure this IP address does not participate in dynamic address allocation.
- 3 At the client, use **ipconfig /release\_all** command to release the IP address dynamically, and use **ipconfig /renew\_all** to re-apply dynamic addresses.

---

## Configure DHCP Relay

As the scale of networks grows and their complexities increase, network configurations become more and more complex. The original BOOTP protocol for static host configuration cannot satisfy the demands of users, especially on the occasions when computers are always on the move (e.g., using laptops or wireless network) and the number of actual computers exceeds that of the available IP addresses. To facilitate users to improve utilization ratio of resources and to support diskless networking mechanisms, the DHCP (Dynamic Host Configuration Protocol) based on BOOTP was developed. Similar to the BOOTP protocol, DHCP works in client-server mode. With this protocol, a DHCP client can dynamically request configuration information from a DHCP server, including important parameters such as assigned IP addresses, subnet masks and default gateways, etc. DHCP server can also conveniently configure this information dynamically for DHCP clients.

However, original DHCP can only take effect in a sub-net, and cannot work across different network segments, which is obviously not economic. So, it is necessary to set a DHCP server on all network segments for dynamic host configuration. This problem is solved by the introduction of DHCP relay, which relays relative messages to a destination DHCP server, so that multiple networks can share a DHCP server, which is more cost-effective and convenient for centralized management.

**Figure 127** Schematic diagram of DHCP relay

The above figure is the schematic diagram of DHCP relay. Its working principle is as follows:

After starting DHCP client, a configuration request message is broadcast and the DHCP relay router will send the message to the designated DHCP server on the other network after processing it properly. According to the information provided by the client, the server sends configuration information to the client via DHCP relay and completes the dynamic configuration of host.

DHCP relay actually realizes transparent transmission of broadcast messages, i.e. transmitting broadcast messages of DHCP clients to DHCP servers on other network segments. Besides, the user can also configure transparent transmission for broadcast messages of designated protocols as required, to enable specific protocol broadcast messages of this network segment to arrive at other network segments. Similarly, the destinations are specified by IP auxiliary addresses. For example, transmit TFTP and DNS protocol messages transparently to corresponding servers.

To implement the DHCP relay, users have to configure IP auxiliary addresses to specify the DHCP server addresses.

## Configure DHCP Relay

DHCP configuration includes:

- Configure interface relay address
- Configure transparent transmission forwarding protocol.

### 1 Configure interface relay address

To implement DHCP relay function, you need to configure IP relay address to specify DHCP server address. For DHCP relay, IP relay address specifies DHCP server. After configuration the broadcast messages received by this interface will be sent to the relay address. The interface configured with IP helper address should support broadcast mode. An interface can be configured with up to 20 relay addresses.

Perform the following task in Ethernet interface view.

**Table 380** Configure interface relay address

| Operation                         | Command                                           |
|-----------------------------------|---------------------------------------------------|
| Configure interface relay address | <code>ip relay-address ip-address</code>          |
| Delete interface relay address    | <code>undo ip relay-address [ ip-address ]</code> |

By default, an interface has no IP address.

### 2 Configure transparent transmission forwarding protocol

UDP needs to be forwarded Broadcast messages of common protocols usually adopt UDP. The destination port number of UDP is configured to set the transparent transmission protocol. For example, transparent transmission of TFTP broadcast messages (port number 69) and DNS protocol broadcast messages (port number 53) can be configured. At most 20 transparent transmission forwarding protocols can be configured.

Perform the following task in system view.

**Table 381** Configure transparent transmission forwarding protocol

| Operation                                           | Command                                    |
|-----------------------------------------------------|--------------------------------------------|
| Add transparent transmission forwarding protocol    | <b>ip relay protocol udp port</b>          |
| Delete transparent transmission forwarding protocol | <b>undo ip relay protocol udp [ port ]</b> |

By default, no transparent transmission forwarding protocol is configured.

## Display and Debug DHCP Relay

**Table 382** Display and debug of DHCP relay

| Operation                                                                    | Command                            |
|------------------------------------------------------------------------------|------------------------------------|
| Display the current transparent transmission protocol                        | <b>display ip relay protocol</b>   |
| Display helper addresses of respective interfaces                            | <b>display ip relay-address</b>    |
| Turn on DHCP relay and transparent transmission debugging information switch | <b>debugging ip relay protocol</b> |

## DHCP Relay Configuration Example

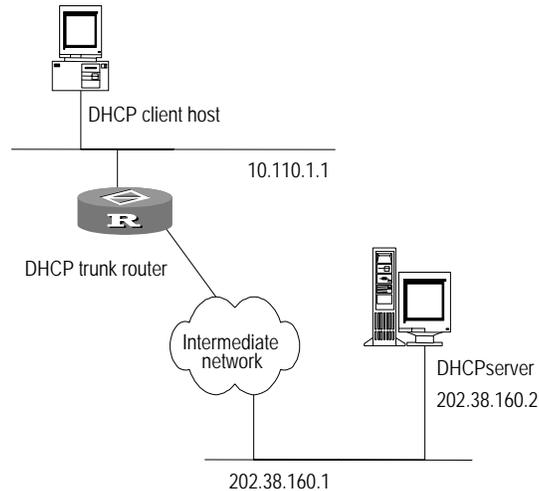
### I. Configuration Requirement

DHCP client host is in the network segment 10.110.0.0, while DHCP server is in the network segment 202.38.0.0. DHCP relay router needs to relay DHCP messages, so that DHCP client hosts can obtain configuration information such as IP address from DHCP server through application.

DHCP server should be assigned with an address pool in network segment 10.110.0.0, so that it can assign proper address information to the DHCP client host on the network segment. Meanwhile, the route to 10.110.0.0 should be available on DHCP server.

## II. Networking Diagram

**Figure 128** Networking diagram of an DHCP relay configuration example



## III. Configuration Procedure

- 1 Configure DHCP relay router:

```
[Router-Ethernet0] ip address 10.110.1.1 255.255.0.0
[Router-Ethernet0] ip relay-address 202.38.160.2
```

To configure helper address 202.38.160.2 on the Ethernet interface 0 you need to specify the address for the DHCP server. When requesting for configuration information, the DHCP client host sends out a DHCP broadcast message. After receiving the broadcast message, the Ethernet interface of the DHCP relay router processes and sends it to the helper address of the interface, i.e. the DHCP server. The DHCP server returns the generated reply message to the DHCP relay router, then the router notifies the DHCP client host of the reply message.

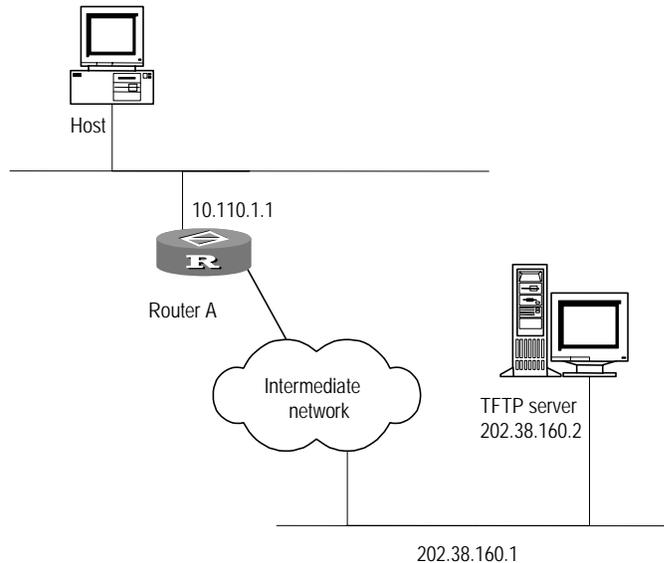
## Configuration example of transparent transmission forwarding protocol

### I. Configuration Requirements

The host and TFTP server should not be in the same network segment. As the host does not know the IP address of TFTP server, it sends a request message with the broadcast address as the destination address so as to transmit it transparently to the TFTP server via router A.

## II. Networking Diagram

**Figure 129** Configuration example of transparent transmission forwarding protocol



## III. Configuration Procedure

### 1 Configure Router A:

```
[Router] ip relay protocol udp 69
[Router] interface ethernet 0
[Router-Ethernet0] ip address 10.110.1.1 255.255.0.0
[Router-Ethernet0] ip relay-address 202.38.160.2
```

## Troubleshooting DHCP

When DHCP relay or transparent transmission function is abnormal, locate the fault with **display** command or debugging information. Here are some common faults as examples to illustrate the troubleshooting procedure.

### Fault 1: (DHCP client host fails to obtain configuration information.)

Troubleshooting: perform as follows.

- Check whether the DHCP server is configured with the address pool of the network segment where the DHCP client host is located.
- Check whether the DHCP relay router and the DHCP server have routes reachable to each other.
- Check whether the DHCP relay router is configured with the correct helper address on the client host interface, and whether multiple helper addresses have caused a collision.

### Fault 2: fail to forward transparent transmission protocol.

Troubleshooting: perform as follows.

- Display the current forwarding protocol.
- Display the helper addresses configured for the interface.
- Check whether there is a reachable route between the source and target equipment of transparent transmission.

- Check whether the transparent transmission router itself is configured with services of the protocol transmitted transparently.

## Configure Network Address Translation (NAT)

Network Address Translation (NAT), also known as address proxy, implements the function for the private network to visit the external network.

### Private Network Address and Public Network Address

Private address refers to the address of the internal network or the host computer. Public address refers to the sole IP address worldwide on the Internet. The Internet Address Allocation Organization prescribes that the following IP addresses be retained as private addresses:

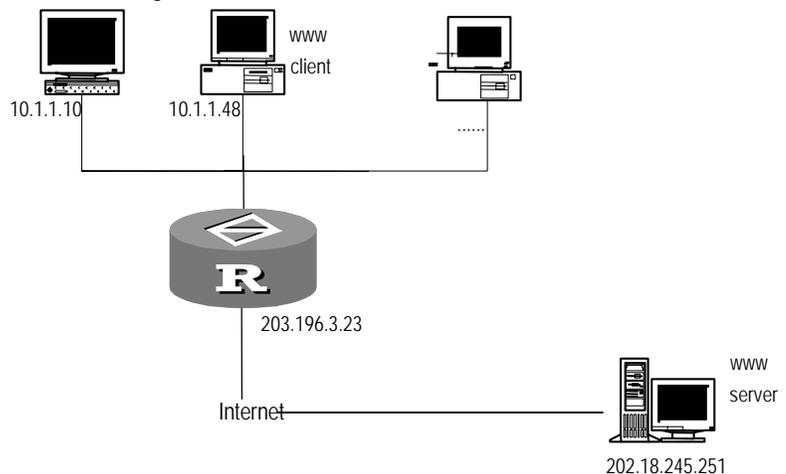
- 10.0.0.0 --- 10.255.255.255
- 172.16.0.0 --- 172.31.255.255
- 192.168.0.0 --- 192.168.255.255

That is to say, the addresses within the three ranges will not be allocated on the Internet. They can be used internally in a unit or a company. The enterprises can select appropriate internal network addresses according to their forecast of the number of internal host computers and networks in future. The internal network addresses of different enterprises can be the same. Disorders are most likely to occur, if a company select the network segments outside the three ranges above as the internal network address.

### Under which condition should the address be translated

As shown in the diagram above: The address needs to be translated when the host computer of the internal network visits the Internet or communicates with the host computers of the external networks.

**Figure 130** Schematic diagram of Network Address Translation (NAT)



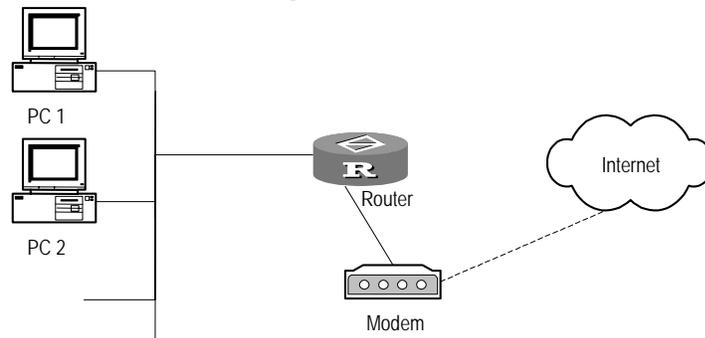
The address of the internal network is 10.0.0.0 network segment, while the formal external IP address is 203.196.3.23. The internal host computer 10.1.1.48 visits the server 202.18.245.251 outside the network by means of WWW. The host computer 10.1.1.48 sends one data message with the source port selected as 6048 and the destination port as 80. After it passes by the proxy server, the source address and port of the data message will probably be changed to

203.196.3.23:32814. The destination address and port remains unchanged. In the proxy server, it maintains one corresponding table of address port. After the WWW server of the external network returns a result, the proxy server will translate the destination IP address and port in the result data message to 10.1.1.48:6084. In this way, the internal computer 10.1.1.48 will be able to visit the external server.

### The role the Network Address Translation (NAT) plays

During the course of the development of the Internet, Network Address Translation first emerged as a solution to tackle the problem of Internet address shortage. As show in the diagram below: after address translation, PC1 and PC2 will have access to the resources on the Internet by Modem.

**Figure 131** Access the Internet through address translation



### Mechanism of Network Address Translation (NAT)

The mechanism of address translation is to translate the IP address and port number of the host computer in the network to the external network address and port number, to implement the translation from <internal address + port number> to <external address + port number>.

### Characteristic of Network Address Translation (NAT)

- Transparent address allocation to the user (allocation of the external addresses)
- Achievement of "transparent routing" effect. The routing here refers to the ability to forward IP message, not a technique of the exchange of routing information.

### Advantages and Disadvantages of Network Address Translation (NAT)

Advantages:

- It enables the host computer of the external network to visit the network resources through this function.
- It provides privacy protection for the internal host computer.

Disadvantages:

- IThe header of the data message concerning IP address can't be encrypted, as the IP address in the data message needs to be translated. In application protocol, FTP link encryption can't be used. Otherwise, the port command of FTP can't be translated correctly.

- The debugging of the network becomes even more difficult. For instance, when one host machine of the internal network attempts to attack other networks, it is very difficult to pinpoint which computer is attacking computer, since the IP address of the host machine is shielded.

### Performance of Network Address Translation (NAT)

When the speed of the broadband of the link is below 1Mbps, the address translation has little impact on the performance of the network. In this case, the bottleneck of the network transmission is on the transmission line. When the speed is above 1Mbps, the address translation will have some impact on the performance of the routers.

### Configure NAT NAT configuration includes:

- Configure the address pool
- Configure the correlation between the access control list and address pool
- Configure the correlation between the access control list and the interface (EASY IP)
- Configure the internal server
- Configure the valid time of address translation

#### 1 Configure the address pool

The address pool is a pool of the consecutive IP addresses. When the internal data packet arrives at the external network through address translation, it will select one address from the address pool as the translated source address.

Please process the following configurations in the system view.

**Table 383** Configure address pool

| Operation               | Command                                                |
|-------------------------|--------------------------------------------------------|
| Define one address pool | <b>nat address-group start-addr end-addr pool-name</b> |
| Delete one address pool | <b>undo nat address-group pool-name</b>                |

All the addresses in the address pool should be consecutive. For the most, 64 addresses can be defined in each address pool.



*An address pool can not be deleted, if it is correlated to one access control list and address translation has started.*

#### 2 Configure the correlation between the access control list and address pool

Multiple-to-multiple address translation can be implemented, after the access control list and the address pool are correlated. The access control list is generated by **rule** command. It defines some rules, according to the format of the header of the IP data packet message and the header of data packet of the lower layer protocol it bears, which denotes the enable or disable of the data packets with certain features. For the data packet configured with NAT, it goes though address analysis before the message is forwarded. For the data packet no configured with NAT, it goes ahead with the normal forwarding process.

s according to this correlation relationship the addresses are translated. When the data packets of the internal network are to be transmitted to the external network: firstly, it is determined if the data packets are allowed according to the

access control list, then locate the corresponding data pool according to the correlation. Thus, the source address is translated into one address in the data pool and the address translation process is completed. In the translation correlation form, the necessary corresponding information of the translation, including access list, data pool information and the HASH table index corresponding to the address pool are recorded.

HASH table is correlated to the data pool. That is to say, “the data packet that implements address translation using the addresses in the address pool” will have the record recorded in HASH table. During the translation, we can find the data pool that corresponds with the data packet according to the translation relationship. According to the address pool, we can find HASH and records the translation record in the corresponding HASH table. In the restoration process, the address pool can be located according to the destination address. And according to the address pool, the relevant HASH table can be located, to implement restoration operation.

Please carry out the following configuration under interface view.

**Table 384** Configure the correlation between the access control list and address pool

| Operation                                                                | Command                                                     |
|--------------------------------------------------------------------------|-------------------------------------------------------------|
| Add the correlation between the access control list and address pool.    | <b>nat outbound acl-number address-group pool-name</b>      |
| Delete the correlation between the access control list and address pool. | <b>undo nat outbound acl-number address-group pool-name</b> |

By default, the access control list is not correlated to any address pools.

### 3 Configure the incidence between the access control list and the interface (EASY IP feature)

Configure the correlation between the access control and the interface is also known as EASY IP feature. It refers to taking the IP address of the interface as the translated source address directly during the course of address translation, which is applicable to two conditions. In dial view, the user hopes to take the interface IP address obtained through negotiation as the translated source address; or the user hopes to take the IP address of the interface itself as the translated source address.

Please carry out the following configuration under interface view.

**Table 385** Configure the correlation between the access control list and the interface

| Operation                                                             | Command                                       |
|-----------------------------------------------------------------------|-----------------------------------------------|
| Add the correlation between the access control list and interface.    | <b>nat outbound acl-number interface</b>      |
| Delete the correlation between the access control list and interface. | <b>undo nat outbound acl-number interface</b> |

By default, the access control list is not correlated to any interface.

### 4 Configure the Internal Server

The user can map the corresponding external address, the external port number etc. to the internal server, to implement function for the external network to visit the internal server. The mapping table between the internal server and external network address and port number is configured by **nat server** command. During the course of address restoration, the destination address of the external data packet will be looked up according to the configuration of the user. To visit the internal server, it is translated to the destination address and port number of the

corresponding internal server. During the course of address translation, it will look up the resource address of the message, to determine if the message is sent from the internal server. If yes, the source address is translated to the corresponding public network address.

The information the user needs to configure includes: external address, external port, external server address and the type of internal server port and protocol.

Please carry out the following configuration under interface view.

**Table 386** Configure the Internal Server

| Operation                  | Command                                                                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add one internal server    | <code>nat server global global-addr { global-port   any   domain   ftp   pop2   pop3   smtp   telnet   www } inside inside-addr { inside-port   any   domain   ftp   pop2   pop3   smtp   telnet   www } { protocol-number   ip   icmp   tcp   udp }</code> |
| Delete one internal server | <code>undo nat server { global   inside } address { port   any   domain   ftp   pop2   pop3   smtp   telnet   www } { protocol-number   ip   icmp   tcp   udp }</code>                                                                                      |



*inside-port is indispensable, ranging 1 to 65535.*



*If global-port is not defined, its value equals to that of inside-port.*



*When deleting one internal server, if the global key word is used, then the external address, port and protocol information also need to be provided; If inside key word is used, only the internal address and port number need to be provided.*



*The protocol can be TCP, UDP, IP or ICMP.*

#### 5 Configure the Timeout of address translation

As the HASH table used in the address translation can't be saved permanently, the user can set up the Timeout of address translation for TCP, UDP and ICMP protocol. If this address is not used for translation within the time set up, the system will delete the link.

Please process the following configurations in the system view.

**Table 387** Configure the Timeout of address translation

| Operation                                                       | Command                                                  |
|-----------------------------------------------------------------|----------------------------------------------------------|
| Configure the Timeouts of NAT                                   | <code>nat aging-time { tcp   udp   icmp } seconds</code> |
| Restore the default value of the Timeout of address translation | <code>nat aging-time default</code>                      |

By default, the Timeout for TCP address translation is 240 seconds and 40 seconds for UDP address translation.

The Timeout for ICMP address translation is 20 seconds.

**Display and Debug NAT** **Table 388** Display and debug NAT

| Operation                                           | Command                                                                                           |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Browse the condition of NAT                         | <code>display nat [ translations [ global <i>ip-address</i>   inside <i>ip-address</i> ] ]</code> |
| Clear up the mapping table of NAT                   | <code>nat reset</code>                                                                            |
| Enable the information debugging of NAT event       | <code>debugging nat event</code>                                                                  |
| Enable the information debugging of NAT data packet | <code>debugging nat packet</code>                                                                 |

**Typical NAT Configuration Example**

**An enterprise is connected to WAN by the address translation function of an internal server.**

**I. Networking Requirement**

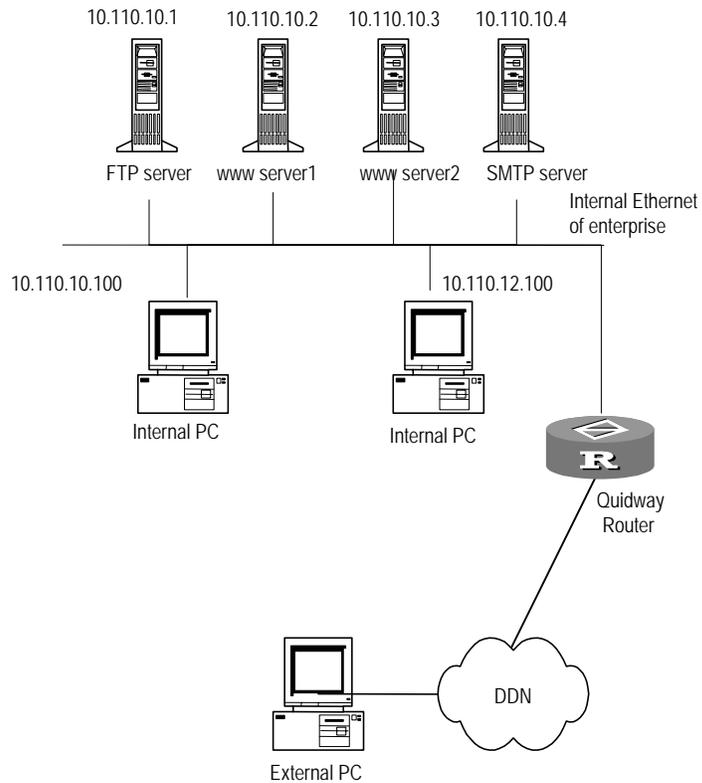
An enterprise is connected to WAN by the address translation function of the 3Com Router series. It is required that the enterprise can access the Internet via serial port 0 of the 3Com Router series, and provide WWW, FTP and SNMP services to the outside, as well as two WWW servers. The internal network address of the enterprise is 10.110.0.0/16.

There are three legal public network IP addresses of the enterprise from 202.38.160.101 to 202.38.160.103. The internal FTP server address is 10.110.10.1, using the public network address 202.38.160.101. The internal WWW server1 address is 10.110.10.2. The internal WWW server 2 address is 10.110.10.3, using the 8080 port for external communications, and the two WWW servers both use the public network address 202.38.160.102. The internal SNMP server address 10.110.10.4. It is expected to provide uniform server IP address to the outside, using the public network address 202.38.160.103.

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.

## II. Networking Diagram

Figure 132 NAT configuration case networking diagram 1



## III. Configuration Procedure

a Configure address pool and access list

```
[Router] nat address-group 202.38.160.101 202.38.160.105 pool 1
[Router] acl 1
[Router-acl-1] rule permit source 10.110.10.0 0.0.0.255
```

b Allow address translation of segment at 10.110.10.0/24

```
[Router-Serial0] nat outbound 1 address-group pool
```

c Set internal FTP server

```
[Router-Serial0] nat server global 202.38.160.101 inside 10.110.10.1
ftp tcp
```

d Set internal WWW server 1

```
[Router-Serial0] nat server global 202.38.160.102 inside 10.110.10.2
www tcp
```

e Set internal WWW server 2

```
[Router-Serial0] nat server global 202.38.160.102 8080 inside
10.110.10.3 www tcp
```

f Set internal SNMP server

```
[Router-Serial0] nat server global 202.38.160.103 inside 10.110.10.4
snmp udp
```

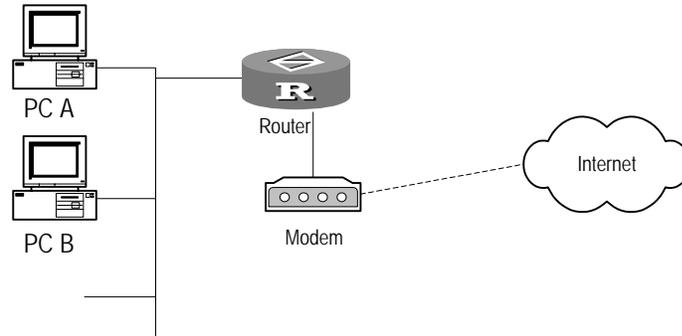
The internal LAN of an enterprise can dial-up to access Internet by the address translation.

### I. Networking Requirement

The internal LAN of an enterprise can dial-up to access Internet through serial port S0 by the address translation of the 3Com Router series.

### II. Networking Diagram

Figure 133 NAT configuration case networking diagram 2



### III. Configuration Procedure

- 1 Configure address access control list and dialer-list

```
[Router] acl 1
[Router-acl-1] rule permit source 10.110.10.0 0.0.0.255
[Router] dialer listen-rule 1 ip 10.110.10.0 255.255.255.0
```

- 2 Configure dial-up property for the interface

```
[Router-Serial0] physical-mode async
[Router-Serial0] link-protocol ppp
[Router-Serial0] ip address ppp-negotiate
[Router-Serial0] ppp pap local-user 169 password simple 169
[Router-Serial0] modem
[Router-Serial0] dialer enable-legacy
[Router-Serial0] dialer-group 1
[Router-Serial0] dialer number 169
```

- 3 Correlate the address translation list and the interface

```
[Router-Serial0] nat outbound 1 interface
```

- 4 Configure a default route to serial 0

```
[Router] ip route-static 0.0.0.0 0.0.0.0 serial 0
```

### Troubleshooting NAT Configuration

#### Fault 1: Address translation abnormal

Troubleshooting: Turn ON the debug switch for NAT, and refer to **debugging nat** in the **debugging** command for specific operation. According to the Debug information displayed on the router, initially locate the failure, and then use other commands to check further. Observe the source address after translation carefully, and make sure that it is the expected address. Otherwise, it is possible that the configuration of address pool is wrong. Meanwhile, make sure that there is routing to return to the address pool segment in the network to be accessed. Take into consideration the influence of firewall and address list of the address conversion itself on address conversion, and also route configuration.

**Fault 2: Internal server abnormal**

Troubleshooting: If an external host cannot access the internal server normally, check the configuration on the internal server host, or the internal server configuration on the router. It's 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 rule** for further check.



# 22

## CONFIGURING IP PERFORMANCE

This chapter contains information on the following topics:

- Configure IP Performance
- Configure TCP Performance
- Configure Fast Forwarding
- Display and Debug IP Performance
- Troubleshooting IP Performance Configuration

---

### Configure IP Performance

To configure IP performance, carry out the following steps:

#### 1 Configure MTU on an Interface

Perform the following configuration in interface view.

**Table 389** Configure maximum transmission unit on an interface

| Operation                                                          | Command                |
|--------------------------------------------------------------------|------------------------|
| Configure maximum transmission unit on an interface                | <b>mtu <i>size</i></b> |
| Restore default value of maximum transmission unit on an interface | <b>undo mtu</b>        |

When the Ethernet interface is encapsulated as Ethernet II, the interface mtu ranges from 46 to 1500 bytes, and default is 1500 bytes. When the Ethernet interface is encapsulated as SNAP, the interface mtu ranges from 46 to 1492 bytes, and 1492 bytes is default value. The serial port mtu ranges from 128 to 1500 bytes, and 1500 bytes is default value. The BRI port mtu value ranges from 128 to 1500 bytes, and 1500 bytes is default value.

#### 2 Configure Queue Length

Perform the following task in system view.

**Table 390** Configure queue length

| Operation                            | Command                                                                        |
|--------------------------------------|--------------------------------------------------------------------------------|
| Configure IP receiving queue length  | <b>ifquelen ip <i>queue-length</i></b>                                         |
| Configure IPX receiving queue length | <b>ifquelen ipx <i>queue-length</i></b>                                        |
| Configure ARP receiving queue length | <b>ifquelen arp <i>queue-length</i></b>                                        |
| Configure interface queue length     | <b>ifquelen interface <i>type number</i> <i>receive-queue queue-length</i></b> |

The range of the receiving queue length of all the protocols is 10~1000 bytes, and 75 bytes is the default value.

#### 3 Configure Router Forwarding Redirect Packets

The following configurations should be made in system view.

**Table 391** Configure router forwarding redirect packets

| Operation                                    | Command                        |
|----------------------------------------------|--------------------------------|
| Configure router forwarding redirect packets | <b>icmp redirect send</b>      |
| Disable router forwarding redirect packets   | <b>undo icmp redirect send</b> |

By default, router forwarding redirect packets is enabled.

#### 4 Configure Router Receiving/Forwarding Source Route Packets

The following configurations should be made in system view.

**Table 392** Configure router receiving/forwarding source address route packets

| Operation                                                          | Command                            |
|--------------------------------------------------------------------|------------------------------------|
| Configure router receiving/forwarding source address route packets | <b>ip option source-route</b>      |
| Disable router receiving/forwarding source address route packets   | <b>undo ip option source-route</b> |

By default, router receiving/forwarding source address route packets is disabled.

## Configure TCP Performance

To configure TCP performance, carry out the following steps:

### 1 Configure TCP Header Compression

When small messages are transmitted on low-rate physical lines (such as PSTN), the TCP header occupies an obviously larger portion in the messages. To raise transmission efficiency, TCP header compression can be configured on this interface. At present, TCP head compression can only be used on PPP links.

Perform the following task in interface view.

**Table 393** Enable/disable TCP header compression

| Operation                           | Command                        |
|-------------------------------------|--------------------------------|
| Enable TCP/IP VJ header compression | <b>ppp compression vj</b>      |
| Disable TCP header compression      | <b>undo ppp compression vj</b> |

TCP header compression is disabled in default status.

### 2 Configure TCP Timers

The following TCP timers can be configured:

- Synwait timer: When a syn message is sent, TCP starts the synwait timer. If no response message is received till synwait timeout, TCP connection will be terminated.
- Finwait timer: When the TCP connection status changes from FIN\_WAIT\_1 to FIN\_WAIT\_2, the finwait timer is started. If no FIN message is received till the finwait timer timeout, then TCP connection is terminated.
- Size of the receiving and sending window for the connection-oriented Socket.

Perform the following task in system view.

**Table 394** Configure TCP Timers

| Operation                                  | Command                              |
|--------------------------------------------|--------------------------------------|
| Configure synwait timer for TCP connection | <b>tcp timer syn-timeout seconds</b> |
| Configure FIN_WAIT_2 timer for TCP         | <b>tcp timer fin-timeout seconds</b> |

|                                                                        |
|------------------------------------------------------------------------|
| Configure the size of the receiving and sending window for TCP Socket. |
|------------------------------------------------------------------------|

|                        |
|------------------------|
| <b>tcp window size</b> |
|------------------------|

The Synwait timer's timeout ranges between 2~600 seconds, with a default value of 75 seconds. The Finwait timer's timeout ranges between 76~3600 seconds, with a default value of 675 seconds. The value of window-size ranges between 1~32Kbytes, with a default value of 4Kbytes.

## Configure 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 to forward the message, and creates MAC frame suitable for output of the message. The created MAC frame is 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 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 greatly simplifies the queuing of IP messages, 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 3Com Router supports Fast forwarding on various high-speed link interfaces, such as Ethernet, synchronous PPP, frame relay and HDLC.

Besides, the 3Com Router also supports Fast forwarding when firewall is configured.

Fast forwarding implemented via the 3Com Router contains the following features:

- Support fast forwarding on all types of high-speed link interfaces, including Ethernet, synchronous PPP, frame-relay and HDLC etc.
- Provide fast forwarding when the firewall is configured.
- Support load sharing and improve packets forwarding efficiency greatly.

The performance of Fast forwarding sometimes will be affected by some characteristics such as message queue management and message header compression. Fast forwarding is not conducted for fragmented messages.

Fast-forwarding Configuration includes:

- Enable/Disable fast-forwarding on an interface
  - Configure fast-forwarding table size
- 1 Enable/Disable fast-forwarding on an interface

You can disable fast-forwarding as needed. For example, if load sharing is required when forwarding packets, fast-forwarding should be disabled in the forwarding direction of the interface.

Perform the following configuration in interface view.

**Table 395** Enable/Disable fast-forwarding on an interface

| Operation                                                  | Command                            |
|------------------------------------------------------------|------------------------------------|
| Enable fast-forwarding in both directions of the interface | <b>ip fast-forwarding</b>          |
| Enable fast-forwarding on the inbound interface            | <b>ip fast-forwarding inbound</b>  |
| Enable fast-forwarding on the outbound interface           | <b>ip fast-forwarding outbound</b> |

|                                          |                                |
|------------------------------------------|--------------------------------|
| Disable fast-forwarding on the interface | <b>undo ip fast-forwarding</b> |
|------------------------------------------|--------------------------------|

By default, fast-forwarding is enabled in the input/output directions of the interface.

When fast-forwarding is carried out on an interface, note that:

- You can disable fast-forwarding as necessary. For example, if load sharing is required, fast-forwarding must be disabled in the forwarding direction of the interface.
- If fast-forwarding has been configured on an interface, the interface will not send any ICMP redirected packets.

## 2 Configure fast-forwarding table size

**Table 396** Perform the following configuration in system view

| Operation                                      | Command                                                            |
|------------------------------------------------|--------------------------------------------------------------------|
| Configure a fast-forwarding table size         | <b>ip fast-forwarding cache-size { 4k   16k   64k   256k   1m}</b> |
| Restore the default fast-forwarding table size | <b>undo ip fast-forwarding cache-size</b>                          |

The fast-forwarding table size on a router defaults to 4K, that is, up to 4K entries are allowed in the table.



*Fast-forwarding table size depends on the memory capacity. The larger the memory capacity is, the larger the configurable fast-forwarding table size will be.*

## Display and Debug Fast Forwarding

**Table 397** Display and Debug fast forwarding

| Operation                                           | Command                                        |
|-----------------------------------------------------|------------------------------------------------|
| Display IP fast-forwarding cache                    | <b>display ip fast-forwarding cache</b>        |
| Display IP fast-forwarding flow-control Information | <b>display ip fast-forwarding flow-control</b> |
| Clear contents in the fast forwarding cache         | <b>reset ip fast-forwarding cache</b>          |

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.

## Display and Debug IP Performance

**Table 398** Display and Debug IP address

| Operation                                       | Command                                     |
|-------------------------------------------------|---------------------------------------------|
| Display TCP connection status                   | <b>display tcp status</b>                   |
| Display interface table information             | <b>display ip interface [ type number ]</b> |
| Display IP traffic and statistical information. | <b>display ip statistics</b>                |
| Turn on IP debugging information                | <b>debugging ip packet</b>                  |
| Turn on TCP debugging information               | <b>debugging tcp packet</b>                 |
| Turn on TCP cession debugging information       | <b>debugging tcp [ event   packet ]</b>     |
| Turn on UDP debugging information               | <b>debugging udp packet</b>                 |
| Clear IP statistical information.               | <b>reset ip counters</b>                    |

## Troubleshooting IP Performance Configuration

### Fault 1: TCP and UDP are created upon IP protocol, and IP is able to provide data packet transmission. However, TCP and UDP protocols do not work normally

Troubleshooting: Turn on corresponding debugging switches to check the debugging information

- Use the **debugging udp** command to turn on the UDP debugging switch, and trace the UDP data packet. When the router sends or receives UDP data packets, the packet content format can be displayed in real time, so problems can be located.

The UDP data packet format is as follows:

```
UDP output packet:
Source IP address: 202.38.160.1
Source port: 1024
Destination IP Address 202.38.160.1
Destination port: 4296
```

- Use the **debugging tcp** command to turn on the TCP debugging switch, and trace the TCP data packet. TCP has two data packet format options: one is to debug and trace the receiving/sending of TCP packets in all TCP connections with this equipment as one end. The specific operation is as follows:

```
[Router] info-center enable
[Router] debugging tcp packet
```

The TCP packets received or sent can be checked in real time, and the specific format is as follows:

```
TCP output packet:
Source IP address: 202.38.160.1
Source port: 1024
Destination IP Address 202.38.160.1
Destination port: 4296
Sequence number: 4185089
Ack number: 0
Flag: SYN
Packet length: 60
Data offset: 10
```

Another data packet format is to debug and trace packets with SYN, FIN or RST setting.

```
[Router] info-center enable
[Router] debugging tcp event
```

The TCP packets received or sent can be checked in real time, with the same packet format as above.

# 23

## CONFIGURING IP COUNT

This chapter contains information on the following topics:

- IP Count Introduction
- IP Count Configuration
- Display and Debug IP Count
- Typical Configuration Example
- Troubleshooting

---

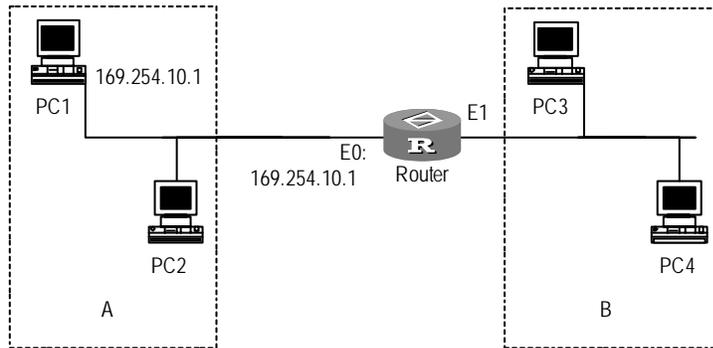
### IP Count Introduction

IP Count makes the statistics about the input and output packets, and the packets denied by the firewall as well. When making the statistics, the router classifies the bidirectional (in and out) IP packets by testing whether they match any IP Count lists and whether they are denied by the firewall. At the same time of making data statistics, the total numbers of packets and bytes are recorded.

As shown in the following figure, if IP Count has been enabled on the output interface Ethernet1, the statistics will be made on the flows transmitted from this interface to the network B. A flow destined for the B network can be identified by an IP triplet (source address, destination address and protocol). Through the statistics that has been made, you can know the outgoing traffic size. If a firewall for filtering outgoing packets has been configured on the interface, IP Count will record the addresses from which the packets are denied by the firewall, and make the statistics on the denied packets and bytes.

Likewise, if IP Count is enabled on the incoming interface Ethenet0, the statistics will be made on the flows from the A network to the router. If a firewall for filtering the incoming packets has been enabled on the interface, the IP Count module can make statistics on the packets denied by the firewall.

**Figure 134** Networking for an IP Count application



IP Count mainly implements the following functions:

- Configure IP Count list
- Make statistics on the output and input packets
- Make statistics on the packets processed by the firewall
- Display all packet statistics
- Clear all packet statistics

## IP Count Configuration

Basic Configuration includes:

- Enable IP Count Service
- Enable IP Count on an interface

Advanced Configuration includes:

- Configure IP Count list
- Configure upper threshold for accounting entries in Interior-List
- Configure upper threshold for accounting entries in Exterior-List
- Configure timeout time of IP Count statistics list entries

### 1 Enable IP Count Service

This command can be used to enable or disable IP Count service. You can configure IP Count to make statistics on the packets that the router has input or output depending on the specific requirements on the router.

Perform the following configuration in system view.

**Table 399** Enable/Disable IP Count service

| Operation        | Command                           |
|------------------|-----------------------------------|
| Enable IP Count  | <code>ip count enable</code>      |
| Disable IP Count | <code>undo ip count enable</code> |

By default, IP Count is not enabled.

### 2 Configure IP Count on an Interface

Configuring IP Count on an interface can enable packet accounting on the interface. You can configure to make statistics on the packets input or output on the interface, as well as packets denied by firewall.

Perform the following configuration in interface view.

**Table 400** Configure IP Count on an interface

| Operation                                                                                          | Command                                                                     |
|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Set IP Count to make statistics on the input packets on the current interface                      | <b>ip count inbound-packets</b>                                             |
| Disable IP Count to make statistics on the input packets on the current interface                  | <b>undo ip count inbound-packets</b>                                        |
| Set IP Count to make statistics on the output packets on the current interface                     | <b>ip count outbound-packets</b>                                            |
| Disable IP Count to make statistics on the output packets on the current interface                 | <b>undo ip count outbound-packets</b>                                       |
| Set IP Count to make statistics on the packets denied by the firewall on the current interface     | <b>ip count firewall-denied [ inbound-packets   outbound-packets ]</b>      |
| Disable IP Count to make statistics on the packets denied by the firewall on the current interface | <b>undo ip count firewall-denied [ inbound-packets   outbound-packets ]</b> |

By default, IP Count is not enabled on interfaces.

### 3 Configure IP Count List

IP Count list is configured for the purpose of classifying the statistics made by IP Count. That is, if IP Count lists have been configured, IP Count service will determine whether an input or output packet matches any IP Count list before making statistics on it. If a match has found, the statistics about the packet will be retained in Interior-List. If not, it will be kept in Exterior-List.

Perform the following configuration in system view.

**Table 401** Configure IP Count list

| Operation                  | Command                                        |
|----------------------------|------------------------------------------------|
| Configure an IP Count list | <b>ip count table ip-address mask</b>          |
| Delete the IP Count list   | <b>undo ip count table [ ip-address mask ]</b> |

By default, IP Count statistics rules are not configured.

### 4 Configure Upper Threshold of Exterior-List Accounting Entries

The following command is used for specifying count maximum of exterior, that is, the max entries number of the packets incompliant with the IP Count lists.

Perform the following configuration in system view.

**Table 402** Specify count maximum of exterior

| Operation                                     | Command                                   |
|-----------------------------------------------|-------------------------------------------|
| Specify count maximum of exterior             | <b>ip count exterior-threshold number</b> |
| Restore the default count maximum of exterior | <b>undo ip count exterior-threshold</b>   |

The default max entries number of exterior is set to 0, namely, the packets that do not match the rules will not be counted.

#### 5 Configure Upper Threshold of Interior-List Accounting Entries

The following command is used for specifying count maximum of interior, that is, the max entries number of the packets compliant with the IP Count lists.

Perform the following configuration in system view.

**Table 403** Specify count maximum of interior

| Operation                                     | Command                                         |
|-----------------------------------------------|-------------------------------------------------|
| Specify count maximum of interior             | <code>ip count interior-threshold number</code> |
| Restore the default count maximum of interior | <code>undo ip count interior-threshold</code>   |

By default, the upper threshold of Interior-List entries is 512.

#### 6 Configure Timeout of IP Count Entries

The following command is used for configuring timeout time for IP Count entries. If no new packets are received within the timeout time, IP Count will assume that the accounting entries have timed out and the accounting entries will be deleted from the list.

Perform the following configuration in system view.

**Table 404** Configure the period that an IP Count entry exists before it times out

| Operation                                            | Command                               |
|------------------------------------------------------|---------------------------------------|
| Configure the timeout time of IP Count entries       | <code>ip count timeout minutes</code> |
| Restore the default timeout time of IP Count entries | <code>undo ip count timeout</code>    |

By default, IP Count entries time out after 720 minutes.

## Display and Debug IP Count

**Table 405** Display and debug IP Count

| Operation                               | Command                                                                                                        |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Clear statistics of IP Count            | <code>reset ip count</code>                                                                                    |
| Display IP Count lists                  | <code>display ip count table</code>                                                                            |
| Display statistics of IP Count          | <code>display ip count { inbound-packets   outbound-packets } { exterior   interior   firewall-denied }</code> |
| Enable IP Count debugging at all levels | <code>debugging ip count [ data   error ]</code>                                                               |

## Typical Configuration Example

### I. Networking Requirements

As shown in Figure 4-1, the router is connected to PC1 and PC2 via the interface Ethernet0, and to PC3 and PC4 via Ethernet1. The router is required to make statistics on the packets that the router transmitted to and received from PC1. PC1 is assigned with the address 169.254.10.1 and the mask 255.255.0.0.

## II. Networking Diagram

See Figure 4-1 Networking for IP Count application for reference.

## III. Configuration Procedure

### 1 Configure the router

#### a Enable IP Count service

```
[Router] ip count enable
```

#### b Specify count maximum of exterior-list to 10

```
[Router] ip count exterior-threshold 10
```

#### c Specify count maximum of interior-list to 10

```
[Router] ip count interior-threshold 10
```

#### d Configure an IP Count list

```
[Router] ip count table 169.254.10.1 255.255.0.0
```

#### e Enter the interface view of the interface Ethernet 0 and assign it with the address 169.254.10.2.

```
[Router] interface ethernet 0
```

```
[Router-Ethernet0] ip address 169.254.10.2 255.255.0.0
```

#### f Configure IP Count to make statistics on the packets input and output on the interface.

```
[Router-Ethernet0] ip count inbound-packets
```

```
[Router-Ethernet0] ip count outbound-packets
```

## IV. Test Procedure

### 1 Ping the router on PC1.

```
ping -n 5 169.254.10.2
```

### 2 Execute the **display** command of IP Count to view the IP Count statistics.

```
[Router] display ip count inbound-packets interior
```

```
Input packets in Interior-list
```

| Src          | Dst          | Packets | Bytes | Protocol |
|--------------|--------------|---------|-------|----------|
| 169.254.10.1 | 169.254.10.2 | 5       | 420   | ICMP     |

```
[Router] display ip count outbound-packets interior
```

```
Output packets in Interior-list
```

| Src          | Dst          | Packets | Bytes | Protocol |
|--------------|--------------|---------|-------|----------|
| 169.254.10.2 | 169.254.10.1 | 5       | 420   | ICMP     |

## Troubleshooting

### Fault 1: Executing the **display ip count** command but no packet information is displayed.

Troubleshooting:

- 1 First, analyze the information that is output by executing the **display ip count** command. The prompt "\*\*\*\*\* Disable" means that the statistics has not been made yet on the data information requiring display. In other words, IP Count has not been configured on the interface of the router.
- 2 IP Count has been configured on the interface. Execute the **display ip count** command, but still, no packet information is displayed. This time, the prompt "Src Dst Packets Bytes Protocol" appears, which means that IP Count has not been enabled. Use the **ip count enable** command to enable IP Count service.



# 24

## CONFIGURING IPX

This chapter contains information on the following topics:

- IPX Protocol Overview
- Configure IPX

---

### IPX Protocol Overview

Novell IPX protocol is a connectionless protocol. Though both data and destination IPX address are included in IPX packet, the protocol cannot confirm whether a packet has been forwarded successfully. Such functions are provided by the protocol at the layer above IPX. In IPX, any IPX packet is considered as an independent entity, not related to any other IPX packets logically or sequentially.

In network model, IPX protocol is in network layer and is the only path for information transmission between the upper-layer protocol and the lower-layer protocol. IPX protocol functions to fill in addresses, route and forward information packets. For packets generated at the upper-layer, IPX forwards them out directly. For user data packets, IPX will first find the correct path in RIP route information table, and then forward them out.

#### IPX address

IPX address consists of network and node, represented as network.node. Network number is the unique identifier of the physical network, which is 4-byte long and is expressed by eight hexadecimal digits. The preamble 0 can be omitted and not input.

Node value is, of 6 bytes long, the unique identifier of one node. Every two bytes are followed by ".", and then the node value is divided into three groups. Each group is represented with four hexadecimal numbers with the preamble 0 omitted.

The following is an example of IPX address:

```
bc.0.0cb.47
```

Here, the network ID is bc (more specifically, it is 000000bc), the node value is 0.0cb.47 (more specifically, it is 0000.00cb.0047). All digits are hexadecimal. In the command help, IPX address is expressed in the form of N.H.H.H.

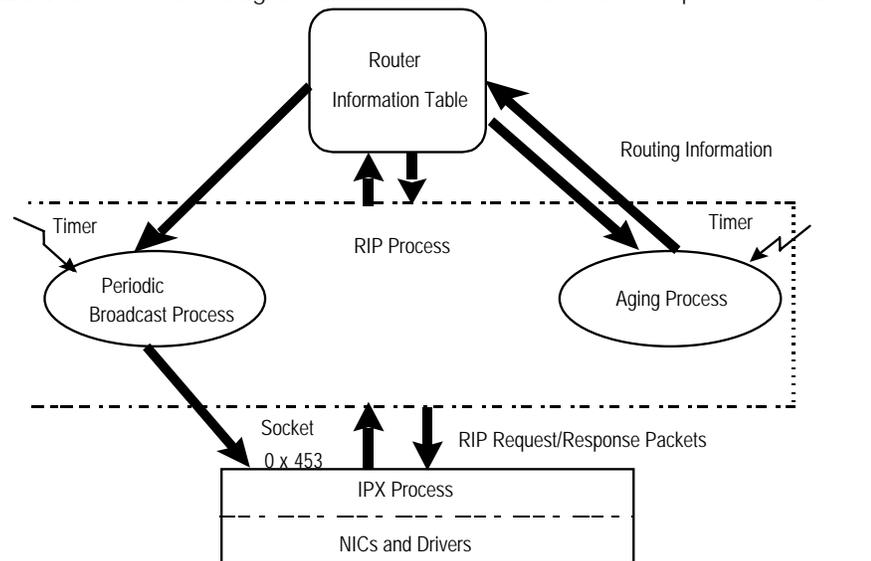
#### RIP

A router mainly functions to forward packets between networks. When a client sends a packet between networks, instead of knowing what path the packet should pass to reach the destination, it only knows to transmit the packet to the nearest router and forward it via the next router. So a router must provide the

network routing information which can be sent to destination or needs to be forwarded, so that when a packet is received, the next router can be found to transmit the packet. The routing information here can be configured both statically and dynamically. In a router, collection and maintenance of dynamic routing information are realized by RIP.

RIP is an abbreviation for Routing Information Protocol. A router creates and maintains an inter-network routing information database (usually called router information table) through RIP. When the router starts, RIP begins exchange of routing information with external RIPs enabled hosts constantly. When creating a new path, RIP adds its routing information into the router information table, and when finding a faulty path, RIP deletes its routing information from the router information table. It can be seen that the router information table reacts flexibly to inter-network error and congestion. In case of error and congestion, the router information table can be modified dynamically to change the path. The following diagram describes the relation between main components of RIP.

**Figure 135** Schematic diagram of the relation between main components of RIP



### SAP

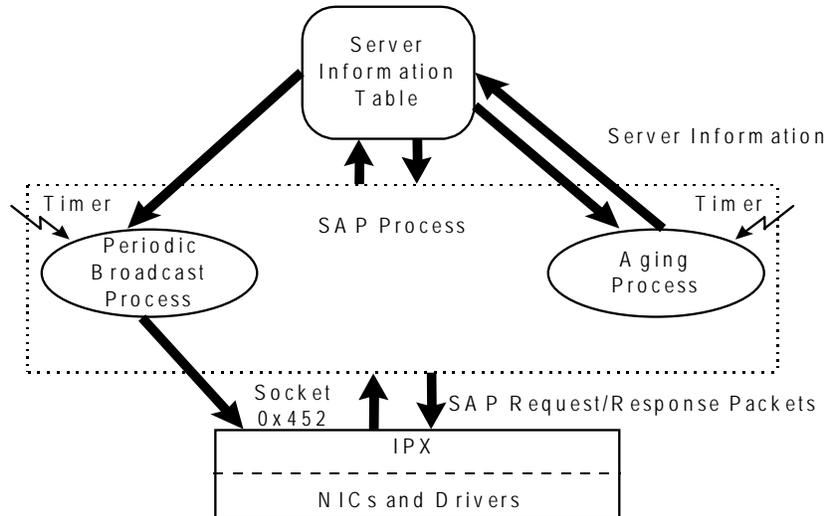
SAP is an abbreviation for Service Advertising Protocol. SAP allows providing various service nodes, such as file server, print server, NetWare access server and remote control console server, and broadcasting their service types and addresses. When servers start, they broadcast their services through SAP, and when servers are shut down, they indicate the termination of services through SAP.

Through SAP, a router creates and maintains an inter-network service information database, usually called service information table. It tells what services are provided by the network, and what inter-network addresses these servers have. This is an important function, for a workstation cannot establish session with file servers if it does not know their addresses.

A server that provides services will periodically broadcast its services and address to the adjacent sites. Clients cannot use such information directly, it is collected by SAP agents in different routers on the network, and saved in their server information tables. Since server information is often dynamically updated by SAP,

clients can always obtain the latest server addresses. The following diagram describes the relation between main components of SAP.

**Figure 136** Schematic diagram of the relation between main components of SAP



## Configure IPX

IPX configuration includes:

- Activate/deactivate IPX
- Enable IPX interface
- Adjust Novell IPX delay value
- Configure relative parameters of IPX RIP
- Configure relative parameters of IPX SAP
- Modify length of service information reserve queue
- Use trigger refresh
- Deactivate horizontal division
- Configure IPX packet management
- Modify encapsulation format of IPX frame
- Configure IPX on WAN

### 1 Activate/Deactivate IPX

Perform the following task in system view.

**Table 406** Activate/deactivate IPX

| Operation      | Command                               |
|----------------|---------------------------------------|
| Activate IPX   | <code>ipx enable [ node node ]</code> |
| Deactivate IPX | <code>undo ipx enable</code>          |

If the node of a router is not specified, then the router will use the MAC address of its first Ethernet interface as its node address.

### 2 Enable IPX Interface

After activating the IPX function of a router, each independent interface must be assigned with a network ID so that IPX can run on the interface.

Perform the following task in interface view.

**Table 407** Enable IPX interface

| Operation            | Command                          |
|----------------------|----------------------------------|
| Enable IPX interface | <code>ipx network network</code> |
| Delete IPX interface | <code>undo ipx network</code>    |

By default, IPX is disabled on all interfaces after being started.

Delete interface IPX, then IPX configuration is removed from the interface, static service information and static routing information will be deleted.

### 3 Configure Relative Parameters of IPX RIP

#### a Configure IPX static route

RIP is used by IPX to decide the best path. Though a routing protocol can refresh a routing table dynamically, you may want to add a static route to routing table manually, and clearly specify how to arrive at a destination. Thus, the priority of IPX routes is adopted in the 3Com Router series, there is, the default priority of static routes is 10 and that of dynamic routes is 60. Smaller value indicates higher priority of the route. When selecting routes, among all routes to the same destination, a router selects the one of highest priority.

Note that once you have created a static route, if one section of the route is faulty, communication will be interrupted and the message will be sent to a destination that does not exist.

Perform the following task in system view.

**Table 408** Configure IPX RIP static route

| Operation                  | Command                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------|
| Configure IPX static route | <code>ipx route network.node tick ticks hop hops [ preference value]</code>                        |
| Remove IPX static route    | <code>undo ipx route { network [ network.node   float   static   preference value ]   all }</code> |

By default, there is no static route.

The default priority of IPX static route is 10 and that of IPX dynamic route is 60. Smaller value indicates higher priority of the route. For default route, the value of *network.node* should be FFFFFFFE.

After configuring a default route, enable/disable it according to actual conditions.

**Table 409** Enable/Disable a Default Route

| Operation               | Command                             |
|-------------------------|-------------------------------------|
| Enable a default route  | <code>ipx default-route</code>      |
| Disable a default route | <code>undo ipx default-route</code> |

By default, enable a default route, i.e. all packets which cannot find their routing can be forwarded via this route.

#### b Configure updating interval of IPX RIP

You can set the interval for RIP to update IPX module. The router will send RIP updated broadcast message at intervals.

Perform the following task in system view.

**Table 410** Configure RIP updating period

| Operation                                    | Command                                    |
|----------------------------------------------|--------------------------------------------|
| Configure RIP updating period                | <b>ipx rip timer update <i>seconds</i></b> |
| Restore default value of RIP updating period | <b>undo ipx rip timer update</b>           |

By default, the time interval for RIP updating period is adjusted to be 60 seconds.

**c** Configure aging period of IPX RIP

Perform the following task in system view.

**Table 411** Configure RIP aging period

| Operation                                 | Command                                     |
|-------------------------------------------|---------------------------------------------|
| Adjust RIP aging period                   | <b>ipx rip multiplier <i>multiplier</i></b> |
| Restore default value of RIP aging period | <b>undo ipx rip multiplier</b>              |

By default, the aging period of a routing table item is 3 times that of RIP updating period. In other words, if a routing table item is not updated after 3 RIP updating periods, it will be deleted from the table, so will the corresponding dynamic service information table item be deleted from the server information table.

**d** Configure the maximum size of RIP update packet

Perform the following task in interface view.

**Table 412** Configure the maximum size of RIP update packet

| Operation                                        | Command                         |
|--------------------------------------------------|---------------------------------|
| Configure the maximum size of RIP update packet  | <b>ipx rip mtu <i>bytes</i></b> |
| Restore default value of RIP updated packet size | <b>undo ipx rip mtu</b>         |

By default, the maximum size of the RIP update packet is 432 bytes.

**e** Configure the maximum number of IPX parallel route

Usually, there is more than one best route to the same destination, which are called parallel routes. When the number of parallel route (N) configured exceeds 1, the system will implement load-sharing function automatically. Reuse multiple paths to send data.

Configuring parallel routes can decrease the possibility of congestion, but occupy relatively large memory. Parallel routes are not recommended when the memory is not abundant, however, to configure parallel routes can reduce the probability of blockage.

Perform the following task in system view.

**Table 413** Configure the maximum number of IPX parallel route

| Operation                                                   | Command                                        |
|-------------------------------------------------------------|------------------------------------------------|
| Configure the maximum number of IPX parallel route          | <b>ipx rip load-balance-path <i>number</i></b> |
| Restore the maximum number of IPX parallel route to default | <b>undo ipx rip load-balance-path</b>          |

By default, there is one parallel route to a destination.

**f** Configure length of route reserve queue

When the length of a route reserve queue is 1, the system only saves one route for a destination. If this unique route is faulty, it will be deleted by the system and there will be no route to the destination while searching for the substitute routes, resulting in huge loss of packets. When the length of a route reserve queue exceeds 1, if one route is deleted, it will be replaced with another one as soon as possible, so as to prevent huge loss of packets. However, increasing the length of the route reserve queue in turn increases the system memory that will be occupied by IPX module.

Perform the following task in system view.

**Table 414** Configure length of route reserve queue

| Operation                                                | Command                                 |
|----------------------------------------------------------|-----------------------------------------|
| Configure length of route reserving queue                | <b>ipx rip max-reserve-paths length</b> |
| Restore default value of length of route reserving queue | <b>undo ipx rip max-reserve-paths</b>   |

By default, the length of a route reserve queue is 4.

#### 4 Configure Relative Parameters of IPX SAP

##### a Configure IPX static service information table item

Generally, only the service notified by NetWare server and saved by the router can be used. In special cases, special services can be specified to use, so that the client can always use this special service. Similar to IPX routes, IPX service information priority is adopted, and smaller value means higher priority of service information. If the route related to the static service information is invalid or deleted, the static service information will be prevented from broadcasting, until the router finds a new valid route related to the service information.

Perform the following task in system view.

**Table 415** Configure static service information table item

| Operation                             | Command                                                                                           |
|---------------------------------------|---------------------------------------------------------------------------------------------------|
| Add one static service information    | <b>ipx service service-type name network.node socket hop hopcount [ preference preference ]</b>   |
| Delete one static service information | <b>undo ipx service { service-type [ name [ network.node ] ] [ preference preference] }   all</b> |

By default, the priority of static service information is 10, and that of dynamic service information is 60.

##### b Configure updating period of IPX SAP

In a huge network, one IPX SAP broadcast occupies much of the bandwidth. For interfaces running protocols such as PPP, X.25 and frame relay, the bandwidth is limited, therefore changing IPX SAP updating period is an effective method to reduce bandwidth occupation. You should make sure that all servers and routers on the network have the same SAP updating period, otherwise, the router might think that a server fails to work, while the server is still working.

Perform the following task in system view.

**Table 416** Configure IPX SAP updating period

| Operation                                    | Command                                    |
|----------------------------------------------|--------------------------------------------|
| Configure SAP updating period                | <b>ipx sap timer update <i>seconds</i></b> |
| Restore default value of SAP updating period | <b>undo ipx sap timer update</b>           |

By default, the updating period of IPX SAP is 1 tick (i.e. 1/18 seconds).

**c** Configure SAP aging period

Perform the following task in system view.

**Table 417** Configure SAP aging period

| Operation                                 | Command                                     |
|-------------------------------------------|---------------------------------------------|
| Configure SAP aging period                | <b>ipx sap multiplier <i>multiplier</i></b> |
| Restore default value of SAP aging period | <b>undo ipx sap multiplier</b>              |

By default, the service information which is not updated in three update periods will be deleted.

If a service information table item is not updated after 3 updating periods, it will be deleted from the server information table.

**d** Configure size of SAP updating message

Perform the following task in interface view.

**Table 418** Configure size of SAP maximum updated message

| Operation                                                    | Command                         |
|--------------------------------------------------------------|---------------------------------|
| Configure size of SAP maximum updated message                | <b>ipx sap mtu <i>bytes</i></b> |
| Restore default value of size of SAP maximum updated message | <b>undo ipx sap mtu</b>         |

By default, the Max. length of the service update packet is 480 bytes.

**e** Configure reply to SAP GNS request

You can set the processing mode of SAP GNS request by router:

- whether to reply with the nearest service information or by polling all service information known by the router
- whether to reply to SAP GNS request or not

Usually, a router will reply to GNS request with the service information of the nearest server. There may also be exceptions: if the nearest server is local server, then the router will not reply to the GNS request from this network segment.

Please configure **ipx sap gns-round-robin** command in system view, and configure **ipx sap gns-disable-reply** command in interface view.

**Table 419** Configure reply to SAP GNS request

| Operation                                              | Command                          |
|--------------------------------------------------------|----------------------------------|
| Configure Process GNS request in Round Robin algorithm | <b>ipx sap gns-load-balance</b>  |
| Disable replying to GNS request                        | <b>ipx sap gns-disable-reply</b> |

By default, a router replies to GNS request with the service information of the nearest server.

**f** Configure length of service information reserve queue

If the length of a service information reserve queue is 1, the system saves only one service information. If the server to which the only service information corresponds is faulty, system will delete this information, and you cannot find any server to provide such service while searching for the substitute service information. When the length of a service information reserve queue exceeds 1, if one service information is deleted, it will be replaced with the next service information as soon as possible, so that you will have no trouble finding server. However, increasing the length of the service information reserve queue means in turn increases the system memory that will be occupied by IPX module.

**Table 420** Configure length of service information reserve queue

| Operation                                                            | Command                                  |
|----------------------------------------------------------------------|------------------------------------------|
| Configure length of service information reserving queue              | <b>ipx sap max-reserve-server length</b> |
| Restore default value of length of service information reserve queue | <b>undo ipx sap max-reserve-server</b>   |

### 5 Configure Using Touch-Off for an Interface

RIP and SAP of IPX send updating broadcast packets periodically. If you do not want routers to send broadcast packets all the time, touch-off can be used on an interface, so that updating messages will be sent only when the route or the service information changes.

Perform the following task in interface view.

**Table 421** Configure Using touch-off for an interface

| Operation                                     | Command                            |
|-----------------------------------------------|------------------------------------|
| Configure Using touch-off for an interface    | <b>ipx update-change-only</b>      |
| Configure Disabling touch-off on an interface | <b>undo ipx update-change-only</b> |

By default, touch-off is disabled on the interface.

### 6 Disable Split-Horizon

Split-horizon algorithm can avoid generating route loop. Split-horizon means that routes received from a specific interface are not to be sent from this interface. In special circumstances, split-horizon shall be disabled, sacrificing efficiency to achieve correct transmission of routes. It is recommended not to disable the RIP split-horizon unless necessary. Disabling split-horizon has no effect on point-to-point links.

Perform the following task in interface view.

**Table 422** Disable split-horizon

| Operation             | Command                       |
|-----------------------|-------------------------------|
| Disable split-horizon | <b>undo ipx split-horizon</b> |
| Enable split-horizon  | <b>ipx split-horizon</b>      |

By default, split-horizon is enabled on the interface.

### 7 Configure the Delay of Interface Sending IPX Packets

The delay indicates the speed at which an interface forwards IPX messages: long delay means slow forwarding, and short delay means Fast forwarding. In this way, the delay is important for the system to decide the best routing. You can adjust the value of delay for the interface to send IPX messages.

Perform the following task in interface view.

**Table 423** Configure the delay of interface sending IPX packets

| Operation                                            | Command                      |
|------------------------------------------------------|------------------------------|
| Configure the Delay of Interface Sending IPX Packets | <b>ipx tick <i>ticks</i></b> |
| Restore default value of interface delay             | <b>undo ipx tick</b>         |

By default, the delay of Ethernet interface is 1 tick, For asynchronous serial port is 30 ticks and that for WAN port is 6 ticks. The range of *ticks* is: 0~30000.

## 8 Configure Management of IPX Packet

By default, the router usually discards the broadcast packet of type 20, but you can also enable such packet to be sent to other network segments by configuring routers.

Perform the following task in interface view.

**Table 424** Configure management of IPX packet

| Operation                                          | Command                             |
|----------------------------------------------------|-------------------------------------|
| Enable propagation of broadcast packet of type 20  | <b>ipx netbios-propagation</b>      |
| Disable propagation of broadcast packet of type 20 | <b>undo ipx netbios-propagation</b> |

## 9 Modify Encapsulation Format of IPX Frame on Interface

**Table 425** Encapsulation format of IPX frame

| Interface type     | Encapsulation format supported                 |
|--------------------|------------------------------------------------|
| Ethernet interface | Ethernet_SNAP<br>Ethernet_II<br>802.3<br>802.2 |
| WAN interface      | PPP<br>FR<br>X.25                              |

Perform the following task in interface view.

**Table 426** Modify encapsulation format of IPX frame on interface

| Operation                                                                  | Command                                                      |
|----------------------------------------------------------------------------|--------------------------------------------------------------|
| Modify encapsulation format of IPX frame on an interface                   | <b>ipx encapsulation [ dot3   dot2   ethernet-2   snap ]</b> |
| Restore default value of encapsulation format of IPX frame on an interface | <b>undo ipx encapsulation</b>                                |

By default, the encapsulation format of IPX frame on Ethernet interface is Ethernet 802.3, and that on WAN interface is PPP.

## 10 Configure IPX on WAN

In the 3Com Router series, commands such as **dialer route**, **fr map** and **x25 map**, can be used to configure mapping from IPX address to link layer address, so as to run IPX on WAN. For detailed configurations, refer to relative chapters in *Link Layer Protocol*.

**Display and Debug IPX** Table 427 Display and Debug IPX

| Operation                                                     | Command                                                                                                                                                                           |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display interface status and interface parameters of IPX      | <b>display ipx interface</b> [ <i>type number</i> ]                                                                                                                               |
| Display IPX routing information table                         | <b>display ipx routing-table</b> [ <i>network</i>   <i>static</i>   <i>default</i> ] [ <i>verbose</i> ]                                                                           |
| Display IPX server information table                          | <b>display ipx service-table</b> [ <i>type service-type</i>   <i>name name</i>   <i>network network</i>   <i>socket socket</i>   <i>order { net   type }</i> ] [ <i>verbose</i> ] |
| Display type and quantity of packets received and transmitted | <b>display ipx statistics</b>                                                                                                                                                     |
| Clear IPX statistical information.                            | <b>reset ipx statistics</b>                                                                                                                                                       |

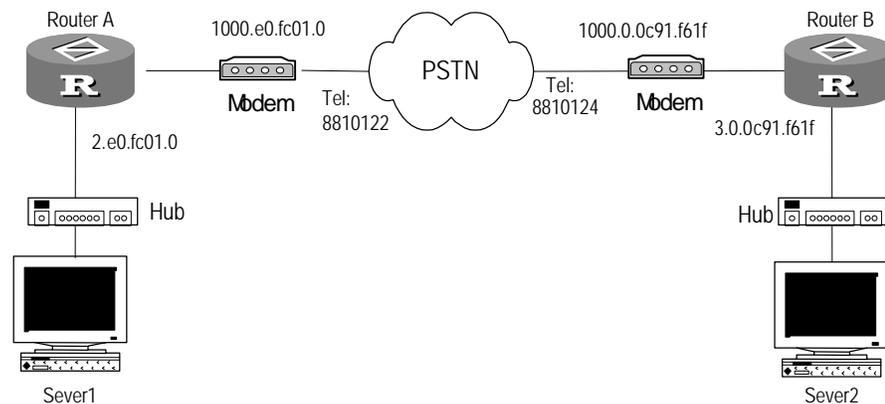
### Typical IPX Configuration Example

#### I. Networking Requirement

Networking with Router A and Router B. Here, both Server1 and Server2 are installed with NetWare 4.1. Server1 is the master server, its external network ID is 2, packet encapsulation format Arpa, and internal network ID 937f. Server2 is the slave server, its network ID is 3, packet encapsulation format is Snap, and internal network ID is 9300. The node of Ethernet interface of Router A is 00e0.fc01.0000, and its telephone number is 8810122. The node of Ethernet interface of Router B is 0.0c91.f61f, and its telephone number is 8810124.

#### II. Networking Diagram

Figure 137 Networking diagram of IPX configuration example



#### III. Configuration Procedure

##### 1 Configure Router A:

###### a Activate IPX

```
[Router] ipx enable
```

###### b Activate IPX module on interface Ethernet0, the network ID being 2

```
[Router] interface ethernet 0
[Router-Ethernet0] ipx network 2
```

###### c Set encapsulation format of packets on Ethernet interface to Ethernet\_II.

```
[Router-Ethernet0] ipx encapsulation ethernet-2
[Router-Ethernet0] exit
```

- d Activate IPX module on interface Serial0, the network ID being 1000.  
Configuring BDR parameter

```
[Router] interface serial 0
[Router-Serial0] dialer enable-legacy
[Router-Serial0] dialer-group 1
[Router-Serial0] ipx network 1000
```

- e Configure an address map to Router B

```
[Router-Serial0] dialer route ipx 1000.0.0c91.f61f 8810124
[Router-Serial0] quit
```

- f Configure a static route to network ID 3

```
[Router] ipx route 3 1000.0.0c91.f61f tick 10 hop 2
```

- g Configure a static route to network ID 9300

```
[Router] ipx route 9300 1000.0.0c91.f61f tick 10 hop 2
```

- h Configure an information about Server2 file service

```
[Router] ipx service 4 server2 9300.0000.0000.0001 451 hop 2
```

- i Configure an information about Server2 directory service

```
[Router] ipx service 26B tree 9300.0000.0000.0001 5 hop 2
```

- j Configure dialing rules

```
[Router] dialer-rule 1 ipx permit
```

## 2 Configure Router B:

- a Activate IPX module

```
[Router] ipx enable
```

- b Activate IPX function on interface Ethernet0, the network ID being 3

```
[Router] interface ethernet 0
[Router-Ethernet0] ipx network 3
```

- c Set encapsulation format of packets on Ethernet interface to Ethernet\_SNAP

```
[Router-Ethernet0] ipx encapsulation snap
[Router-Ethernet0] quit
```

- d Activate IPX module on interface Serial0, the network ID being 1000.  
Configuring BDR parameter

```
[Router] interface serial 0
[Router-Serial0] dialer-group 1
[Router-Serial0] ipx network 1000
```

- e Configure an address map to Router A:

```
[Router-Serial0] dialer route ipx 1000.00e0.fc01.0000 8810122
[Router-Serial0] quit
```

- f Configure a static route to network ID 2

```
[Router] ipx route 2 1000.00e0.fc01.0000 tick 10 hop 2
```

- g Configure a static route to network ID 9300

```
[Router] ipx route 937f 1000.00e0.fc01.0000 tick 10 hop 2
```

- h Configure an information about Server1 file service

```
[Router] ipx service 4 server1 937f.0000.0000.0001 451 hop 2
```

i Configure an information about Server1 directory service

```
[Router] ipx service 26B tree 937f.0000.0000.0001 5 hop 2
```

```
[Router] ipx service 278 tree 937f.0000.0000.0001 4006 hop 2
```

j Configure dialing rules

```
[Router] dialer-rule 1 ipx permit
```

# 25

## CONFIGURING DLSw

This chapter contains information on the following topics:

- DLSw Protocol Overview
- Configuration of DLSw
- Display and Debug DLSw
- Typical DLSw Configuration Example
- Diagnosis and Troubleshooting of DLSw Fault

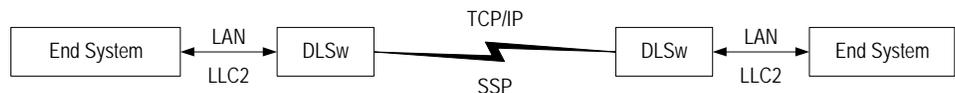
---

### DLSw Protocol Overview

Data Link Switch Protocol (DLSw) is a method designed by Advanced Peer-to-Peer Networking (APPN) Implementers Workshop (AIW) to load SNA through TCP/IP (SNA is a network protocol introduced by IBM in 1970's and completely correspondent with OSI reference model). DLSw technology is one of the solutions for implementing the transmission across WANs via SNA protocol.

The operating principle of DLSw is shown in the following diagram:

**Figure 138** DLSw principle diagram



From the above diagram, you may find out the router with DLSw transforms the frame in format LLC2 on the local SNA equipment into SSP frame which can be encapsulated into TCP messages. Then it sends SSP frame to the remote end through TCP channel across WANs, and transforms SSP frame into the corresponding frame in LLC2 format at the remote end site, finally sends the latter to the next-hop SNA equipment. In another words, DLSw makes the local terminating equipment “think” the remote equipment locates in the same network. With the differences from transparent bridge, DLSw transforms the original LLC2 protocol frame into SSP protocol frame instead of transparent-transmitting to the next hop directly, so as to encapsulate the existing data into TCP messages. It features local acknowledgement mechanism, thus reducing unnecessary data transmission (confirming frame and maintaining alive frame) and resolving the overtime problem of data link control.

With DLSw technology, the transmission across TCP/IP via SDLC link protocol can also be implemented. The procedure is to transform the messages in SDLC format into the messages in LLC2 format, then utilize DLSw to intercommunicate with the remote end. DLSw also supports intercommunication of different media between LAN and SDLC.

## Configuration of DLSw

DLSw configuration includes:

- Create DLSw local peer entity
- Create DLSw remote end peer entity
- Configure Bridge set connecting to DLSw
- Configure to add Ethernet port to Bridge set
- Configure link layer protocol for interface encapsulation to be SDLC
- Configure SDLC role
- Configure SDLC virtual MAC address
- Configure SDLC address
- Configure SDLC peer entity
- Configure XID of SDLC
- Configure to add the synchronous interface encapsulated with SDLC to Bridge set
- Configure to stop running DLSw
- Configure baud rate of synchronous interface
- Configure encoding view of synchronous interface
- Configure idle time encoding view of synchronous interface
- Configure parameters of DLSw timer
- Configure other parameters of LLC2
- Configure other parameters of SDLC

### 1 Create DLSw Local Peer Entity

Creating TCP channel is the first step for establishing DLSw connection. To create TCP channel, you have to firstly configure DLSw local peer entity in order to specify the IP address of the local end for establishing TCP connection, then the request sent by the remote end router can be received for establishing TCP connection. One router can only configure one local peer entity.

Please process the following configurations in the system view.

**Table 428** Create DLSw local peer entity

| Operation                     | Command                                                                                                                                                                    |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create DLSw local peer entity | <code>dlsw local ip-address [ init-window init-window-size ] [ max-frame max-frame-size ] [ max-window max-window-size ] [ permit-dynamic ] [ vendor-id vendor-id ]</code> |
| Delete DLSw local peer entity | <code>undo dlsw local</code>                                                                                                                                               |

No DLSw local peer entity is created by default.

### 2 Create DLSw Remote Peer

You need to configure the remote peer to establish TCP channel after configuring the local peer. The router will continuously attempt to establish TCP connection with the remote router. One router can configure several remote peers. TCP channels can be connected with several remote end routers by configuring several remote peers.

Please perform the following configurations in system view.

**Table 429** Create DLSw remote end peer entity

| Operation                          | Command                                                                                                                                                                                                                                                 |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create DLSw remote end peer entity | <b>dlsw remote ip-address</b> [ <b>backup backup-peer-address</b> ] [ <b>priority priority-value</b> ] [ <b>max-frame max-frame-size</b> ] [ <b>max-queue max-queue-length</b> ] [ <b>linger minutes</b> ] [ <b>compatible { 3com   nonstandard }</b> ] |
| Delete DLSw remote end peer entity | <b>undo dlsw remote ip-address</b>                                                                                                                                                                                                                      |

No DLSw remote end peer entity is created by default.

When creating remote backup-peer, note:

When the remote backup peer is created, the **tcp ip-address** should be the IP address of peer backup entity and the **backup backup-peer-address** should be the IP address of the remote master peer, which has established TCP connection. That is, the user should ensure that TCP connection has been established between the local peer and the remote peer before creating a remote backup peer. When a remote peer is created for the first time, meanwhile, the remote backup peer is also being created, the system will prompt the following information: `Primary peer ip address does not exist`

This prompt indicates that the user should create a remote master peer before creating the backup peer.

If the TCP connection of the master link fails, the backup link can be used to maintain the connection (the backup TCP connection link can be found via the **display dlsw remote** command) until its **linger minutes** timeout.

### 3 Configure Bridge set Connecting to DLSw

DLSw technology is developed on the basis of bridge technology. Bridge set is a unit for forwarding by bridge. Several Ethernet ports can be configured into a Bridge set in order to forward messages among them. To forward the messages of the specified Bridge set to the remote end over TCP connection, you need to use this command to connect a local Bridge set to DLSw. In another words, the messages of the local Bridge set can be forwarded to the remote end through TCP channel. You can use the command several times to connect several Bridge sets to DLSw, so that all of them can be forwarded through TCP channel.

Please process the following configurations in the system view.

**Table 430** Configure Bridge set connecting to DLSw

| Operation                               | Command                                                 |
|-----------------------------------------|---------------------------------------------------------|
| Configure Bridge set connecting to DLSw | <b>dlsw bridge-set</b><br><b>Bridge-set-number</b>      |
| Delete Bridge set connecting to DLSw    | <b>undo dlsw bridge-set</b><br><b>Bridge-set-number</b> |

No Bridge set connecting to DLSw is configured by default.

### 4 Configure to Add Ethernet Port to Bridge Set

LLC2 message on an Ethernet port can be forwarded to the remote end peer entity through the corresponding TCP channel after the Ethernet port is added to the Bridge set.

Please process the following configurations in the Ethernet interface view.

**Table 431** Configure to add ethernet port to Bridge set

| Operation                                                      | Command                                            |
|----------------------------------------------------------------|----------------------------------------------------|
| Configure to add Ethernet port to Bridge set                   | <b>bridge-set</b><br><b>bridge-set-number</b>      |
| Delete the configuration of adding Ethernet port to Bridge set | <b>undo bridge-set</b><br><b>Bridge-set-number</b> |

No Ethernet port is added to Bridge set by default.

## 5 Configure Link Layer Protocol for Interface Encapsulation as SDLC

SDLC is a link layer protocol relative to SNA. The working principle is very similar to HDLC. To allow DLSw to operate normally, the encapsulation protocol of synchronous interface link layer should be changed to SDLC.

Please process the following configurations in the synchronous interface view.

**Table 432** Configure link layer protocol for Interface encapsulation to be SDLC

| Operation                                                            | Command                   |
|----------------------------------------------------------------------|---------------------------|
| Configure link layer protocol for interface encapsulation to be SDLC | <b>link-protocol sdlc</b> |

By default, the link layer protocol of synchronous interface encapsulation is PPP.

Note that SDLC link protocol cannot load IP protocol, so you should remove all of the commands related with IP, such as delete interface IP address, before encapsulating SDLC.

## 6 Configure SDLC Role

SDLC is a link layer protocol in the unbalanced mode. In another words, the connected equipment on the both ends does not have unequal priority. One of the parts is the primary station that plays the leading role and controls the whole connection process and its role is *primary*. The other part is the secondary station that is controlled in a passive mode and its role is *secondary*. Subscribers need to configure role for the interface encapsulated with SDLC protocol.

Please process the following configurations in the synchronous interface view.

**Table 433** Configure SDLC role

| Operation           | Command                                    |
|---------------------|--------------------------------------------|
| Configure SDLC role | <b>sdlc status { primary   secondary }</b> |
| Delete SDLC role    | <b>undo sdlc status</b>                    |

SDLC role shall be configured according to the role of SDLC equipment connecting with this router. If SDLC equipment connecting with the interface is *primary*, the interface should be set to *secondary*. If the connected equipment is *secondary*, the interface should be set to *primary*.

Generally, the central IBM mainframes are *primary*, and terminal equipment is *secondary*, such as Unix host and ATM machine.

## 7 Configure SDLC Virtual MAC Address

Originally, DLSw is designed for LLC2 type of protocol to establish the mapping relationship of virtual circuit through MAC address. Thus, you have to specify MAC address for SDLC virtual circuit in order to allow SDLC message to participate in

forwarding. This command is used to specify the virtual MAC address on the interface, thus providing source MAC address for transforming SDLC message into LLC2 message.

Please process the following configurations in the synchronous interface view.

**Table 434** Configure SDLC virtual MAC address

| Operation                          | Command                                                |
|------------------------------------|--------------------------------------------------------|
| Configure SDLC virtual MAC address | <b>sdlc mac-map local mac-address [ sdlc-address ]</b> |
| Delete SDLC virtual MAC address    | <b>undo sdlc mac-map local [ sdlc-address ]</b>        |

There is no SDLC virtual MAC address by default.

Note that there are two forms of SDLC virtual MAC address: one is not followed by `sdlc-address`, in this form, the address to be configured is the shared VMAC address on the interface; the other is followed by `adlc-address`, that is, the VMAC is configured for the specified ADLC address node. When one ADLC node is configured with its own VMAC, it will use this VMAC address as the source MAC address for DLSw; if the node does not have its own VMAC, it will use the shared VMAC address, and applies its own `sdlc-address` as the last byte of the VMAC address, so as to differentiate between this address and other ADLC nodes.

## 8 Configure SDLC Address

SDLC protocol permits that several virtual circuits exist in a SDLC physic link. The one end connects to the primary station and the other end connects to the secondary station. You should specify the SDLC address of each virtual circuit so as to differentiate the virtual circuit. SDLC is unbalanced mode through sharer or SDLC switch. One primary equipment can be connected with several secondary equipment and the relationship is unique. However, connection cannot be established between secondary equipment. It can ensure that communication normally operates in one group of SDLC equipment only if the addresses of secondary equipment are identified. This command is used to specify SDLC address for virtual circuit. The address is unique in a physical interface. The SDLC address configured on the synchronous interface is the de facto address of SDLC secondary station.

Please process the following configurations in the synchronous interface view.

**Table 435** Configure SDLC address

| Operation              | Command                                  |
|------------------------|------------------------------------------|
| Configure SDLC address | <b>sdlc controller sdlc-address</b>      |
| Delete SDLC address    | <b>undo sdlc controller sdlc-address</b> |

There is no SDLC synchronous interface address by default.

SDLC addresses range from 0x01 to 0xFE. The SDLC address on a router is valid for one physical interface. That is, the SDLC addresses configured on the different interfaces can be same.

## 9 Configure SDLC Peer Entity

This command is used to specify a next-hop MAC address on the other end for a SDLC virtual address so as to provide the destination MAC address when transforming from SDLC to LLC2. When setting up DLSw, one SDLC address should be configured with one corresponding partner. The MAC address of

partner shall be the MAC address of the remote end SNA equipment (physical addresses of such equipment as Ethernet and Token-Ring) or next-hop MAC address composed of SDLC.

Please process the following configurations in the synchronous interface view.

**Table 436** Configure SDLC peer entity

| Operation                  | Command                                                |
|----------------------------|--------------------------------------------------------|
| Configure SDLC peer entity | <b>sdlc mac-map remote mac-addr<br/>sdlc-addr</b>      |
| Delete SDLC peer entity    | <b>undo sdlc mac-map remote mac-addr<br/>sdlc-addr</b> |

By default, synchronous interface is not configured with SDLC peer entity.

Note the differences between the word digital order of Token-Ring and Ethernet. When configuring Token-Ring, you can configure it according to the address labeled on the equipment directly. When configuring Ethernet, you should reverse every Byte. For example, as to Ethernet MAC address, it should be configured to 0007.3fc0.5a12 if the mark is 00e0.fc03.a548. Thereinto, the first byte "00" of 00e0 is reversed as "00", the binary form of the second byte "e0" is 11100000, after reversed, it is 00000111, that is "07" in hexadecimal form. Computed in this way, "3fc0" is reversed form of "fc03", and "5a12" is the reversed form of "a548".

#### 10 Configure XID of SDLC

XID is used to identify an identity of equipment in SNA. Generally, there are two kinds of equipment - PU2.0 and PU2.1. PU2.1 equipment is configured with XID and can show their identities each other by exchanging XID. PU2.0 equipment does not exchange XID and it does not include XID. Thus PU2.1 equipment does not need this command, but you have to specify a XID for PU2.0 equipment.

Please process the following configurations in the synchronous interface view.

**Table 437** Configure XID of SDLC

| Operation             | Command                                     |
|-----------------------|---------------------------------------------|
| Configure XID of SDLC | <b>sdlc xid sdlc-address<br/>xid-number</b> |
| Delete XID of SDLC    | <b>undo sdlc xid sdlc-address</b>           |

By default, synchronous interface is not configured with XID of SDLC.

#### 11 Configure to Add the Sync Interface to Bridge Set

To allow the synchronous interface encapsulated with SDLC to participate in DLSw forwarding, you need to use this command to add SDLC interface to a Bridge set. The Bridge set on Ethernet interface takes part in the local forwarding, but the Bridge set configured in the SDLC only takes part in DLSw forwarding, that is, all of the data on it will be forwarded to TCP channels.

Please process the following configurations in the synchronous interface view.

**Table 438** Add synchronous Interface to Bridge set

| Operation                                                              | Command                                      |
|------------------------------------------------------------------------|----------------------------------------------|
| Add synchronous interface to Bridge set                                | <b>bridge-set<br/>bridge-set-number</b>      |
| Delete the configuration of adding synchronous interface to Bridge set | <b>undo bridge-set<br/>bridge-set-number</b> |

**12** Configure to Stop Running DLSw

Please carry out the following configuration under overall view.

**Table 439** Configure to stop running DLSw

| Operation           | Command                 |
|---------------------|-------------------------|
| Enable running DLSw | <b>dlsw enable</b>      |
| Stop running DLSw   | <b>undo dlsw enable</b> |

By default, the system does not run DLSw protocol.

After using this command, the system will release all the dynamic resources but reserve the existing configuration.

**13** Configure Baud Rate of Sync Interface

All of the above commands are some of basic commands for configuring DLSw. SNA equipment have diversified sorts and quite differences in the factual environment. The following commands are some frequently used adjustment parameters used to make the different equipment compatible.

Please process the following configurations in the synchronous interface view.

**Table 440** Configure baud rate of synchronous Interface

| Operation                                    | Command                  |
|----------------------------------------------|--------------------------|
| Configure baud rate of synchronous interface | <b>baudrate baudrate</b> |

By default, the baud rate of the serial interface on SNA equipment is 9600bps.

**14** Configure Encoding Mode of Sync Interface

There are two kinds of encoding modes including NRZI and NRZ on the synchronous serial interface. The routers in our company generally use NRZ encoding mode, but the encoding mode of the serial ports in some SNA equipment uses NRZI. So you need to change the encoding of routers according to the encoding mode used by the connected equipment.

This command is used to change the encoding mode of synchronous serial interface.

Please process the following configurations in the synchronous interface view.

**Table 441** Configure encoding mode of synchronous Interface

| Operation                                             | Command               |
|-------------------------------------------------------|-----------------------|
| Configure NRZI encoding mode of synchronous interface | <b>code nrzi</b>      |
| Delete NRZI encoding mode of synchronous interface    | <b>undo code nrzi</b> |

By default, the synchronous interface uses encoding mode NRZ.

**15** Configure Idle Time Encoding Mode of Sync Interface

The SDLC serial ports of the 3Com Router series of routers is identified with "7E" during the idle time, but all of the serial ports on some SDLC equipment use high level working status "1" during the idle time. To improve the compatibility with the equipment, you need to change the idle time encoding mode of the routers.

Please process the following configurations in the synchronous interface view.

**Table 442** Configure Idle time encoding mode of synchronous Interface

| Operation                                                  | Command               |
|------------------------------------------------------------|-----------------------|
| Configure idle time encoding mode of synchronous interface | <b>idle-mark</b>      |
| Restore idle time encoding mode of synchronous interface   | <b>undo idle-mark</b> |

By default, the synchronous interface uses encoding mode "7E".

Generally, the idle time encoding mode of synchronous interface doesn't need to be modified. You may need to configure this command when connecting AS/400, that is, to change the idle time encoding mode in order to accelerate the polling rate of AS/400.

## 16 Configure Parameters of DLSw Timer

The values of various timers used when DLSw established virtual circuits can be modified by configuring DLSw protocol timer.

Please carry out the following configuration in system view.

**Table 443** Configure parameters of DLSw timer

| Operation                                                 | Command                                                                                                                               |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Configure parameters of DLSw timer                        | <b>dls w timer [ cache seconds ] [ connected seconds ] [ keepalive seconds ] [ local-pending seconds ] [ remote-pending seconds ]</b> |
| Restore the default value of each parameter of DLSw timer | <b>undo dls w timer [cache   connected   keepalive   local-pending   remote-pending ]</b>                                             |

By default, **cache seconds** is 120; **connected seconds** is 300; **keepalive seconds** is 30; **local-pending seconds** is 10; **remote-pending seconds** is 30.

It is recommended that subscribers do not modify or configure the parameters of DLSw timers in the common conditions.

## 17 Configure Other Parameters of LLC2

### a Configure LLC2 Local Acknowledgement Delay Time

The message transmitted by SNA over Ethernet is LLC2 message. Some working parameters of LLC2 can be modified by configuring the commands related to LLC2.

LLC2 local acknowledgement delay time refers to max wait time of delay acknowledgement when receiving a piece of LLC2 data message.

Please process the following configurations in the Ethernet interface view.

**Table 444** Configure LLC2 local acknowledgement delay time

| Operation                                                          | Command                              |
|--------------------------------------------------------------------|--------------------------------------|
| Configure LLC2 local acknowledgement delay time                    | <b>llc2 timer ack-delay mseconds</b> |
| Restore the default value of LLC2 local acknowledgement delay time | <b>undo llc2 timer ack-delay</b>     |

By default, LLC2 local acknowledgement delay time is 100 ms.

### b Configure LLC2 Premature Acknowledgement Window

LLC2 pre-answer refers to sending answer packet to the peer in advance after receiving the specified amount of packets. This parameter and local answer display time in 1 controls the time to send answer packet together. If any condition is satisfied, the answer packet will be sent, that is, it sends acknowledgement message to the other part in advance after receiving the nth message.

Please process the following configurations in the Ethernet interface view.

**Table 445** Configure LLC2 premature acknowledgement window

| Operation                                                                 | Command                  |
|---------------------------------------------------------------------------|--------------------------|
| Configure the length of LLC2 premature acknowledgement window             | <b>llc2 max-ack n</b>    |
| Restore the default length value of LLC2 premature acknowledgement window | <b>undo llc2 max-ack</b> |

By default, the length of LLC2 premature acknowledgement window is 3.

**c** Configure LLC2 Local Acknowledgement Window

LLC2 adopts the window mechanism when sending packets, while not requiring the timely reply for each packet. LLC2 can wait for the replies from the peer at the same time after the whole window has been sent. LLC2 local acknowledgement window size is the Max. amount of packets that LLC2 can send before receiving the replies.

Please process the following configurations in the Ethernet interface view.

**Table 446** Configure LLC2 premature acknowledgement window

| Operation                                                                 | Command                           |
|---------------------------------------------------------------------------|-----------------------------------|
| Configure the length of LLC2 Premature Acknowledgement Window             | <b>llc2 receive-window length</b> |
| Restore the default length value of LLC2 premature acknowledgement window | <b>undo llc2 receive-window</b>   |

By default, the length of LLC2 local acknowledgement window is 7.

**d** Configure Modulo Value of LLC2

LLC2 uses modulo mode to number the information message like X25 protocol. The modulo value is 8 or 128. Ethernet generally uses modulo 128.

Please process the following configurations in the Ethernet interface view.

**Table 447** Configure modulo value of LLC2

| Operation                                      | Command                 |
|------------------------------------------------|-------------------------|
| Configure Modulo Value of LLC2                 | <b>llc2 modulo n</b>    |
| Restore the default value of LLC2 modulo value | <b>undo llc2 modulo</b> |

By default, the modulo value of LLC2 is 128.

**e** Configure Retransmission Number of LLC2

LLC2 retransmission number indicates the retransmission number of information frame before receiving no acknowledgement frame sent by the other part.

Please process the following configurations in the Ethernet interface view.

**Table 448** Configure retransmission number of LLC2

| Operation                                                      | Command                              |
|----------------------------------------------------------------|--------------------------------------|
| Configure retransmission number of LLC2                        | <b>llc2 max-transmission retries</b> |
| Restore the default value of the retransmission number of LLC2 | <b>undo llc2 max-transmission</b>    |

By default, the retransmission number of LLC2 is 20.

**f** Configure LLC2 Local Acknowledgement Time

LLC2 local acknowledgement time refers to max wait time for waiting for the other part's acknowledgement after sending a piece of LLC2 data message.

Please process the following configurations in the Ethernet interface view.

**Table 449** Configure LLC2 local acknowledgement time

| Operation                                                    | Command                        |
|--------------------------------------------------------------|--------------------------------|
| Configure LLC2 Local Acknowledgement Time                    | <b>llc2 timer ack mseconds</b> |
| Restore the default value of LLC2 local acknowledgement time | <b>undo llc2 timer ack</b>     |

By default, LLC2 local acknowledgement time is 200 ms.

**g** Configure BUSY Status Time of LLC2

When it queries the station, LLC2 will wait for the next query if the station is busy.

The interval of re-querying LLC2 Busy station.

Please process the following configurations in the Ethernet interface view.

**Table 450** Configure BUSY status time of LLC2

| Operation                                             | Command                         |
|-------------------------------------------------------|---------------------------------|
| Configure BUSY status time of LLC2                    | <b>llc2 timer busy mseconds</b> |
| Restore the default value of BUSY status time of LLC2 | <b>undo llc2 timer busy</b>     |

By default, BUSY status time of LLC2 is 300 ms.

**h** Configure P/F Wait Time of LLC2

P/F wait time of LLC2 refers to duration waiting for correct information frame after sending frame P.

Please process the following configurations in the Ethernet interface view.

**Table 451** Configure P/F wait time of LLC2

| Operation                                          | Command                         |
|----------------------------------------------------|---------------------------------|
| Configure P/F wait time of LLC2                    | <b>llc2 timer poll mseconds</b> |
| Restore the default value of P/F wait time of LLC2 | <b>undo llc2 timer poll</b>     |

By default, P/F wait time of LLC2 is 5000 ms.

**i** Configure REJ Status Time of LLC2

REJ status time of LLC2 refers to duration waiting for correct information frame after refusing frame.

Please process the following configurations in the Ethernet interface view.

**Table 452** Configure REJ status time of LLC2

| Operation                                            | Command                           |
|------------------------------------------------------|-----------------------------------|
| Configure REJ status time of LLC2                    | <b>llc2 timer reject mseconds</b> |
| Restore the default value of REJ status time of LLC2 | <b>undo llc2 timer reject</b>     |

By default, REJ status time of LLC2 is 500 ms.

**j** Configure Queue Length of Sending Message of LLC2

Please process the following configurations in the Ethernet interface view.

**Table 453** Configure queue length of sending message of LLC2

| Operation                                                            | Command                           |
|----------------------------------------------------------------------|-----------------------------------|
| Configure queue length of sending message of LLC2                    | <b>llc2 max-send-queue length</b> |
| Restore the default value of queue length of sending message of LLC2 | <b>undo llc2 max-send-queue</b>   |

By default, the queue length of sending message of LLC2 is 50.

**18** Configure Other Parameters of SDLC

**a** Configure Queue Length of Sending Message of SDLC

Please process the following configurations in the synchronous interface view.

**Table 454** Configure queue length of sending message of SDLC

| Operation                                                            | Command                           |
|----------------------------------------------------------------------|-----------------------------------|
| Configure queue length of sending message of SDLC                    | <b>sdlc max-send-queue length</b> |
| Restore the default value of queue length of sending message of SDLC | <b>undo sdlc max-send-queue</b>   |

By default, the queue length of sending message of SDLC is 50.

**b** Configure SDLC Local Acknowledgement Window

SDLC Local Acknowledgement Window adopts the window mechanism when sending packets, while not requiring the timely reply for each packet. SDLC Local Acknowledgement Window can wait for the replies from the peer at the same time after the whole window has been sent.

Please process the following configurations in the synchronous interface view.

**Table 455** Configure SDLC local acknowledgement window

| Operation                                                             | Command                   |
|-----------------------------------------------------------------------|---------------------------|
| Configure the length of SDLC local acknowledgement window             | <b>sdlc window length</b> |
| Restore the default length value of SDLC local acknowledgement window | <b>undo sdlc window</b>   |

By default, the length of SDLC local acknowledgement window is 7.

**c** Configure Modulo Value of SDLC

SDLC uses modulo mode to number the information message like X25 protocol. The modulo value is 8 or 128. SDLC generally uses modulo 8.

Please process the following configurations in the synchronous interface view.

**Table 456** Configure modulo value of SDLC

| Operation                                      | Command                 |
|------------------------------------------------|-------------------------|
| Configure Modulo Value of SDLC                 | <b>sdlc modulo n</b>    |
| Restore the default value of SDLC modulo value | <b>undo sdlc modulo</b> |

By default, the modulo value of SDLC is 8.

**d** Configure Maximum Receivable Frame Length N1 of SDLC

Maximum frame length of SDLC refers to byte number of maximum transmissible and receivable message, not including parity bit and stop bit.

Please process the following configurations in the synchronous interface view.

**Table 457** Configure maximum receivable frame length of SDLC

| Operation                                                            | Command                  |
|----------------------------------------------------------------------|--------------------------|
| Configure Maximum Receivable Frame Length of SDLC                    | <b>sdlc max-pdu n</b>    |
| Restore the default value of maximum receivable frame length of SDLC | <b>undo sdlc max-pdu</b> |

By default, the maximum receivable frame length of SDLC is 265 bytes.

Generally, the length is 265 for some PU2.0 equipment and 521 for IBM AS/400. We often need to configure our equipment to be of the same values as the connected SDLC equipment.

**e** Configure Retransmission Number N2 of SDLC

The retransmission number N2 of SDLC refers to the retransmission number before receiving no acknowledgement packet sent by the other part.

Please process the following configurations in the synchronous interface view.

**Table 458** Configure retransmission number of SDLC

| Operation                                                      | Command                              |
|----------------------------------------------------------------|--------------------------------------|
| Configure retransmission number of SDLC                        | <b>sdlc max-transmission retries</b> |
| Restore the default value of the retransmission number of SDLC | <b>undo sdlc max-transmission</b>    |

By default, the retransmission number of SDLC is 20.

**f** Configure Poll Time Interval of SDLC

Poll time interval of SDLC refers to wait time interval between two SDLC nodes polled by SDLC primary station.

Please process the following configurations in the synchronous interface view.

**Table 459** Configure poll time interval of SDLC

| Operation                                               | Command                         |
|---------------------------------------------------------|---------------------------------|
| Configure poll time interval of SDLC                    | <b>sdlc timer poll mseconds</b> |
| Restore the default value of poll time interval of SDLC | <b>undo sdlc timer poll</b>     |

By default, the poll time interval of SDLC is 100 ms.

**g** Configure SAP address for transforming SDLC to LLC2

When transforming SDLC message to LLC2 message, it needs both SAP and MAC addresses. This command is used to specify SAP address used when transforming LLC2 for a SDLC byte.

Generally, the SAP address used by SNA protocol is 0x04, 0x08 or 0x0C.

Please process the following configurations in the synchronous interface view.

**Table 460** Configure SAP address for transforming SDLC to LLC2

| Operation                                                                     | Command                                       |
|-------------------------------------------------------------------------------|-----------------------------------------------|
| Configure local SAP address for transforming SDLC to LLC2                     | <b>sdlc sap-map local lsap<br/>sdlc-addr</b>  |
| Restore the default value of local SAP address for transforming SDLC to LLC2  | <b>undo sdlc sap-map local<br/>lsap</b>       |
| Configure remote SAP address for transforming SDLC to LLC2                    | <b>sdlc sap-map remote dsap<br/>sdlc-addr</b> |
| Restore the default value of remote SAP address for transforming SDLC to LLC2 | <b>undo sdlc sap-map remote<br/>dsap</b>      |

By default, both LSAP and DSAP of LLC2 are 04.

#### h Configure Data Bi-directional Transmission Mode of SDLC

This command is used to allow the synchronous serial port of the encapsulated SDLC protocol to work in the bi-directional data transmission mode. In other words, you can restore the time to wait for a reply used by secondary station to the default value

Please process the following configurations in the synchronous interface view.

**Table 461** Configure data bi-directional transmission mode of SDLC

| Operation                                               | Command                       |
|---------------------------------------------------------|-------------------------------|
| Configure data bi-directional transmission mode of SDLC | <b>sdlc simultaneous</b>      |
| Delete data bi-directional transmission mode of SDLC    | <b>undo sdlc simultaneous</b> |

By default, SDLC data uses bi-directional (alternate) transmission mode.

#### i Configure Acknowledgement Wait Time T1 of SDLC Primary Station

Acknowledgement wait time T1 of primary station refers to the duration that the primary station waits for acknowledgement from secondary station after sending information frame.

Please process the following configurations in the synchronous interface view.

**Table 462** Configure acknowledgement wait time T1 of SDLC primary station

| Operation                                                                      | Command                        |
|--------------------------------------------------------------------------------|--------------------------------|
| Configure acknowledgement wait time T1 of SDLC Primary Station                 | <b>sdlc timer ack mseconds</b> |
| Restore the default value of acknowledgement wait time of SDLC primary station | <b>undo sdlc timer ack</b>     |

By default, the acknowledgement wait time T1 of SDLC primary station is configured to be 3000 ms.

#### j Configure Acknowledgement Wait Time T2 of SDLC Secondary Station

Acknowledgement wait time T2 of secondary station refers to the duration that the secondary station waits for acknowledgement from primary station after sending information frame.

Please process the following configurations in the synchronous interface view.

**Table 463** Configure acknowledgement wait time T2 of SDLC secondary station

| Operation                                                                           | Command                                 |
|-------------------------------------------------------------------------------------|-----------------------------------------|
| Configure acknowledgement wait time T2 of SDLC secondary station                    | <b>sdlc timer lifetime<br/>mseconds</b> |
| Restore the default value of acknowledgement wait time T2 of SDLC secondary station | <b>undo sdlc timer lifetime</b>         |

By default, the acknowledgement wait time T2 of SDLC secondary station is configured to be 500 ms.

## Display and Debug DLSw

**Table 464** Display and debug DLSw

| Operation                                                     | Command                                                             |
|---------------------------------------------------------------|---------------------------------------------------------------------|
| Display interface Bridge set information                      | <b>display dlsw bridge-entry</b>                                    |
| Display performance exchange information                      | <b>display dlsw information [ local ] [ ip-address ip-address ]</b> |
| Display Information about DLSw circuits running in the router | <b>display dlsw circuits [ circuit-id ] [verbose]</b>               |
| Display remote end peer entity information                    | <b>display dlsw remote [ ip-address ip-address ]</b>                |
| Clear entry buffer memory information of Bridge set           | <b>reset dlsw circuits [ circuit-id ]</b>                           |
| Clear virtual circuit information                             | <b>debugging dlsw circuit</b>                                       |
| Open debugging information switch of DLSw virtual circuit     | <b>debugging dlsw core</b>                                          |
| Open debugging information switch of DLSw status machine      | <b>debugging dlsw event</b>                                         |
| Open debugging information switch of DLSw abnormal events     | <b>debugging dlsw packet</b>                                        |
| Open debugging information switch of DLSw messages            | <b>debugging dlsw tcp</b>                                           |
| Open debugging information switch of DLSw peer entity         | <b>debugging sdlc event</b>                                         |
| Open debugging information switch of SDLC events              | <b>debugging sdlc packet</b>                                        |
| Open debugging information switch of SDLC messages            | <b>display dlsw bridge-entry</b>                                    |

## Typical DLSw Configuration Example

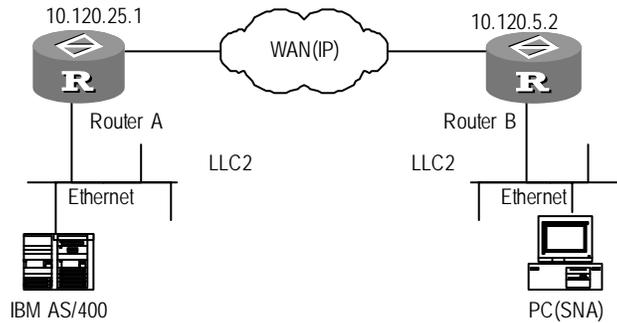
### DLSw Configuration of LAN-LAN

#### I. Networking Requirement

LAN-LAN working mode is used. The two running SNA and LAN are connected by IP across WAN.

## II. Networking Diagram

**Figure 139** Networking diagram of DLSw configuration of LAN-LAN



## III. Configuration Procedure

### 1 Router A Configuration:

```
[Router] dlsw local 10.120.25.1
[Router] dlsw remote 10.120.5.2
[Router] dlsw bridge-set 5
[Router] interface ethernet 0
[Router-Ethernet0] bridge-set 5
```

### 2 Router B Configuration:

```
[Router] dlsw local 10.120.5.2
[Router] dlsw remote 10.120.25.1
[Router] dlsw bridge-set 7
[Router] interface ethernet 0
[Router-Ethernet0] bridge-set 7
```

Thus, the two LANs across WAN are connected together. Note that we don't list the related IP commands here, but you have to make sure that IPs of the configured local-peer and remote-peer can be intercommunicated each other. The notes apply for the following sections.

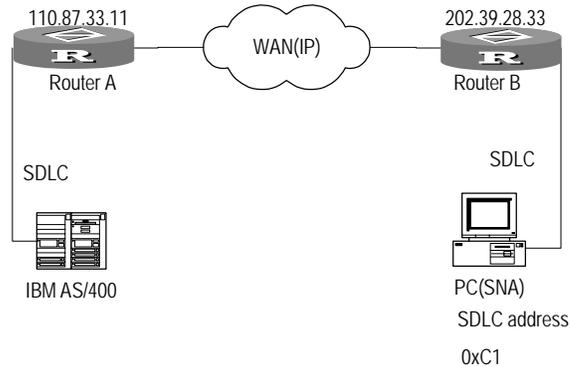
## DLSw Configuration of SDLC-SDLC

### I. Networking Requirement

The two SDLCs across WAN are connected together by using SDLC-SDLC working mode.

## II. Networking Diagram

**Figure 140** Networking diagram of DLSw configuration of SDLC-SDLC



## III. Configuration Procedure

### 1 Router A Configuration:

```
[Router] dlsw local 110.87.33.11
[Router] dlsw remote 202.39.28.33
[Router] dlsw bridge-set 1
[Router] interface serial 0
[Router-Serial0] link-protocol sdlc
[Router-Serial0] baudrate 9600
[Router-Serial0] code nrzi
[Router-Serial0] sdlc status secondary
[Router-Serial0] sdlc mac-map local 00-00-11-11-00-00
[Router-Serial0] sdlc controller c1
[Router-Serial0] sdlc mac-map remote 00-00-22-22-00-c1 c1
[Router-Serial0] bridge-set 1
```

### 2 Router B Configuration:

```
[Router] dlsw local 202.39.28.33
[Router] dlsw remote 110.87.33.11
[Router] dlsw bridge-set 1
[Router] interface serial 1
[Router-Serial1] link-protocol sdlc
[Router-Serial1] baudrate 9600
[Router-Serial1] code nrzi
[Router-Serial1] sdlc status primary
[Router-Serial1] sdlc mac-map local 00-00-22-22-00-00
[Router-Serial1] sdlc controller c1
[Router-Serial1] sdlc mac-map remote 00-00-11-11-00-c1 c1
[Router-Serial1] bridge-set 1
```

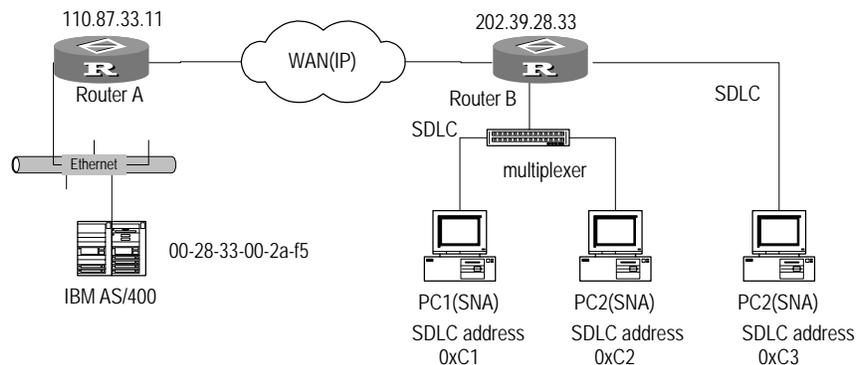
## Transform Configuration from SDLC-LAN Remote End Media to DLSw

### I. Networking Requirement

This example is a typical transform configuration from SDLC-LAN to DLSw and SDLC includes multipoint support function. Among this, the connected node C1 and C2 are nodes of PU2.0 type (ATM) and C3 is node of PU2.1 type (OS2). The port connected to multiplexer uses NRZ encoding mode and the port connected separately uses NRZI encoding mode.

## II. Networking Diagram

Figure 141 Networking Diagram of SDLC-LAN



## III. Configuration Procedure:

### 1 Router A Configuration:

```
[Router] dlsw local 110.87.33.11
[Router] dlsw remote 202.39.28.33
[Router] dlsw bridge-set 1
[Router] interface ethernet 0
[Router-Ethernet0] bridge-set 1
```

### 2 Router B Configuration:

```
[Router] dlsw local 202.39.28.33
[Router] dlsw remote 110.87.33.11
[Router] dlsw bridge-set 1
[Router] interface serial 0
[Router-Serial0] link-protocol sdslc
[Router-Serial0] baudrate 9600
[Router-Serial0] sdslc status primary
[Router-Serial0] sdslc mac-map local 00-00-12-34-56-00
[Router-Serial0] sdslc controller c1
[Router-Serial0] sdslc xid c1 03e00001
[Router-Serial0] sdslc mac-map remote 00-14-cc-00-54-af c1
[Router-Serial0] sdslc controller c2
[Router-Serial0] sdslc xid c2 03e00002
[Router-Serial0] sdslc mac-map remote 00-14-cc-00-54-af c2
[Router-Serial0] bridge-set 1
[Router-Serial0] interface serial 1
[Router-Serial1] link-protocol sdslc
[Router-Serial1] baudrate 9600
[Router-Serial1] code nrzi
[Router-Serial1] sdslc status primary
[Router-Serial1] sdslc mac-map local 00-00-22-22-00-00
[Router-Serial1] sdslc controller c3
[Router-Serial1] sdslc mac-map remote 00-14-cc-00-54-af c3
[Router-Serial1] bridge-set 1
```

Note that MAC address of partner is the same as MAC address of AS/400 network card when configuring router B, but the word digital order on Ethernet and Token-Ring are reversed, thus you should reverse the MAC addresses to configure them. If the other part is Token-Ring, then you do not need to reverse it. In the

above example, c1 and c2 are the equipment of PU2.0 type, and c3 is the equipment of PU2.1 type.

---

## Diagnosis and Troubleshooting of DLSw Fault

The normal communication of DLSw requires the sound coordination between the two SNA equipments and two routers operating DLSw, which participate in the communication. Problem in the co-ordination between any of the two points is likely to result in failure in connection.

### **Fault 1: TCP channel can not be created. The status shown is DISCONNECT when using command display dlsw remote.**

Creating TCP channel is the first step for the successful connection of DLSw. If TCP connection can't be established, the problem lies between the two routers. Generally, the problem is the configuration of IP address of the router. You can check if the IP address of remote-peer is accessible by the ping command with the source address. Also you can use display ip routing-table command to see if there is any route to the network segment. TCP connection can be created once both parties have established correct routes.

### **Fault 2: circuit can not be created correctly. To display dlsw circuits, the virtual circuit can't attain CONNECTED state.**

There are many causes that circuit can't be created. First of all, please make sure that TCP connection to the opposite end is successfully established. If TCP connection can be established successfully, while circuit can't be created, this is generally caused by the problem in the coordination of the router and SNA equipment, mainly the problem of SDLC configuration.

Firstly, open the debugging switch of SDLC to observe if the SDLC interface can receive and send messages successfully. You can use display interface command to observe the condition of receiving and sending messages on the interface. If the messages can't be received and sent correctly, it is generally because something is wrong with the encoding mode of the interface, baud rate or clock configuration. Generally, this can be solved by modifying the interface configuration parameter of the router or adjusting the configuration parameter of SDLC equipment.

If the messages can be received and sent correctly, please check if the configuration PU type is correct. You can use sdhc xid command to configure XID, changing the setup of PU type.

If the messages can be received and sent correctly, you can check with display dlsw circuits verbose command to see if the virtual circuit can enter into CIRCUIT\_EST status. If CIRCUIT\_EST is not accessible all the time, it suggests that something is wrong with the coordination between the MAC address and the partner configured. Generally, this can be solved by modifying configuration parameters such as sdhc partner.

If circuit can attain CIRCUIT\_EST state, but can not attain CONNECTED state, it suggests that the SDLC configuration of the router and the configuration of SNA equipment are not matching. Check the configuration of SDLC equipment on both ends and the configuration of the router to see if the configuration of the XID of SNA equipment (PU2.1) and the configuration of XID of the router (PU2.0) are correct. If nothing is wrong with the configuration, check the SDLC line on the

active equipment of SDLC (such as AS/400 or S390) is activated. Sometimes, communication can be implemented after you activate SDLC line manually.



# VI

# ROUTING

- Chapter 26 IP Routing Protocol
- Chapter 27 Configuring Static Routes
- Chapter 28 Configuring RIP
- Chapter 29 Configuring OSPF
- Chapter 30 Configuring BGP
- Chapter 31 Configuring IP Routing Policy
- Chapter 32 Configuring IP Policy Routing





of the router should be used to transfer a data packet to a sub-network or a host, so the packet can reach the next router on this path, or reach the host as a directly connected destination without passing through other routers.

The routing table consists of the following key items:

- **Destination address:** Identifies the destination address or destination network of IP packets.
- **Network mask:** Identifies, together with the destination address, the address of the route segment where the destination host or router is located. For example, if the destination address is 129.102.8.10 and the network mask is 255.255.0.0, the address of the route segment for the destination host or router is 129.102.0.0. The mask consists of several consecutive 1s and 0s, which can be expressed with dotted decimal system or with the number of consecutive 1s in the mask.
- **Output interface:** Indicates the interface of the router that forwards the IP packet.
- **Next hop IP address:** Indicates the next router to which the IP packet will be forwarded.
- **The priority of this route added to IP routing table:** Determines the best route. There may be different next hops to the same destination. These routes can be found by different routing protocols or they may be static routes configured manually. The route with higher priority (smaller value) is the best route. The user can configure multiple routes with different priorities to the same destination and select one to forward messages.

According to the destination of a route, it can be classified as:

- **Sub-network route:** The route whose destination is a sub-network
- **Host route:** The route whose destination is a host

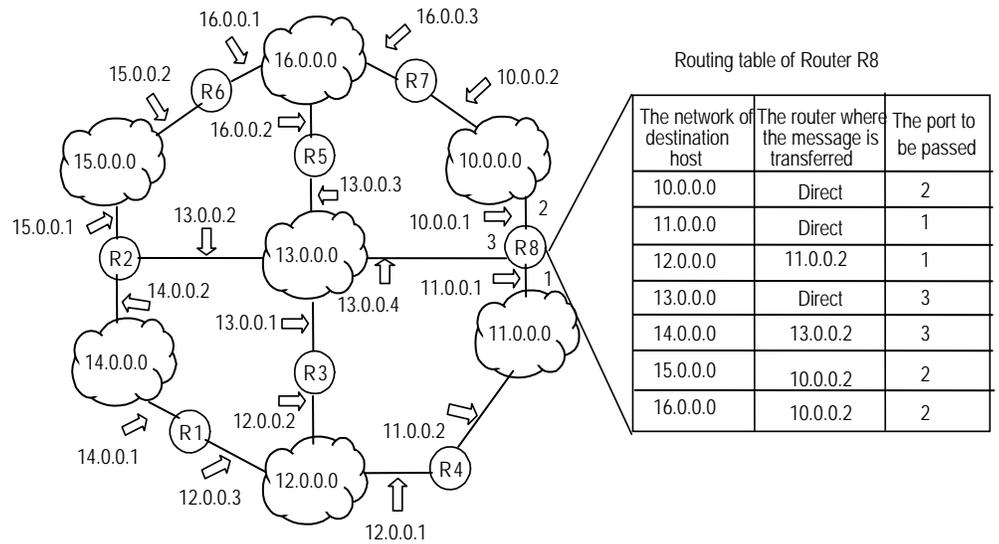
According to the connection mode between the destination and the router, you can classify the router as:

- **Direct route:** The destination address and the router are located in the same segment.
- **Indirect route:** The destination address and the router are not located in the same segment.

To keep the routing table within a certain size, a default route is set. Whenever a data packet fails to find the routing table, the default route is selected to transfer the data packet.

In complicated networks, the digits assigned to a router in each network are its network address. For example, if router 8 (R8) is connected to three networks, it has 3 IP addresses and 3 physical ports. The routing table is shown in the figure below.

**Figure 143** Routing table illustration



3Com routers support not only static route configuration, but also dynamic routing protocols such as RIP, OSPF and BGP. Depending on the interface status and user configuration, a router can automatically obtain some direct routes during their operation.

**Routing Management Strategy**

3Com routers support both manual configuration of a static route to a specific destination and dynamic routing protocol configuration which finds the route with the routing algorithm to interact with other routers in the network. Both static routes configured by the user and dynamic routes found by the routing protocol are uniformly administered in the router.

**Routing Protocol and Routing Priority**

Different routing protocols (including static routes) can find different routes to the same destination, but not all these routes are optimal. In fact, at a certain moment, the current route to a destination is determined only by a unique routing protocol. As a result, every routing protocol (including static route) is assigned a priority. When there are multiple route information sources, the route found by higher-priority routing protocols become the current route. The routing protocols and their default routing priorities (the less the value, the higher the priority) are shown in the Table 465.

Here, 0 stands for a directly connected route and 255 stands for any route from unknown sources or terminals.

**Table 465** Routing Protocol and Routing Priority

| Routing Protocol or Type | Corresponding Routing Priority |
|--------------------------|--------------------------------|
| Direct (Connected)       | 0                              |
| OSPF                     | 10                             |
| STATIC                   | 60                             |
| RIP                      | 100                            |
| IBGP                     | 130                            |

| Routing Protocol or Type | Corresponding Routing Priority |
|--------------------------|--------------------------------|
| OSPF ASE                 | 150                            |
| EBGP                     | 170                            |
| Unknown                  | 255                            |

Except for the direct route (Connected), the priority of each dynamic routing protocol can be manually configured according to specific requirements. In addition, each static route can have a different priority.

### Support of the Route Backup

A backup route allows a router to automatically select another route to transmit data packets when the line changes, and enhances the user network reliability. To implement route backup, you can set a different priority to the multiple routes to the same destination. In fact, a user can set the highest priority to the route passing the main path, and take turns to reduce the priority to the routes passing backup paths. Normally, the router will send data through the main path. When a fault occurs on the line, the route will be hidden, and router will select the backup route with second-highest priority for data transmission. In this way, the switchover from the active interface to the backup interface is implemented. When the main path is recovered, the router recovers the route and begins reselecting routes. Since the recovered route has the highest priority, it selects this main route to transmit data.

### Sharing Routes Learned

As different protocols find different routes due to the various algorithms adopted by each protocol, the problem of sharing the findings of different protocols is of concern. On 3Com routers, a route learned by a routing protocol can be imported to another routing protocol. Each protocol has its own route import mechanism.

# 27

## CONFIGURING STATIC ROUTES

This chapter covers the following topics:

- Static Route Overview
- Configuring a Static Route
- Displaying and Debugging the Routing Table
- Static Route Configuration Example
- Troubleshooting a Static Route Configuration

---

### Static Route Overview

A static route is a special route that allows a router to transmit packets over one path to a specified destination. Proper setting and application of the static route can guarantee network security effectively and at the same time, ensure bandwidth for important applications.



*If the topology changes due to network failure or other problems, the static route cannot change automatically and requires the intervention of administrator.*

The static route has the following attributes:

- **Reachable route:** Normally all routes are reachable and an IP packet is sent to the next hop according to the route identified by the destination -- a common application of static routes.
- **Unreachable route:** When a static route to a certain destination has the "reject" attribute, all IP packets to this destination are discarded and destination unreachable information is given.
- **Black hole route:** When a static route to a certain destination has "black hole" attribute, all IP packets to this destination will be discarded.

Here, the attributes **reject** and **blackhole** are normally used to control the scope of destinations reachable by this router, to facilitate network fault diagnosis.

### Default Route

Default route is one type of static route that is used when no matching route is found or when there is no suitable route. In the routing table, the default route is the route to network 0.0.0.0 (mask is 0.0.0.0). You can check whether the default route is properly set through the result of **display ip routing-table** command. If the destination address of the message does not match any route item in the routing table, the default route is selected. If there is no default route, this message will be discarded and an ICMP message will be returned to the source terminal, indicating that the destination address or network is unreachable.

Default routes are very useful in network. In a typical network with hundreds of routers, dynamic routing protocols may consume lots of bandwidth resource. Using default route means that you can replace high bandwidth links with adequate bandwidth links to meet the requirements of communication for a large number of subscribers.

## Configuring a Static Route

Configuring static and default routes involves tasks described in the following sections:

- Configuring a Static Route
- Configuring a Default Route

## Configuring a Static Route

Perform the following configurations in system view.

**Table 466** Configure a Static Route

| Operation                | Command                                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure a static route | <code>ip route-static ip-address { mask   mask-length } { interface-type interface-number   nexthop-address } [ preference value ] [ reject   blackhole ]</code> |
| Delete a static route    | <code>undo ip route-static { all   ip-address { mask   mask-length } [ interface-type interface-number   nexthop-address ] [ preference value ] }</code>         |

The explanation of each parameter is as follows:

- IP address and network mask  
IP address is shown in dotted decimal format. The 1s in the 32 bit mask must be continuous. The mask can also be presented in the dotted decimal format or by the mask length, that is, the number of "1"s in the mask.
- Transmitting interface or next hop address  
In the configuration of static routes, the transmitting interface **interface-type interface-number** or the next hop address **nexthop-address** can be designated as required by the actual conditions.

You can specify the transmitting interfaces in the following cases:

- For interfaces that support resolution from the network address to the link layer address (like Ethernet interface supporting ARP), if a host address has been specified for *ip-address* and *mask* (or *mask-length*), and if the destination address is in a network directly connected to this interface, then you can specify the transmitting interface.
- For a point-to-point type interface, specifying the transmitting interface implies specifying the address of next hop. In this case the address of the remote interface is considered the address of next hop. If the serial interface is encapsulated with the PPP protocol, the IP address of the node on other end can be determined through PPP consultation. Then you only need to specify the transmitting interface instead of the address of next hop.

When NBMA interfaces like the interface encapsulated with X.25 or frame relay or dial-up interface support point-to-multipoint mode, besides configuring the IP route, you must also set up the secondary route at the link layer and map from the

IP address to the link layer address (such as `dialer route ip`, `x.25 map ip` or `fr map ip` commands, and so on). In this case, you cannot specify the transmitting interface for the static route and must configure the IP address of the next hop.

Actually, all the route items must mark the address of the next hop. According to the destination address of packets, an IP router searches for the matching route in the routing table. Only when the address of next hop is specified in the route, can the link layer find a corresponding address through this address and transfer packets.

However, in certain cases (such as PPP encapsulated in link layer), the address of the node on the other end may be unknown when the router is configured so that the sending interface has to be specified. In addition, if the sending interface has been specified, it is not necessary to change the router's configuration when the address of the node connected on the other end is changed

- Preference  
Different preference configurations can achieve flexible route management. For example, when configuring multiple routes to the same destination, if the same preference is designated, load balancing can be realized. If different preferences are designated, route standby can be realized.
- Other parameters  
The `reject` and `blackhole` attributes refer to unreachable routes and black hole routes respectively.

### Configuring a Default Route

Perform the following configurations in system view.

**Table 467** Configure a Default Route

| Operation                 | Command                                                                                                                                                |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure a default route | <code>ip route-static 0.0.0.0 { 0.0.0.0   0 } { interface-type interface-number   nexthop-address } [ preference value ] [ reject   blackhole ]</code> |
| Delete a default route    | <code>undo ip route-static 0.0.0.0 { 0.0.0.0   0 } [ interface-type interface-number   nexthop-address ] [ preference value ]</code>                   |

The parameters of this command mean the same as those in static route configuration.

### Displaying and Debugging the Routing Table

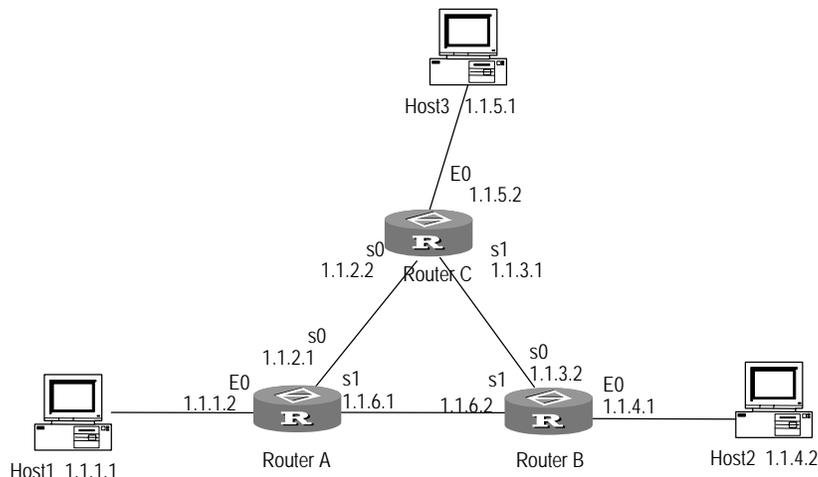
**Table 468** Displaying and Debugging the Routing Table

| Operation                                             | Command                                          |
|-------------------------------------------------------|--------------------------------------------------|
| Display the abstract information of the routing table | <code>display ip routing-table</code>            |
| Display the information of specific route             | <code>display ip routing-table ip-address</code> |
| Display the detailed information of the routing table | <code>display ip routing-table verbose</code>    |
| Display the radix information of the routing table    | <code>display ip routing-table radix</code>      |
| Display the static routing table                      | <code>display ip routing-table static</code>     |

## Static Route Configuration Example

By configuring a static route, any two hosts or routes can communicate with each other.

**Figure 144** Example of static route configuration



To configure a static route:

- 1 Configure the static route for RouterA:

```
[RouterA] ip route-static 1.1.4.0 255.255.255.0 1.1.6.2
[RouterA] ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

- 2 Configure the static routes for RouterB:

```
[RouterB] ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
[RouterB] ip route-static 1.1.1.0 255.255.255.0 1.1.6.1
```

- 3 Configure the static routes for RouterC:

```
[RouterC] ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
[RouterC] ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

## Troubleshooting a Static Route Configuration

The status of the physical interface and link layer protocol is UP, but IP packets cannot be forwarded normally.

Troubleshooting:

- Use the **display ip routing-table static** command to check whether related static routes are configured correctly or not.
- Use the **display ip routing-table** command to see whether this static route is already effective or not.
- Check whether the next hop address is specified or specified correctly on the NBMA type interface.
- Check the secondary routing table of the link layer on the NBMA interface to see if the configuration is correct.

# 28

## CONFIGURING RIP

This chapter covers the following topics:

- RIP Overview
- Configure RIP
- Displaying and Debugging RIP
- RIP - Unicast Configuration Example
- Troubleshooting RIP

---

### RIP Overview

The Routing Information Protocol (RIP) is an interior gateway and dynamic routing protocol based on the Distance-Vector (D-V) routing algorithm. RIP uses User Datagram Protocol (UDP) packets to exchange routing information and adopts hop count to measure the distance from the destination, called the routing cost. In RIP, a hop count that is equal to or larger than 16 is defined as infinity (the destination network or host is unreachable) so RIP is generally applied to medium-sized networks, such as a campus network. RIP is not designed for complicated and large-sized networks.

RIP has two versions, RIP-1 and RIP-2. RIP-2 supports simple text authentication and MD5 authentication, as well as the variable-length sub-net masks.

To improve performance and prevent route loops, RIP supports split-horizon, poisoned reverse using triggered update. This allows the importation of routes that are obtained by other routing protocols.

Each router that runs RIP manages a database that includes route items of all reachable routers on the network. A route item includes the following information.

- **Destination address:** The address of the host or network.
- **Next-hop address:** The address of the next router through which this route passes to get to the destination.
- **Interface:** The interface where messages are forwarded.
- **Metric value:** The overhead for the router to get to the destination. It is an integer ranging from 0 to 16.
- **Timer:** The last time the route item was modified.
- **Route tag:** The tag indicates whether it is an internal routing protocol route or an external routing protocol route.

The procedure of running RIP can be described as follows:

- 1 When a specific router is starting RIP for the first time, it broadcasts request messages to the neighbor routers. After receiving the request messages, the neighbor routers respond to the request and return response messages including local routing information.
- 2 After receiving the response message, the router modifies the local routing table and sends triggered modified messages to the neighboring routers by broadcasting the route modification information. After receiving the triggered modified message, the neighboring routers forward them to their neighbors. After a series of triggered modification broadcasting, all routers can receive and maintain the latest routing information.
- 3 At the same time, RIP broadcasts the local routing table to the neighbor routers every 30 seconds. The neighbor routers receive the message and maintain the local routes. Then they select the best route to broadcast the route modification information to their neighbor networks. In this way, the updated routing information can be globally effective. Also, RIP applies a timeout mechanism to dispose of an outdated route and to make sure that the route is real-time and effective.

Though RIP is widely used by most of the router manufacturers, it has limitations:

- It supports a very limited number of routers: RIP is only suitable to small autonomous systems, such as most campus networks and local networks with simple structure and high continuity.
- The route calculations depend on a fixed metric: RIP cannot update its metric in real time to adapt to network changes. The metric defined by an administrator remains constant until it is updated artificially.
- It may cost considerable network bandwidth to update its information: RIP broadcasts an update message every 30 seconds so it may cause low efficiency in a network with a lot of nodes.

---

## Configure RIP

Begin all configuration tasks by first enabling the RIP routing process and associating a network with an RIP routing process, then configure other functional features related to RIP protocol. The task of configuring the interface-related features is not subject to whether RIP has been enabled.



*The original interface parameters become invalid after the RIP is closed.*

Configuring RIP includes tasks described in the following sections:

- Enabling RIP
- Enabling RIP at the Specified Network
- Defining a Neighboring Router
- Specifying RIP Version
- Configuring Check Zero Field of RIP Version 1
- Specifying the Status of an Interface
- Disabling Host Routes
- Enabling Route Summarization for RIP Version 2
- Configuring RIP-2 Packet Authentication on the Interface

- Configuring RIP Horizontal Segmentation on the Interface
- Configuring Route Import for RIP
- Specifying Default Route Metric Value for RIP
- Specifying Additional Route Metric Values for RIP
- Setting Route Preference
- Configuring Route Distribution for RIP
- Resetting RIP

### Enabling RIP

To enter RIP view, you must first enable RIP, then configure the parameters related to the RIP protocol. Interface-related parameters are not subject to enabling of RIP.

Perform the following configurations in system view.

**Table 469** Enabling RIP

| Operation                         | Command         |
|-----------------------------------|-----------------|
| Enable RIP and enter the RIP view | <b>rip</b>      |
| Disable RIP                       | <b>undo rip</b> |

By default, RIP is not enabled.

The parameters related to an interface are also invalid after RIP is turned off.

### Enabling RIP at the Specified Network

To flexibly control RIP operation, you can configure a corresponding network segment to RIP network so that RIP messages can be received and transmitted through the specified interface.

Perform the following configurations in RIP view.

**Table 470** Enable RIP at the Specified Network

| Operation                                      | Command                                      |
|------------------------------------------------|----------------------------------------------|
| Specify a list of networks associated with RIP | <b>network { network-number   all }</b>      |
| Delete a list of networks associated with RIP  | <b>undo network { network-number   all }</b> |

The **undo network** command is associated with RIP by default after RIP is enabled.

After enabling RIP, you must specify a list of networks with the RIP, since RIP works only on the interface of specified network segment. RIP won't receive or forward a route on interfaces of non-specified network segments, and it functions as if these interfaces do not exist. The **network-number** attribute specifies the address of the enabled or disabled network or it can designate the network address of the interfaces.

When the **network** command is used for a specified address, the interface of the network segment of this address is enabled. For example: **network 129.102.1.1**, use either the **display current-configuration** or the **display rip** command, to see network 129.102.0.0.

## Defining a Neighboring Router

RIP is a broadcast protocol. It exchanges routing information with non-broadcasting networks in unicast mode.

Perform the following configurations in RIP view.

**Table 471** Define a Neighboring Router

| Operation                                                        | Command                     |
|------------------------------------------------------------------|-----------------------------|
| Define a neighboring router                                      | <b>peer ip-address</b>      |
| Cancel exchanging routing information with a neighboring router. | <b>undo peer ip-address</b> |

By default, no neighboring routers are defined.

Normally, this command is not recommended because the node on the other end does not need to receive two identical packets at the same time. Also when a peer sends messages, it is also subject to the restrictions of such commands as **rip work**, **rip output**, **rip input** and **network**.

## Specifying RIP Version

RIP-2 has two sending modes, broadcasting and multicasting, with message multicasting as the default mode. The multicast address in RIP-2 is 224.0.0.9. The advantage of multicasting is that the host not running RIP in the network does not receive RIP broadcast messages. In addition, message multicasting can also prevent the host running RIP-1 from incorrectly receiving and processing the routes with subnet mask in RIP-2.

When RIP-1 is running on the interface, the interface receives and transmits the broadcast packets of RIP-1 and RIP-2 but does not receive RIP-2 multicast messages. When RIP-2 is running on the interface, the interface can receive and transmit RIP-1 and RIP-2 broadcast packets but cannot receive RIP-2 multicast packets. When the interface runs in RIP-2 multicast mode, it receives and transmits the RIP-2 multicast packets and does not receive the RIP-1 and RIP-2 broadcast packets.

Perform the following configurations in interface view.

**Table 472** Specify RIP Version

| Operation                                            | Command                                        |
|------------------------------------------------------|------------------------------------------------|
| Configure the interface to run RIP-1                 | <b>rip version 1</b>                           |
| Configure the interface to run RIP-2                 | <b>rip version 2 [ broadcast   multicast ]</b> |
| Restore the default RIP version run on the interface | <b>undo rip version</b>                        |

By default, the interface runs RIP-1.

## Configuring Check Zero Field of RIP Version 1

The **check zero** command is used by the router to validate the version of the RIP Version 1 message. RFC 1058 stipulates that the ZERO FIELD in the RIP Version 1 header must be set to zero. If the **checkzero** parameter is set and the router receives a message with the zero field not 0, the router will discard the RIP message because it is the wrong version.

RIP Version 2 does not have provisions for a zero field in its header so this configuration is invalid for RIP-2.

Perform the following configurations in RIP view.

**Table 473** Configure Check Zero Field of RIP Version 1

| Operation                                 | Command               |
|-------------------------------------------|-----------------------|
| Enable check zero field of RIP version 1  | <b>checkzero</b>      |
| Disable check zero field of RIP version 1 | <b>undo checkzero</b> |

RIP VERSION 1 enables zero field check by default.

### Specifying the Status of an Interface

You can specify the working status of RIP on an interface, such as whether RIP is running on the interface and whether updated messages are transmitted or received on the interface.

Perform the following configurations in interface view.

**Table 474** Specify the Status of an Interface

| Operation                                                 | Command                |
|-----------------------------------------------------------|------------------------|
| Specify running RIP on the interface                      | <b>rip work</b>        |
| Disable running RIP on the interface                      | <b>undo rip work</b>   |
| Specify receiving RIP update packets on the interface     | <b>rip input</b>       |
| Disable receiving RIP update packets on the interface     | <b>undo rip input</b>  |
| Specify sending RIP update packets on the interface       | <b>rip output</b>      |
| Disable transmitting RIP updated packets on the interface | <b>undo rip output</b> |

By default, an interface can both receive and send RIP update packets.

The **undo rip work** command is similar to **undo network** command in that the interface using either command no longer transmits an RIP route. They differ in that in **undo rip work** mode, routes of related interfaces are forwarded and in **undo network** mode, routes of related interfaces are not forwarded, as if an interface was missing.

In addition, **rip work** functions similar to the combination of two commands **rip input** and **rip output**.

### Disabling Host Routes

In some special cases, a router may receive large number of host routes from the same network segment. These routes consume lots of network resources and are of little use to route addressing. You can use the **undo host-route** command to reject the messages of the host routes.

Perform the following configurations in RIP view.

**Table 475** Disable a Host Route

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                               |                        |
|-------------------------------|------------------------|
| Disable receiving host routes | <b>undo host-route</b> |
| Enable receiving host routes  | <b>host-route</b>      |

By default, the router is enabled to receive the host routes.

### Enabling Route Summarization for RIP Version 2

Route summarization summarizes the routes of different subnets within the same natural network segment and sends the summary to other network segments as a summarized route with a natural mask. Route summarization largely reduces the network expenditure and the routing table size.

RIP-1 always sends routes with natural mask. RIP-2 supports sub-net mask and routes of unknown category. If the sub-net route needs to be broadcast, RIP-2 route summary function can be disabled.

Perform the following configurations in RIP view.

**Table 476** Enable Route Summarization

| Operation                                             | Command             |
|-------------------------------------------------------|---------------------|
| Enable automatic route summarization                  | <b>summary</b>      |
| Disable the automatic summarization function of RIP-2 | <b>undo summary</b> |

By default, RIP-2 automatic route summarization is enabled.

### Configuring RIP-2 Packet Authentication on the Interface

Authentication for packets is not supported by RIP Version 1. But RIP Version 2 supports authentication.

RIP Version 2 supports authentication in two modes: simple text authentication and MD5 authentication. Security is not ensured in simple text authentication. Simple text means that the unencrypted authentication is transmitted with the packets, therefore simple text authentication does not apply to a situation that requires a high level of security. MD5 authentication has two message formats, in compliance of the requirements of RFC1723 (RIP Version 2 Carrying Additional Information) and RFC2082 (RIP Version 2 MD5 Authentication).

3Com routers support both formats.

Perform the following configurations in interface view.

**Table 477** Configure Authentication for RIP Version 2

| Operation                                                       | Command                                                         |
|-----------------------------------------------------------------|-----------------------------------------------------------------|
| Specify a password for RIP Version 2 simple text authentication | <b>rip authentication-mode simple password</b>                  |
| Specify a key-string for RIP Version 2 MD5 authentication       | <b>rip authentication-mode md5 key-string string</b>            |
| Set the packet format type of RIP-2 MD5 authentication          | <b>rip authentication-mode md5 type [ nonstandard   usual ]</b> |
| Cancel authentication for RIP Version 2                         | <b>undo rip authentication-mode</b>                             |

By default, RIP Version 2 packets are not authenticated on an interface. If MD5 authentication type is not specified, the nonstandard authentication type is used by the router.

### Configuring RIP Horizontal Segmentation on the Interface

RIP is a Distance-Vector algorithm routing protocol. It uses the split-horizon algorithm to avoid loop routes. Split-horizon means that routes received at a certain interface are not sent to the same interface. If correct transmission of routes is more important than efficiency, then split-horizon should be disabled.

Disabling split-horizon mechanism is not effective on point-to-point connection links.

Perform the following configurations in interface view.

**Table 478** Configure RIP Horizontal Segmentation on the Interface

| Operation                                                                 | Command                       |
|---------------------------------------------------------------------------|-------------------------------|
| Configure RIP horizontal segmentation on the interface                    | <b>rip split-horizon</b>      |
| Prohibit the interface from using split-horizon when sending RIP packets. | <b>undo rip split-horizon</b> |

By default, the interface use split-horizon when sending RIP packets.

### Configuring Route Import for RIP

RIP allows importing the routes learned from other protocols.

Perform the following configurations in RIP view.

**Table 479** Configure Route Import for RIP

| Operation                         | Command                                                                 |
|-----------------------------------|-------------------------------------------------------------------------|
| Configure route import for RIP    | <b>import-route protocol [ cost cost ] [ route-policy policy-name ]</b> |
| Cancel route distribution for RIP | <b>undo import-route protocol</b>                                       |

By default, RIP does not import routes from other domains into the routing table.

The *protocol* attribute specifies the source routing domain that can be imported. At present RIP can import routes domain such as Connected, Static, OSPF, OSPF-ASE, and BGP.

See “Configure Route Import” in “Configuration of IP Routing Policy” for the details of importing routes.

### Specifying Default Route Metric Value for RIP

The **import-route** command is used to import routes of other routing protocols. If **import-route** is not followed by the value of a routing metric, then the parameter value of **default-med** command is set as the metric value when distributing other routing protocols.

Perform the following configurations in RIP view.

**Table 480** Specify a Default Route Metric Value for RIP

| Operation                                      | Command                  |
|------------------------------------------------|--------------------------|
| Specify default route metric value for RIP     | <b>default-cost cost</b> |
| Restore the default route metric value for RIP | <b>undo default-cost</b> |

By default, the default route metric for RIP is 16

Since the route metric of route import cannot be reverted, the dynamic route information may be significantly distorted. Therefore, route import is done cautiously to prevent loss of RIP protocol's performance.

### Specifying Additional Route Metric Values for RIP

The additional routing metric here is to add input or output metric for routes obtained for RIP. The `rip metricin` will add a designated metric value while receiving routes on the interface, then add this route metric value in the routing table. The `rip metricout` does not directly change the route metric value in the routing table, but will add a designated metric value when sending routes on the interface.

Perform the following configurations in interface view.

**Table 481** Specify Additional Route Metric Value for RIP

| Operation                                                                               | Command                           |
|-----------------------------------------------------------------------------------------|-----------------------------------|
| Specify additional route metric value received for RIP                                  | <code>rip metricin metric</code>  |
| Restore the additional route metric value received for RIP to its default value         | <code>undo rip metricin</code>    |
| Specify additional route metric value being advertised for RIP                          | <code>rip metricout metric</code> |
| Restore the additional route metric value being advertised for RIP to its default value | <code>undo rip metricout</code>   |

By default, the additional route metric value received for RIP is 0 but ranges from 0 to 16. Additional route metric value being advertised for RIP is 1, ranging from 1 to 16.

### Setting Route Preference

Each routing protocol has its own preference that decides which routing protocol is used to select the best route by IP route strategy. The greater the value is, the lower the preference. RIP preference can be set manually.

Perform the following configurations in RIP view.

**Table 482** Set Route Preference

| Operation                                         | Command                       |
|---------------------------------------------------|-------------------------------|
| Set the RIP route preference                      | <code>preference value</code> |
| Restore the default value of RIP route preference | <code>undo preference</code>  |

By default, the RIP route preference is 100.

### Configuring Route Distribution for RIP

Perform the following configurations in RIP view.

Configure filtering route information received by RIP.

**Table 483** Filter Routing Information Received by RIP

| Operation                                                    | Command                                                    |
|--------------------------------------------------------------|------------------------------------------------------------|
| Filter routing information received from a specified gateway | <code>filter-policy gateway prefix-list-name import</code> |

| Operation                                                                                                                                          | Command                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Change or cancel filtering the routing information received from a specified gateway                                                               | <code>undo filter-policy gateway<br/>prefix-list-name import</code>                                |
| Filter the routing information received                                                                                                            | <code>filter-policy {acl-number   ip-prefix<br/>prefix-list-name } import</code>                   |
| Change or cancel filtering routing information received                                                                                            | <code>undo filter-policy {acl-number  <br/>ip-prefix prefix-list-name } import</code>              |
| Filter routing information received from a specified gateway and the routing information received according to prefix-list                         | <code>filter-policy ip-prefix<br/>prefix-list-name gateway<br/>prefix-list-name import</code>      |
| Change or cancel filtering the routing information received from a specified gateway and the routing information received according to prefix-list | <code>undo filter-policy ip-prifix<br/>prefix-list-name gateway<br/>prefix-list-name import</code> |

Configure filtering the routing information being advertised

**Table 484** Filter the Routing Information Being Advertised by RIP

| Operation                                                           | Command                                                                                                 |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Filter the routing information being advertised.                    | <code>filter-policy { acl-number  <br/>ip-prefix prefix-list-name } export [<br/>protocol ]</code>      |
| Change or cancel filtering the routing information being advertised | <code>undo filter-policy { acl-number  <br/>ip-prefix prefix-list-name } export [<br/>protocol ]</code> |

By default, RIP does not filter any route information received or being advertised.

The `protocol` attribute specifies the routing domain that can be filtered. At present, RIP can filter routes domain such as Connected, Static, OSPF, OSPF-ASE and BGP. See "Configure Route Filter" of "Configuration of IP Routing Policy" for details.

**Resetting RIP** This command restores the router to the default RIP configuration.

Perform the following configuration in RIP view.

**Table 485** Reset RIP

| Operation | Command            |
|-----------|--------------------|
| Reset RIP | <code>reset</code> |

## Displaying and Debugging RIP

**Table 486** Display and Debug RIP

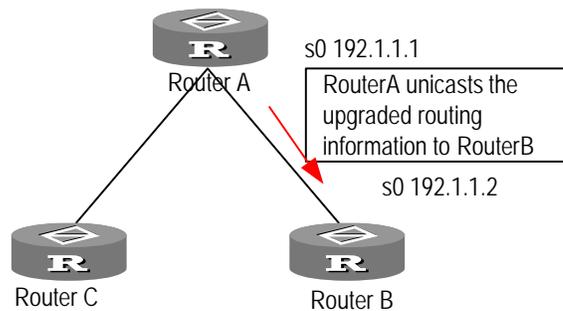
| Operation                                                                | Command                                                     |
|--------------------------------------------------------------------------|-------------------------------------------------------------|
| Display current RIP running status and global configuration information. | <code>display rip</code>                                    |
| Turn on RIP debugging information                                        | <code>debugging rip { packets   receive  <br/>send }</code> |

## RIP - Unicast Configuration Example

RIP is a broadcast protocol so it can only exchange routing information with non-broadcasting networks in unicast mode. This example shows how to configure RIP message unicasting.

Router A connects Router B and Router C with serial lines in non-broadcasting networks. Router A (192.1.1.2) only wants to send the routing updating information to the adjacent Router B (192.1.1.2) without sending the information to Router C.

**Figure 145** Networking diagram of configuring the RIP unicast



To configure RIP unicast:

**1** Configure RIP on Router A:

```
[RouterA] rip
[RouterA-rip] network 192.1.1.0
```

**2** Configure Router A's unicast peer to be Router B.

```
[RouterA-rip] peer 192.1.1.2
```

**3** Configure serial interface Serial 0

```
[RouterA-rip] interface serial 0
[RouterA-Serial0] ip address 192.1.1.1 255.255.255.0
```

## Troubleshooting RIP

No updating messages can be received when the physical connection works well.

This may have the following cause:

- RIP is not running on the corresponding interface (maybe the `undo rip work` command has been executed), or this interface is not included with the `network` command. Multicasting has been configured on the opposite router (perhaps `rip version 2 multicast` command has been executed), but not configured on the local router.

# 29

## CONFIGURING OSPF

This chapter covers the following topics:

- OSPF Overview
- Configuring OSPF
- Displaying and Debugging OSPF
- OSPF Configuration Example

---

### OSPF Overview

Open Shortest Path First (OSPF) is an autonomous, link-state-based internal routing protocol developed by Internet Engineering Task Force (IETF). The current version is version 2 (RFC1583), which features the following:

- Applicable range — Supports networks of various sizes and hundreds of routers.
- Fast convergence — Sends an update message immediately after the topological structure of the network is changed, so the change can be synchronized in the autonomous system.
- No self-loop — OSPF calculates the route with the shortest path tree algorithm through the collected link status. This algorithm ensures that no self-loop route is generated.
- Area division — An AS network can be divided into areas and the routing information between the areas is further abstracted, reducing the bandwidth occupation in the network.
- Equivalent route ----support multiple equivalent routes to the same destination address.
- Route level --- the four levels of routes according to different priorities: intra-area routes, inter-area routes, external route class 1 and external route class 2.
- Authentication ---- support interface-based message authentication to ensure the security of the route computation.
- Multicast ---packets are transmitted and received with multicast address on multicasting link layer, greatly reducing interference to other network devices.

The entire network is composed of multiple autonomous systems (AS). The link state of an AS is collected and transmitted to determine and propagate the route dynamically and then synchronize the information of the AS. Each system is divided into areas. If a router port is allocated to multiple areas, it is an area boundary router (ABR) since it is located at the boundary and connected with multiple areas. Routing information of another area can be learned from the ABR. All ABRs and the routers between them form a backbone area, tagged with

0.0.0.0. All areas must be continuous logically. Thus, a virtual link is introduced to the backbone to ensure that physically separated areas are still connected logically. The router between the ASs is called autonomous system boundary router (ASBR). Routing information, such as static routing, RIP routing, BGP routing, outside the OSPF AS can be learned from the ASBR.

Computation of the OSPF protocol is summarized as follows:

- 1 Every router supporting OSPF maintains a link state database (LSDB) for describing the topology of the entire AS. A router generates the Link State Advertisement (LSA) according to the network topology around it and sends the LSA to other routers on the network by the transmission of protocol packets. Thus, every router receives the LSA from other routers. All LSAs together forms the LSDB.
- 2 The LSA describes the network topology around a router, so the LSDB describes the topology of the whole network. A router can easily convert the LSDB into a weighted directed graph, which shows the real topology of the whole network. Obviously, each router in the autonomous system receives the same topology diagram of the network.
- 3 Each router calculates with the SPF algorithm a shortest path tree with itself as the root. This tree gives the routes to all autonomous systems. External routing information is the leaf sub-node. The external route is flagged by the router by broadcasting it to record additional information for the AS. Obviously, each router gets a different routing table.

In addition, multiple adjacent relationship lists must be created so that each router on the broadcast network and NBMA network can broadcast the local status information (such as available interface information and reachable peer information) to the whole system. Consequently, the route change of any router may be transmitted many times, which is both unnecessary and wastes bandwidth resources. To solve this problem, OSPF protocol selects a designated router (DR). All routers send information to the DR, which broadcasts the network link status. Two non-DR routers (DR Other) do not create neighboring relations with each other and do not exchange any routing information. Then the number of neighboring relations between the routers on the multi-address network is greatly reduced. The OSPF protocol supports IP subnet and the marking and receiving of external routing information. It supports interface-based message authentication to insure the security of route calculation. Messages are transmitted and received in IP multicast mode.

---

## Configuring OSPF

In all configuration tasks, the OSPF-specified interface and area number must be defined first to configure other function features. The configuration of interface-related function features is not restricted by whether OSPF has been enabled. The original interface parameters become invalid after OSPF is terminated.

OSPF configuration includes:

- Specify Router ID
- Enabling OSPF
- Associating an Area-id with the Specified Interface
- Configuring the Network Type of the OSPF Interface

- Configuring Sending Packet Cost
- Configuring a Peer for the NBMA Interface
- Specifying the Router Priority
- Specifying the Hello Interval
- Specifying the Dead Interval
- Specifying the Retransmitting Interval
- Specifying the Transmit-delay
- Configuring a Stubby Area and a Totally Stubby Area
- Configuring an NSSA Area
- Configuring Route Summarization within the OSPF Domain.
- Creating and Configuring a Virtual Link
- Configuring Authentication
- Configuring Route Import for OSPF
- Configuring Parameters when Importing External Routes
- Setting Route Preference

### Specify Router ID

Router ID is a 32-bit integral with symbol, the exclusive ID of a router in the AS. If all interfaces of the router have not been configured with IP addresses, the router ID must be configured in OSPF view, otherwise OSPF will not run.



*The modified router ID takes effect after OSPF is restarted.*

You must configure the router ID, which must be the same as the IP address of a specific interface of this router.

Perform the following configurations in system view.

**Table 487** Specify Router ID

| Operation             | Command                    |
|-----------------------|----------------------------|
| Specify the router ID | <b>router id router-id</b> |
| Delete the router ID  | <b>undo router id</b>      |

Please note when modifying the router ID, the system will display the following message:

```
OSPF: router id has changed. If you want to use new router id, reboot the router.
```

The configuration needs to be saved after the router ID is modified (execute the **save** command in system view). After restarting the router, the new router ID will take effect.

### Enabling OSPF

Perform the following configurations in system view.

**Table 488** Enable OSPF

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                                          |                         |
|------------------------------------------|-------------------------|
| Enable OSPF and enter into the OSPF view | <b>ospf enable</b>      |
| Turn off OSPF                            | <b>undo ospf enable</b> |

By default, OSPF is disabled.

### Associating an Area-id with the Specified Interface

The OSPF protocol divides the autonomous system into areas. An area is the logical group of the router. Some routers belong to different areas (called area boundary router ABR), while a network segment can only be in one area. In other words, each interface running the OSPF protocol must be put in a specific area. The area is flagged with an area ID. The ABR transmits routing information between areas.

In addition, in the same area, all routers must agree unanimously to the parameter configurations of this area. So, in the configuration of routers in the same area, most configuration data must be considered on the basis of this area. Incorrect configurations make it impossible for adjacent routers to transfer information to each other, or can even lead to the blocking or self-loop of routing information.

Perform the following configurations in interface view.

**Table 489** Associate an Area-id with the Specified Interface which runs OSPF

| Operation                                                                  | Command                              |
|----------------------------------------------------------------------------|--------------------------------------|
| Specify an area-id associated with the specified interface which runs OSPF | <b>ospf enable area area-id</b>      |
| Delete an area-id associated with the specified interface                  | <b>undo ospf enable area area-id</b> |

No area-id is associated with the specified interface by default after OSPF is enabled.

After OSPF is enabled, you must specify an area-id associated with the specified interface. OSPF only works on the specified interface.

### Configuring the Network Type of the OSPF Interface

The OSPF protocol calculates the route on the basis of the topological structure of the neighboring network of this router. Each router describes the topology of its neighboring network and transmits this information to all other routers.

OSPF divides the network into 4 types according to the link layer protocols:

- When the link layer is Ethernet, OSPF regards the network type as broadcast by default.
- When the link layer protocol is frame relay, HDLC and X.25, OSPF regards the network type as NBMA by default.
- No link layer protocol is considered as point-to-multipoint type by default. It is usually manually modified from NBMA if the NBMA network is not wholly interconnected.
- When the link layer protocol is PPP, LAPB, OSPF regards the network type as point-to-point by default.

NBMA is a Non Broadcast Multi Access network. The typical network is X.25 and frame relay. Configure the poll-interval to specify the period for sending a polling

hello packet before this interface sets up neighboring relations with the adjacent routers.

The interface can be configured into **nbma** mode on the broadcast network without multi-access capability.

If not all routers are inter-reachable on NBMA network, the interface can be configured into **p2mp** mode.

If the router has only one opposite terminal in NBMA network, the interface can also be changed to **p2p** mode.

The difference between an NBMA network and a point-to-multipoint network includes the following distinctions:

- In the OSPF protocol, NBMA refers to those as fully connected, nonbroadcast and multi-access networks. But point-to-multipoint network does not necessarily require full connection.
- DR and BDR should be elected on NBMA while there is no DR or BDR on point-to-point network.
- NBMA is a default network type. For example, if the link layer protocol is X.25 or frame relay, OSPF regards the network type of this interface as NBMA (whether the network is wholly connected). Point-to-multipoint is not a default network type. No link layer protocol can be considered as a point-to-multipoint protocol because it must be a modification from other network types. The most common practice is to change the not fully connected NBMA to a point-to-multipoint network.
- An NBMA network sends messages in unicast mode and the peer must be configured manually. In point-to-multipoint network, messages are sent either in unicast mode or in multicast mode.

Perform the following configurations in interface view.

**Table 490** Configure the Network Type of the OSPF Interface

| Operation                                        | Command                                                               |
|--------------------------------------------------|-----------------------------------------------------------------------|
| Configure the network type of the OSPF interface | <code>ospf network-type { broadcast   nbma   p2mp   p2p }</code>      |
| Delete the specified OSPF network type           | <code>undo ospf network-type { broadcast   nbma   p2mp   p2p }</code> |

After a new OSPF network type is configured, the old network type on the interface will be replaced automatically.

### Configuring Sending Packet Cost

You can configure the cost of sending a packet on the interface, otherwise OSPF automatically calculates the cost value according to the baud rate of the current interface.

Perform the following configurations in interface view.

**Table 491** Configure Sending Packet Cost

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                               |                       |
|-------------------------------|-----------------------|
| Configure sending packet cost | <b>ospf cost cost</b> |
| Reset the sending packet cost | <b>undo ospf cost</b> |

The default value of the cost of sending a packet on the interface is calculated automatically according to the interface baud rate as follows:

The default value is automatically calculated according to interface baud rate.

- If the baud rate is less than 2000 bps, 2000 is taken, and the overhead value is  $100000000/2000=50000$ .
- If the baud rate is greater than 100000000 bps, 100000000 is taken, and the overhead value is  $100000000/100000000=1$ .
- If the baud rate is between 2000 bps and 100000000bps, the overhead value is the result of  $100000000/\text{interface rate}$ .

### Configuring a Peer for the NBMA Interface

Special configuration is needed for the network of an NBMA interface. Since the adjacent router cannot be found by broadcasting hello packets, the IP address of the adjacent router should be specified manually for the interface, as well as whether the adjacent router has a voting right. This is specified with the **ospf peer ip-address [eligible]** command. To use the eligible attribute, this adjacent router must have no voting right.

On X.25 and frame relay networks, you can configure a map to make the whole network fully connected so there is a virtual circuit between any two routers on the network and they are directly reachable. Then OSPF can process like a broadcast network. The IP address of the adjacent router, and whether it has a voting right, must be specified manually for the interface because the adjacent router cannot be found dynamically by broadcasting hello packets.

Perform the following configurations in interface view.

**Table 492** Configuring a Peer for the NBMA Interface

| Operation                                  | Command                                |
|--------------------------------------------|----------------------------------------|
| Configure a peer for NBMA interface        | <b>ospf peer ip-address [eligible]</b> |
| Cancel or delete a peer for NBMA interface | <b>undo ospf peer ip-address</b>       |

By default, no peer of the NBMA interface is specified.

When you configure the peer of the NBMA interface, the following items are necessary:

- The configured hello timer and dead timer between neighbors must be identical.
- The configured link route type between neighbors must be identical.
- The area number that neighbors belong to must be identical.
- The authentication mode (simple text or MD5), authentication password, and key-id of the area that neighbors belong to must be identical.
- The configured stub attribute of the areas including the neighbors must be consistent.

## Specifying the Router Priority

It is necessary to establish the peer relationship manually between interfaces for multi-point access network, (NBMA and broadcast type networks). But establishing peer relationship occupies large amounts of system resources when there are hundreds of routers in the network. To resolve this issue, OSPF specifies a “designated router” (DR). All routers within the same network segment send the relationship information to the DR, which broadcasts the link status of each network segment. In this way, the number of the peer relationships between different routers on the multi-access network is significantly reduced.

The priority of a router interface determines the qualifications of the interface in voting for the DR. The interface with a higher priority is considered first when the voting rights conflict.

The DR is not designated manually, but voted by all routers in the local network segment. The routers of Priority>0 in the local network segment can be used as the “candidates”. The router with the greatest priority value is selected among all routers that claim to be DR. If two routers have the same priority, the one with greater router ID is selected. Routers vote by Hello packet. Each router writes the DR into the Hello packet and sends it to all other routers on the network segment. When two routers in the same network segment claim to be the DR, the one with the higher priority is chosen. If the priorities are equivalent, the one with higher router ID is chosen. If the priority of a router is 0, it is not selected as the DR or “backup designated router” (BDR).

If a DR fails due to a specific fault, a new DR must be elected, with synchronization. This can take a long time, during which, the route calculation is not correct. To shorten the process, OSPF puts forward the concept of the “backup designated router” (BDR). The BDR is actually a standby for the DR and is voted together with DR. The BDR also creates relations with all neighboring routers in the network segment and exchanges routing information with them. When the DR fails, the BDR becomes the DR immediately without the need for re-election. Because the neighboring relationship is already created, this takeover process is instantaneous. Of course a new BDR needs to be elected again but during the election, the route calculation is not affected.

It should be noted that:

- The DR in the network segment is not necessarily the router with the highest priority. Similarly, the BDR is not necessarily the router with the second highest priority.
- The DR is a role in a single network segment, based on the router interface. A router can be a DR on one interface and a BDR or DROther on another interface.
- The DR is elected on a broadcast interface or NBMA interface. It is not necessary on a point-to-point interface or point-to-multipoint interface.

Perform the following configurations in interface view.

**Table 493** Specify the Router Priority

| Operation                                                            | Command                       |
|----------------------------------------------------------------------|-------------------------------|
| Set the priority of the interface when selecting a designated router | <b>ospf dr-priority value</b> |
| Return to the default router priority                                | <b>undo ospf dr-priority</b>  |

### Specifying the Hello Interval

The Hello packet is periodically sent to the neighboring router to find and maintain OSPF neighbor relationship, and to elect the DR and BDR in the NBMA and broadcast networks. When one router is started, it only sends hello packets to the neighbors whose precedences are larger than 0, that is, the routers can possibly be elected as DR or BDR. You can configure the interval for sending hello packets. If the interval is too short, the network change can be easily found but the network load will be greatly increased. An appropriate value must be selected for the specific network conditions.

On NBMA and point-to-multipoint networks, the *poll-interval* attribute should be configured to specify the period of sending polling hello packet before this interface sets up a neighbor relationship with the adjacent routers.

The *poll-interval* attribute must be at least 3 times the value for *hello-timer*.

Perform the following configurations in interface view.

**Table 494** Specify Hello Interval

| Operation                                                                        | Command                               |
|----------------------------------------------------------------------------------|---------------------------------------|
| Set the time interval for the interface to send hello packets                    | <code>ospf timer hello seconds</code> |
| Return to the default hello interval time                                        | <code>undo ospf timer hello</code>    |
| Specify the length of poll-interval on NBMA and point-to-multipoint network type | <code>ospf timer poll seconds</code>  |
| Return to the default poll interval time                                         | <code>undo ospf timer poll</code>     |

By default, the hello-timer on the **p2p** interface is 10 seconds and the hello timer on the **p2mp** and **nbma** interfaces on the same network segment must be identical.

### Specifying the Dead Interval

The expiration time of a neighboring router means that if a hello packet of the neighbor router (peer) is not received within a certain period, the neighbor router is invalid. You can specify the dead-timer, the period where the peer route fails. The value of the dead-timer must be at least 4 times the value of the hello-timer.

Perform the following configurations in interface view.

**Table 495** Specify Dead Interval

| Operation                                            | Command                              |
|------------------------------------------------------|--------------------------------------|
| Specify the expiration duration of the OSPF neighbor | <code>ospf timer dead seconds</code> |
| Return to the default value of dead interval         | <code>undo ospf timer dead</code>    |

By default, the dead-timer on the **p2p** interface is 40 seconds and on **p2mp** and **nbma** interface the dead-timer is 120 seconds, ranging from 1 to 65535 seconds.

Note that:

- The dead-timer of the router on the same network segment must be the same.
- When you modify the network type, the hello-timer and dead-timer are both restored to their default values.

## Specifying the Retransmitting Interval

The router waits for confirmation from the neighbor to whom it has sent an LSA. If the router does not receive the neighbor's confirmation after a specified interval, the retransmitting interval, it resends the LSA. You can set the time interval for re-transmitting an LSA.

Perform the following configurations in interface view.

**Table 496** Specify Retransmitting Interval

| Operation                                                                | Command                                    |
|--------------------------------------------------------------------------|--------------------------------------------|
| Configure the interval of LSA retransmission for the neighboring routers | <code>ospf timer retransmit seconds</code> |
| Return to the default value of re-transmitting interval                  | <code>undo ospf timer retransmit</code>    |

By default, the retransmitting interval is 5 seconds.

The retransmitting interval must be twice of the period when a message is transmitted between two routers.



The interval for retransmitting an LSA between adjacent routers must not be so small as to cause unnecessary retransmission.

## Specifying the Transmit-delay

The LSA ages in the link status database (LSDB) of the local router (1 is added per second), but not during the process of network transmission. Therefore, it is necessary to add the aging time before the transmission. Set and adjust this parameter according to the actual situation in the low-speed network.

Perform the following configurations in interface view.

**Table 497** Specify Transmit-delay

| Operation                                  | Command                               |
|--------------------------------------------|---------------------------------------|
| Set the delay time of LSA transmission     | <code>ospf trans-delay seconds</code> |
| Return the default value of transmit-delay | <code>undo ospf trans-delay</code>    |

By default, the time for transmit-delay is 1 second.

## Configuring a Stubby Area and a Totally Stubby Area

Usually, OSPF has 5 kinds of LSA packets, as follows:

- **Router-LSA:** Generated by each router and transmitted to the whole area, describing link status and cost of the router.
- **Network-LSA:** Generated by the DR and transmitted to the whole area, describing the link status of local network segment.
- **Net-Summary-LSA:** Generated by the ABR and transmitted to relevant areas, describing routing of certain network segment of the area.
- **Asbr-Summary-LSA:** Generated by the ABR and transmitted to relevant area, describing routing to ASBR.
- **AS-External-LSA:** Generated by the ASBR and transmitted to the whole AS (excluding the Stub area), describing routing to AS external.

A "stub area" is the area that does not advertise the received external LSA, inside which the scale of the routing table and the quantity of the transmitted routing

information is reduced greatly. A default routing (0.0.0.0) is generated for the area by the ABR of the area to insure that these routes are reachable. A stub area is an optional configured attribute, but it does not mean that each area is configurable. Usually, a stub area is located at the boundary of the AS. A non-backbone area with only one ABR or multi-ABR that are not virtually connected between ABRs can be configured as a stub area.

A "totally stubby area" is the area that does not receive Type-3, Type-4, and Type-5 LSA (excluding Type-3 LSA which contains default routing and is generated by the ABR). Inside such areas, there is no route to the outside and other areas of the AS, so the scale of the routing table and the quantity of the transmitted routing information is less.

A totally stubby area is also an optional configured attribute with the configuration conditions that are the same as those of stub areas.

When a stubby area or totally stubby area is configured, the following must be noted:

- The backbone area cannot be configured as a stubby area or totally stub area and the virtual connection cannot pass through a stubby area or totally stub area.
- If one area is configured as stubby area or totally stub area, all routers in this area must be configured with this attribute.
- An ASBR cannot be inside a stubby area or a totally stub area, which means that the exterior route of the AS cannot be transferred to the area.

Perform the following configuration under OSPF view:

**Table 498** Configure Totally Stubby Area of OSPF

| Operation                                                                | Command                                                      |
|--------------------------------------------------------------------------|--------------------------------------------------------------|
| Define an area as stub area or totally stub area and specify cost value. | <code>stub cost cost area area-id [ no-summary ]</code>      |
| Cancel Stub Area                                                         | <code>undo stub cost cost area area-id [ no-summary ]</code> |

By default, no stubby area or totally stub area is configured. The cost of the default routing sent to Stub area is 1.

The area is configured of totally stub area when **no-summary** option is selected

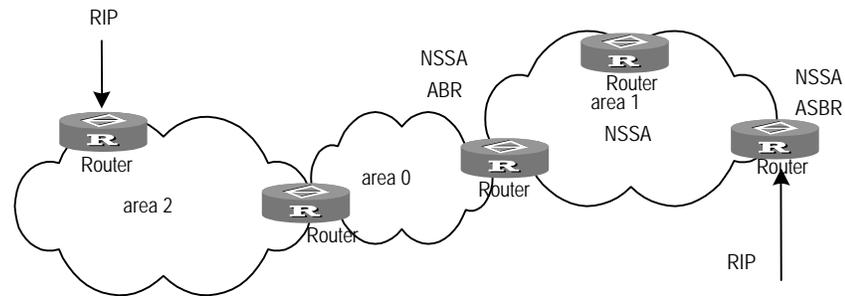
**Configuring an NSSA Area**

NSSA areas are areas that can import external routing by itself and advertise in the AS, but cannot accept external routing generated by another area in the AS. Actually an NSSA area is one form of a stub area, which can conditionally import AS external routing. A new area-NSSA Area and a new LSA-NSSA LSA (or called Type-7 LSA) are added in the RFC1587 OSPF NSSA Option.

The NSSA and stub area are similar in many ways. Neither of them generates or redistributes an AS-External-LSA (namely Type-5 LSA), and both of them can generate and import a Type-7 LSA. Type-7 LSA is generated by the ASBR in an NSSA area, which can only advertise in an NSSA area. When a Type-7 LSA reaches the ABR of an NSSA, the ABR selects whether to transform the Type-7 LSA into an AS-External-LSA to advertise to other areas.

In the following group network, an AS operating the OSPF protocol includes three areas, area 1, area 2, and area 0. Area 0 is the backbone area. The other ASs operate RIP. Area 1 is defined as an NSSA area. After an RIP route advertises to the NSSA ASBR that generates a Type-7 LSA and propagates in Area 1. After the Type-7 LSA reaches the NSSA ABR, it is transformed into a Type-5 LSA that is advertised to Area 0 and Area 2. The RIP route is generated as a Type-5 LSA and propagated in the OSPF AS by the ASBR of Area 2. This Type-5 LSA will not reach Area 1 because Area 1 is an NSSA area. On this point, an NSSA area and a stub area are the same.

**Figure 146** Schematic Diagram of an NSSA Area



Perform the following configuration in OSPF view:

**Table 499** Configure an NSSA Area of OSPF

| Operation                       | Command                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------|
| Configure an area as NSSA area  | <code>nssa area area-id [ default-route-advertise ] [ no-import-route ] [ no-summary ]</code> |
| Cancel the configured NSSA area | <code>undo nssa area area-id</code>                                                           |

By default, no area is configured as an NSSA area.

The `default-route-advertise` attribute generates default a Type-7 LSA. A Type-7 LSA default route is generated on the ABR no matter whether there is a default route 0.0.0.0 in the routing table while applying this parameter. A Type-7 LSA default route is only generated on an ASBR when there is a default route 0.0.0.0 in the routing table.

The `no-import-route` attribute is used on the ASBR, which allows the OSPF route that is imported using the `import-route` command, to not be advertised to the NSSA area. If the NSSA router is both ASBR and ABR, this parameter option is always selected.

**Configuring Route Summarization within the OSPF Domain.**

Route summary provides that the routing information is processed in the ABR. Only one route is sent to other areas for the network segment configured with summary. One area can be configured with multiple summary network segments so that OSPF can summarize multiple network segments. When the ABR sends routing information to other areas, Sum\_net\_Lsa (Type 3 LSA) is generated for each network segment. If there are some continuous network segments in the area, they can be summarized into one network segment with a range command. Then the ABR only sends one summary LSA and all other LSAs in the summary network segment range specified with this command are not sent separately,

which reduces the LSDB in other areas. The configuration of range is only effective when it is configured on the ABR in the stub area.

For example, there are two network segments in an area as follows:

```
202.38.160.0 255.255.255.0
```

```
202.38.180.0 255.255.255.0
```

They are summarized into one network segment: 202.38.0.0 255.255.0.0

When the summary network segment of a specific network is added to an area, the internal routes with the IP addresses that fall in this summary network segment are not broadcast separately to other areas. Only the abstract information of the route of the whole summary network segment is broadcast. If the network segment range is restricted with the **notadvertise** attribute, the abstract information to this network segment route is not broadcast. This network segment is described in the form of an IP address/mask. Receiving the summary network segment and the restriction of the network segment can reduce the inter-area routing information.

Note that the route summary is only effective when configured on an ABR.

Perform the following configurations in OSPF view.

**Table 500** Configure Route Summarization Within OSPF Domain.

| Operation                                         | Command                                                                        |
|---------------------------------------------------|--------------------------------------------------------------------------------|
| Configure route summarization within OSPF domain. | <b>abr-summary address mask mask area area-id [ advertise   notadvertise ]</b> |
| Cancel route summary between areas                | <b>undo abr-summary address mask mask area area-id</b>                         |

By default, inter-area routes are not summarized.

It must be noted that a routing summary configuration is only valid on the ABR.

### Creating and Configuring a Virtual Link

After the OSPF area division, all the areas may not be of equal size. One particular area is unique and that is the backbone area with the area-id of 0.0.0.0. OSPF route update between non-backbone areas is carried out through the backbone area. The OSPF protocol requires that all non-backbone areas be connected to backbone areas and at least one port on an ABR must be in the area 0.0.0.0. If there is no physical connection between an area and the backbone area 0.0.0.0, a virtual link must be created.

If a physical connection is not possible due to the limitation of the network topology, a virtual link can satisfy this requirement. *Virtual link* refers to a logical connection channel between two ABRs that is created through an area of non-backbone area internal routes. Both ends of the virtual link must be ABRs and both ends must be configured at the same time so that the virtual link can take effect. A virtual link is flagged with the ID of the opposite router. The area providing the non-backbone internal route for both ends of the virtual connection is called a *transit area*, whose area-id must also be specified.

The virtual link is activated after the route through the transit area is calculated. It is equivalent to a point-to-point connection between two terminals. Parameters can be configured for this connection like a physical interface, such as sending a hello-timer.

A “logic channel” is provided for multiple routers running OSPF that forwards messages between two ABRs. Since the destination addresses of the protocol messages are not these ABRs, the messages are transparent to them and they are transmitted as ordinary IP messages, while routing information is transmitted directly between the two ABRs. Routing information here means an LSA of Type3 that is generated by ABR. The synchronization of routers in the area is not changed.

When configuring a backbone area, note that:

- The backbone area is responsible for advertising the routing information of the non-backbone area. If the AS is divided into more than one area, one area must be the backbone area, and other areas must be connected with the backbone area directly or logically.
- The backbone area must include all ABRs, and may include routers belonging to the backbone area only. An ASBR may not be inside the backbone area.
- ABRs inside the backbone area must be well connected, and may be connected physically or logically (establishing virtual connection between ABRs).

When configuring a virtual connection, note that:

- A virtual connection can only span one area, which means that the non-backbone area can establish virtual connection with the backbone area only by spanning one other non-backbone area.
- Multiple virtual connections can be connected in series to form a new virtual connection.

Perform the following configurations in OSPF view.

**Table 501** Create and Configuring a Virtual Link

| Operation                           | Command                                                                                                                                                         |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create and configure a virtual link | <code>vlink peer-id router-id transit-area area-id [ hello-timer seconds ] [ retransmit-timer seconds ] [ transit-delay seconds ] [ dead-timer seconds ]</code> |
| Delete the specified virtual link   | <code>undo vlink peer-id router-id transit-area area-id</code>                                                                                                  |

By default, there is no virtual link is created. The attributes for this command have the following default values:

- **area-id**: None
- **router-id**: None
- **hello-timer**: 10 seconds
- **retransmit-timer**: 5 seconds
- **transit-delay**: 1 second

- **dead-timer:** 40 seconds

### Configuring Authentication

OSPF supports simple text authentication and MD5 authentication between adjacent routers.

Perform the following configurations in interface view.

**Table 502** Configure Authentication

| Operation                                                 | Command                                           |
|-----------------------------------------------------------|---------------------------------------------------|
| Specify a password for OSPF simple text authentication    | <b>ospf authentication-mode simple password</b>   |
| Specify the string and key-id for OSPF MD5 authentication | <b>ospf authentication-mode md5 string key-id</b> |
| Cancel authentication on the interface                    | <b>undo ospf authentication-mode</b>              |

By default, the interface does not authenticate OSPF packets.

The maximum length of a password for plain text authentication is 8 characters and for a MD5 string authentication the maximum length of the password is 16 characters. The **key-id** attribute is the key value of MD5 authentication, ranging from 1 to 255.

Note that the configured packet authentication mode, authentication password, and the key-id on the router interface in the same network segment must be consistent.

### Configuring Route Import for OSPF

The dynamic routing protocols on the routers can share routing information. Due to OSPF features, the routes found by other routing protocols are always regarded as the routes outside the AS in processing. In the receiving command, the cost type of the route, cost value, and flag can be specified to overlap default routing parameters.

OSPF uses 4 different route types, whose sequence runs:

- Intra-area route — The route in an area of the AS.
- Inter-area route — The route between different areas of the AS.
- External router Type 1— The received IGP route (such as RIP, STATIC). The reliability of this route is high, so the calculated cost of the external route and the cost of the route inside the AS are in the same numeric level. It is comparable with the cost of OSPF route, i.e. the cost value of external route Type 1 = the cost value from the local router to the corresponding ASBR + the cost value from ASBR to the destination address of the route.
- External router Type 2 — The received EGP route. Due to the concerns of poor reliability of this route, the OSPF protocol considers the cost from the ASBR to outside the AS as much as, or more than, the cost to the ASBR within the AS. Therefore, mainly the former is considered in the calculation of route cost, i.e. the cost value to the external route Type 2 = the cost values from the ASBR to the route destination address. If the values are equal, consider the cost value from the local router to the corresponding ASBR.

Perform the following configurations in OSPF view.

**Table 503** Configure Route Import for OSPF

| Operation                          | Command                                                                                                             |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Configure route import for OSPF    | <code>import-route protocol [ cost cost ] [ type 1   2 ] [ tag tag-value ] [ route-policy policy-name ]</code>      |
| Cancel route distribution for OSPF | <code>undo import-route protocol [ cost cost ] [ type 1   2 ] [ tag tag-value ] [ route-policy policy-name ]</code> |

By default, OSPF does not import routes from other domains into the routing table.

The **protocol** attribute specifies the source routing domain that can be imported. At present, OSPF can import routes domain such as connected, static, RIP, and BGP.

See “Configuring Route Import for OSPF” for the details of routing import.

### Configuring Parameters when Importing External Routes

When the routes found by other routing protocols on the router are received by OSPF as the external routing information of its own AS, some other parameters are needed, including the default cost and default tag of the route. Router tag can be used to identify the information related to the protocol, such as the number OSPF uses as the AS number when receiving BGP protocol.

OSPF specifies two types of cost selection modes of external routing information in the protocol. You can configure receiving the default cost type of the route.

Perform the following configurations in OSPF view.

**Table 504** Configure Parameters When Importing External Routes

| Operation                                                               | Command                                                 |
|-------------------------------------------------------------------------|---------------------------------------------------------|
| Configure the default cost value when OSPF importing external routes    | <code>default import-route cost cost</code>             |
| Return to the default cost value when OSPF importing external routes    | <code>undo default import-route cost</code>             |
| Configure the interval for OSPF importing external routes               | <code>default import-route interval seconds</code>      |
| Return to the default interval value for OSPF importing external routes | <code>undo default import-route interval seconds</code> |
| Configure the upper limit of routes that OSPF can import                | <code>default import-route limit routes</code>          |
| Restore default value of routes that OSPF can import                    | <code>undo default import-route limit</code>            |
| Configure the default tag value when OSPF importing external routes     | <code>default import-route tag tag</code>               |
| Return to the default tag value when OSPF importing external routes     | <code>undo default import-route tag</code>              |
| Configure the default type when OSPF importing external routes          | <code>default import-route type { 1   2 }</code>        |
| Return to the default route type when OSPF importing external routes    | <code>undo default import-route type</code>             |

By default, the cost value is 1, and the tag value is 1. The imported route is external route Type 2, the interval of importing external route is 1 second and at most 150 external routes can be imported in each interval.

### Setting Route Preference

Multiple dynamic routing protocols may be executed on the router at the same time, the problem of information sharing and selection between the routing protocols can occur. The system sets a priority for every routing protocol. When several protocols find the same route, the protocol with higher priority will supercede.

Perform the following configurations in OSPF view.

**Table 505** Set Route Preference

| Operation                                         | Command                         |
|---------------------------------------------------|---------------------------------|
| Specify OSPF route preference                     | <b>preference [ ase ] value</b> |
| Return the default value of OSPF route preference | <b>undo preference [ ase ]</b>  |

By default, OSPF route preference is 10. The preference of the imported external routing protocol is 150.

### Configuring a Route Filter for OSPF

Perform the following configurations in OSPF view.

Configure filtering route information received by OSPF.

**Table 506** Filter the Routing Information Received by OSPF

| Operation                                               | Command                                     |
|---------------------------------------------------------|---------------------------------------------|
| Filter the routing information received                 | <b>filter-policy acl-number import</b>      |
| Change or cancel filtering routing information received | <b>undo filter-policy acl-number import</b> |

By default, OSPF does not filter any route information received.

### Displaying and Debugging OSPF

**Table 507** Display and Debug OSPF

| Operation                                  | Command                                                                                                                                                                         |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display OSPF main information              | <b>display ospf</b>                                                                                                                                                             |
| Display OSPF external routing information  | <b>display ospf ase [ retranse ]</b>                                                                                                                                            |
| Display OSPF statistic information         | <b>display ospf cumulative</b>                                                                                                                                                  |
| Display OSPF LSDB information              | <b>display ospf database [ retranse ]</b>                                                                                                                                       |
| Display OSPF error information             | <b>display ospf error</b>                                                                                                                                                       |
| Display OSPF interface information         | <b>display ospf interface<br/>interface-type interface-number</b>                                                                                                               |
| Display OSPF LSDB detailed information     | <b>display ospf lsa [ router_lsa  <br/>net_lsa   sumnet_lsa   asbr_lsa  <br/>external_lsa   nssa_external_lsa  <br/>adv_rtr   self_originate   ls_id ] [<br/>area area-id ]</b> |
| Display OSPF neighboring point information | <b>display ospf peer</b>                                                                                                                                                        |
| Display OSPF nexthop information           | <b>display ospf nexthop</b>                                                                                                                                                     |

| Operation                                        | Command                                                                                                 |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Display OSPF routing table information           | <code>display ospf routing</code>                                                                       |
| Display the information about OSPF virtual links | <code>display ospf vlink</code>                                                                         |
| Turn on the OSPF debugging packet switches       | <code>debugging ospf { event   packet [ ack   dd   hello   request   update ]   lsa   spf }</code>      |
| Turn off the OSPF debugging packet switches      | <code>undo debugging ospf { event   packet [ ack   dd   hello   request   update ]   lsa   spf }</code> |

### OSPF Configuration Example

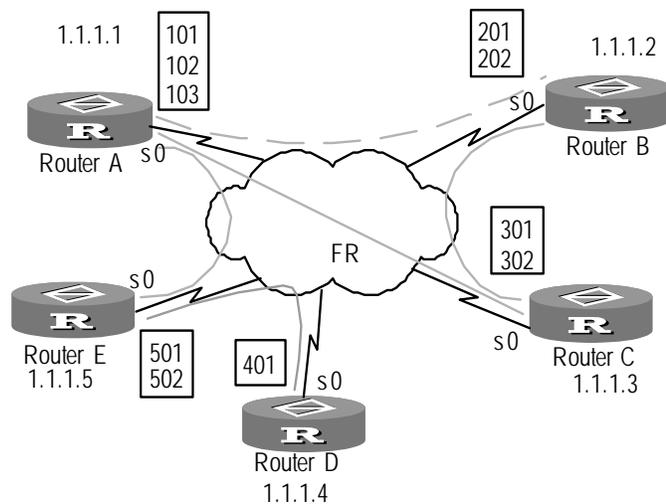
This section describes several different configurations of OSPF with a suggested procedure for each configuration

#### Configuring OSPF on the Point-to-Multipoint Network.

The configuration for this example includes the following features:

- Router A communicates with Router B through DLCI 101, communicates with Router C through DLCI 102, and communicates with Router E through DLCI 103.
- Router B communicates with Router A through DLCI 201 and communicates with Router C through DLCI 202.
- Router C communicates with Router A through DLCI 301 and communicates with Router B through DLCI 302.
- Router D communicates with Router E through DLCI 401.
- Router E communicates with Router A through DLCI 501 and communicates with Router D through DLCI 502.

**Figure 147** Networking diagram of running OSPF on point-to-multipoint interface



To configure OSPF on the point-to-multipoint network

- 1 Configure Router A:
  - a Configure the ip address of interface Serial0, encapsulated into frame relay and configure frame relay mapping table.

```
[RouterA] interface serial 0
[RouterA-Serial0] ip address 1.1.1.1 255.0.0.0
[RouterA-Serial0] link-protocol fr
[RouterA-Serial0] fr map IP 1.1.1.2 dlci 101 broadcast
[RouterA-Serial0] fr map IP 1.1.1.3 dlci 102 broadcast
[RouterA-Serial0] fr map IP 1.1.1.4 dlci 103 broadcast
```

**b** Enable OSPF

```
[RouterA-Serial0] quit
[RouterA] router id 1.1.1.1
[RouterA] ospf enable
[RouterA-ospf] quit
```

**c** Configure the area-id of the interface and the interface type

```
[RouterA] interface serial 0
[RouterA-Serial0] ospf enable area 0
[RouterA-Serial0] ospf network-type p2mp
[RouterA-Serial0] ospf peer 1.1.1.2
[RouterA-Serial0] ospf peer 1.1.1.3
[RouterA-Serial0] ospf peer 1.1.1.4
```

**2** Configure Router B:

**a** Configure the ip address of interface Serial0, encapsulated into frame relay and configure frame relay mapping table.

```
[RouterB] interface serial 0
[RouterB-Serial0] ip address 1.1.1.2 255.0.0.0
[RouterB-Serial0] link-protocol fr
[RouterB-Serial0] fr map ip 1.1.1.1 dlci 201 broadcast
[RouterB-Serial0] fr map ip 1.1.1.3 dlci 202 broadcast
```

**b** Enable OSPF

```
[RouterB-Serial0] quit
[RouterB] router id 2.2.2.2
[RouterB] ospf enable
[RouterB-ospf] quit
```

**c** Configure the area-id of the interface and the interface type

```
[RouterB] interface serial 0
[RouterB-Serial0] ospf enable area 0
[RouterB-Serial0] ospf network-type p2mp
[RouterB-Serial0] ospf peer 1.1.1.1
[RouterB-Serial0] ospf peer 1.1.1.3
```

**3** Configure Router C:

**a** Configure the ip address of interface Serial0, encapsulated into frame relay and configure frame relay mapping table.

```
[RouterC] interface serial 0
[RouterC-Serial0] ip address 1.1.1.3 255.0.0.0
[RouterC-Serial0] link-protocol fr
[RouterC-Serial0] fr map IP 1.1.1.1 dlci 301 broadcast
[RouterC-Serial0] fr map IP 1.1.1.2 dlci 302 broadcast
```

**b** Enable OSPF

```
[RouterC-Serial0] quit
[RouterC] router id 3.3.3.3
[RouterC] ospf enable
```

- c Configure the area-id of the interface and the interface type

```
[RouterC-ospf] quit
[RouterC] interface serial 0
[RouterC-Serial0] ospf enable area 0
[RouterC-Serial0] ospf network-type p2mp
[RouterC-Serial0] ospf peer 1.1.1.1
[RouterC-Serial0] ospf peer 1.1.1.2
```

- 4 Configure Router D:

- a Configure the ip address of interface Serial0, encapsulated into frame relay and configure frame relay mapping table.

```
[RouterD] interface serial 0
[RouterD-Serial0] ip address 1.1.1.4 255.0.0.0
[RouterD-Serial0] link-protocol fr
[RouterD-Serial0] fr map IP 1.1.1.5 dlci 401 broadcast
```

- b Enable OSPF

```
[RouterD] router id 4.4.4.4
[RouterD] ospf enable
[RouterD-ospf] quit
```

- c Configure the area-id of the interface and the interface type

```
[RouterD-Serial0] ospf enable area 0
[RouterD-Serial0] ospf network-type p2mp
[RouterD-Serial0] ospf peer 1.1.1.5
```

- 5 Configure Router E:

- a Configure the ip address of interface Serial0, encapsulated into frame relay and configure frame relay mapping table.

```
[RouterE] interface serial 0
[RouterE-Serial0] ip address 1.1.1.5 255.0.0.0
[RouterE-Serial0] link-protocol fr
[RouterE-Serial0] fr map IP 1.1.1.1 dlci 501 broadcast
[RouterE-Serial0] fr map IP 1.1.1.4 dlci 502 broadcast
```

- b Enable OSPF

```
[RouterE-Serial0] quit
[RouterE] router id 5.5.5.5
[RouterE] ospf enable
```

- c Configure the area-id of the interface and the interface type

```
[RouterE-ospf] quit
[RouterE] interface serial 0
[RouterE-Serial0] ospf enable area 0
[RouterE-Serial0] ospf network-type p2mp
[RouterE-Serial0] ospf peer 1.1.1.1
[RouterE-Serial0] ospf peer 1.1.1.4
```

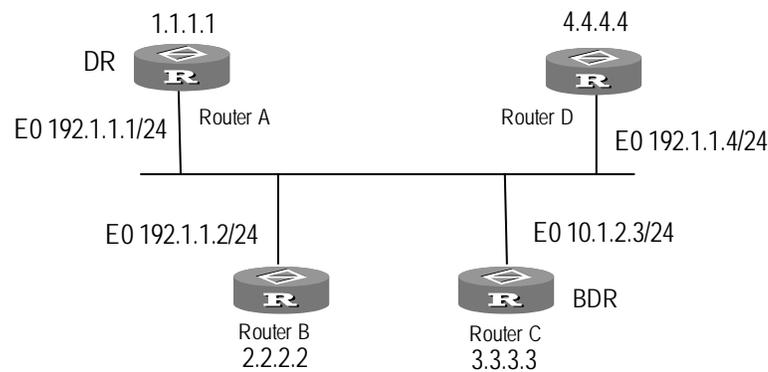
## Configure DR on OSPF Preference

### I. Networking requirement

The following example describes the configuration of route preference of several routers in an OSPF autonomous system. The preference of Router A is 100, the highest on the network, therefore Router A is selected as DR. Router C is of the second highest priority, therefore is chosen as BDR. The preference of Router B is 0, which means that it cannot be a DR. Router D has no preference, so the default value 1 is taken.

## II. Networking diagram

**Figure 148** Networking diagram of configuring “DR” selection of OSPF preference



## III. Configuration procedure

### 1 Configure Router A:

```
[RouterA] interface ethernet 0
[RouterA-Ethernet0] ip address 192.1.1.1 255.255.255.0
[RouterA-Ethernet0] ospf dr-priority 100
[RouterA-Ethernet0] quit
[RouterA] router id 1.1.1.1
[RouterA] ospf enable
[RouterA-ospf] interface ethernet 0
[RouterA-Ethernet0] ospf enable area 0
```

### 2 Configure Router B:

```
[RouterB] interface ethernet 0
[RouterB-Ethernet0] ip address 192.1.1.2 255.255.255.0
[RouterB-Ethernet0] ospf dr-priority 0
[RouterB-Ethernet0] quit
[RouterB] router id 2.2.2.2
[RouterB] ospf enable
[RouterB-ospf] interface ethernet 0
[RouterB-Ethernet0] ospf enable area 0
```

### 3 Configure Router C:

```
[RouterC] interface ethernet 0
[RouterC-Ethernet0] ip address 192.1.1.3 255.255.255.0
[RouterC-Ethernet0] ospf dr-priority 2
[RouterC-Ethernet0] quit
[RouterC] router id 3.3.3.3
[RouterC] ospf enable
[RouterC-ospf] interface ethernet 0
[RouterC-Ethernet0] ospf enable area 0
```

### 4 Configure Router D:

```
[RouterD] interface ethernet 0
[RouterD-Ethernet0] ip address 192.1.1.4 255.255.255.0
[RouterD-Ethernet0] quit
[RouterD] router id 4.4.4.4
[RouterD] ospf enable
[RouterD-ospf] interface ethernet 0
[RouterD-Ethernet0] ospf enable area 0
```

Run **display ospf peer** on Router A to show OSPF peer. Note that Router A has 3 peers.

```
[RouterA] display ospf peer
```

| Peer    | pri | State        | Address   | Interface |
|---------|-----|--------------|-----------|-----------|
| 4.4.4.4 | 1   | full/DROther | 192.1.1.4 | Ethernet0 |
| 3.3.3.3 | 2   | full/BDR     | 192.1.1.3 | Ethernet0 |
| 2.2.2.2 | 0   | full/DROther | 192.1.1.2 | Ethernet0 |

The status of every peer is full, which means that Router A has created neighboring relation with all peers. Only DR and BDR have created neighboring relation with all routers on the network. Router A is DR and Router C is BDR on the network. All other peers are DROther, which means that they are neither DR nor BDR.

Change the preference of Router B to 200:

```
[RouterB-Ethernet0] ospf dr-priority 200
```

Run **display ospf peer** on Router A to show OSPF peers. Note that the preference of Router B has been changed to 200, but it is not DR.

```
[RouterA] display ospf peer
```

| Peer    | pri | State        | Address   | Interface |
|---------|-----|--------------|-----------|-----------|
| 4.4.4.4 | 1   | full/DROther | 192.1.1.4 | Ethernet0 |
| 3.3.3.3 | 2   | full/BDR     | 192.1.1.3 | Ethernet0 |
| 2.2.2.2 | 200 | full/DROther | 192.1.1.2 | Ethernet0 |

Only when the DR no longer exists on the network are the DR changed. Shut down Router A and run **display ospf peer** on Router D to display peers. Note that Router C, which was BDR, now becomes DR and so does Router B.

```
[RouterD] display ospf peer
```

| Peer    | pri | State    | Address   | Interface |
|---------|-----|----------|-----------|-----------|
| 3.3.3.3 | 2   | full/BDR | 192.1.1.3 | Ethernet0 |
| 2.2.2.2 | 200 | full/DR  | 192.1.1.2 | Ethernet0 |

Shutting down the router and restarting leads to the reelection of DR and BDR. Restart router A and run the **display ospf peer** command to display peers. Note that router B is elected DR (whose preference is 200) and Router A becomes BDR (whose preference is 100).

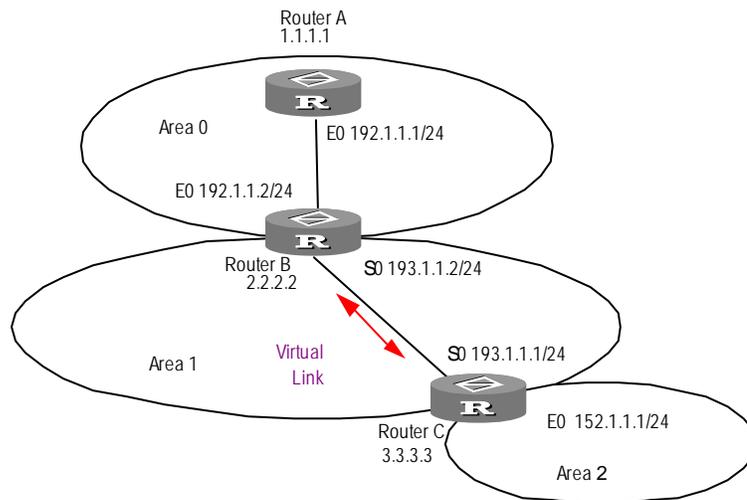
```
[RouterD] display ospf peer
```

| Peer    | pri | State        | Address   | Interface |
|---------|-----|--------------|-----------|-----------|
| 1.1.1.1 | 100 | full/BDR     | 192.1.1.1 | E0        |
| 3.3.3.3 | 2   | full/DROther | 192.1.1.3 | E0        |
| 2.2.2.2 | 200 | full/DR      | 192.1.1.2 | E0        |

## Configuring an OSPF Virtual Link

Area 4 is not directly connected with area 0 in the following diagram. Area 1 serves as the transit area to connect area 4 and area 0. Configure a virtual link between Router B and Router C.

**Figure 149** Networking diagram of configuring OSPF virtual link



To configure an OSPF virtual link:

### 1 Configure Router A:

```
[RouterA] interface ethernet 0
[RouterA-Ethernet0] ip address 192.1.1.1 255.255.255.0
[RouterA-Ethernet0] quit
[RouterA] router id 1.1.1.1
[RouterA] ospf enable
[RouterA-ospf] interface ethernet 0
[RouterA-Ethernet0] ospf enable area 0
```

### 2 Configure Router B:

```
[RouterB] interface ethernet 0
[RouterB-Ethernet0] ip address 192.1.1.2 255.255.255.0
[RouterB-Ethernet0] interface serial 0
[RouterB-Serial0] ip address 193.1.1.2 255.255.255.0
[RouterB-Serial0] quit
[RouterB] router id 2.2.2.2
[RouterB] ospf enable
[RouterB-ospf] interface ethernet 0
[RouterB-Ethernet0] ospf enable area 0
[RouterB-Ethernet0] interface serial 0
[RouterB-Serial0] ospf enable area 1
[RouterB-Serial0] quit
[RouterB] ospf
[RouterB-ospf] Vlink peer-id 3.3.3.3 transit-area 1
```

### 3 Configure Router C:

```
[RouterC] interface ethernet 0
[RouterC-Ethernet0] ip address 152.1.1.1 255.255.255.0
[RouterC-Ethernet0] interface serial 0
[RouterC-Serial0] ip address 193.1.1.1 255.255.255.0
[RouterC-Serial0] quit
```

```

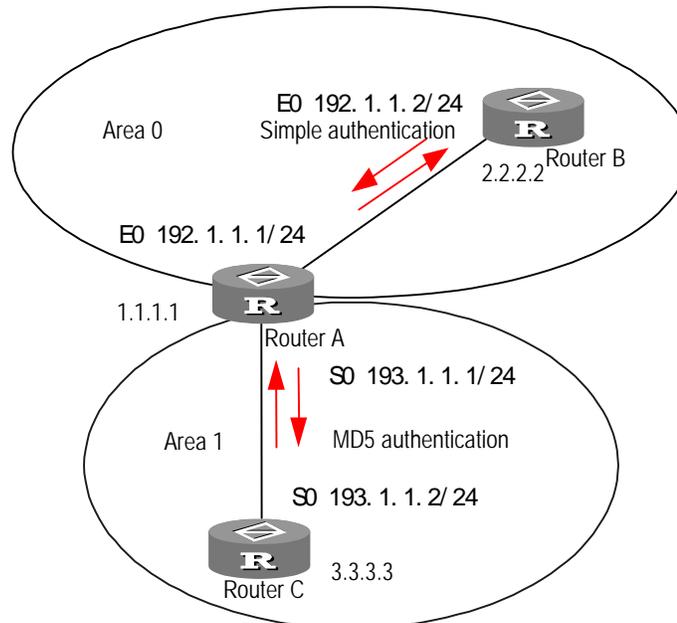
[RouterC] router id 3.3.3.3
[RouterC] ospf enable
[RouterC-ospf] interface ethernet 0
[RouterC-Ethernet0] ospf enable area 2
[RouterC-Ethernet0] interface serial 0
[RouterC-Serial0] ospf enable area 1
[RouterC-Serial0] quit
[RouterC] ospf
[RouterC-ospf] vlink peer-id 2.2.2.2 transit-area 1

```

## Configuring OSPF Peer Authentication

Verify peer authentication with simple text algorithm and MD5 algorithm. Simple text authentication is used when Router A and Router B exchange route updating and MD5 authentication is used when Router A and Router C exchange route updating. The Ethernet interface of Router A and that of Router B are in OSPF area 0. The serial interface of Router A and that of Router B are both in area 1, configured with MD5 authentication.

**Figure 150** Networking diagram of configuring OSPF peer authentication



To configure OSPF peer authentication:

### 1 Configure Router A:

```

[RouterA] router id 1.1.1.1
[RouterA] ospf enable
[RouterA-ospf] interface ethernet 0
[RouterA-Ethernet0] ip address 192.1.1.1 255.255.255.0
[RouterA-Ethernet0] ospf enable area 0
[RouterA-Ethernet0] ospf authentication-mode simple 3Com
[RouterA-Ethernet0] interface serial 0
[RouterA-Serial0] ip address 193.1.1.1 255.255.255.0
[RouterA-Serial0] ospf enable area 1
[RouterA-Serial0] ospf authentication-mode md5 3Com 11

```

### 2 Configure Router B:

```

[RouterB] router id 2.2.2.2

```

```
[RouterB] ospf enable
[RouterB] interface ethernet 0
[RouterB-Ethernet0] ip address 192.1.1.2 255.255.255.0
[RouterB-Ethernet0] ospf enable area 0
[RouterB-Ethernet0] ospf authentication-mode simple 3Com
```

### 3 Configure Router C:

```
[RouterC] router id 3.3.3.3
[RouterC] ospf enable
[RouterC-ospf] interface serial 0
[RouterC-Serial0] ip address 193.1.1.2 255.255.255.0
[RouterC-Serial0] ospf enable area 1
[RouterC-Serial0] ospf authentication-mode md5 3Com 11
```

## Troubleshooting an OSPF Configuration

You have configured OSPF as described previously, but router OSPF fails to run normally.

Perform the following procedures:

- 1 Troubleshoot the local area: First check whether the protocol between the two directly connected routers is running normally. If the peer state machine between the two routers is in FULL status, it means the protocol is running normally. (Note that on broadcast network and NBMA network, the peer state machine between two DROther routers is not in FULL status but in 2 way status. DR, BDR and all other routers are in FULL status).

Use the **display ospf peer** command to view:

```
[Router] display ospf peer

Interface: 202.38.160.1 Area: 0.0.0.2
Neighbors:
RouterID: 2.2.2.2 Address: 202.38.160.2
State:FULL Mode: None Priority: 0
DR: 202.38.160.1 BDR: 202.38.160.1
Last Hello: 14:04 Last Exchange: 0
Authentication Sequence: a51dac
```

View OSPF information on the interface with the **display ospf interface** command.

- Check whether the physical connection and low layer protocol are running normally. If the opposite router cannot ping through the local router, it means that the physical connection and lower layer protocol are faulty.
- If the physical connection and lower layer protocol are normal, check the OSPF parameters configured on the interface. The parameters must be the same as those of the adjacent routers of this interface. The parameters include *hellointerval*, *deadinterval* and *authentication*. The area-id must be the same and the network segment and mask must be consistent (the network segment and mask of point-to-point and virtual link can be different).
- Check whether the *deadinterval* value is at least 4 times the *hellointerval* value on the same interface.
- If the network type is NBMA or point-to-multipoint, or the interface type is manually modified to point-to-point, use command **ospf network-type p2p** to manually specify the peer. In addition, when two routers are connected in

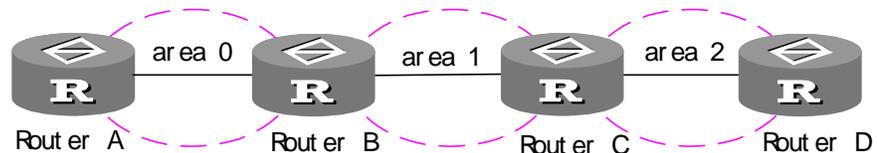
dial-up mode, although the PPP protocol is encapsulated on the link layer, it is still NBMA type. The peer must be specified manually. Use the `ospf peer ip-address` command.

- If the network type is broadcast network or NBMA, at least the priority of one interface must be over 0.
  - If an area is configured to a stub area, all routers connected with this area must be configured to stub areas.
  - The interface type of two adjacent routers must be the same.
  - If two or more areas are configured, at least one area must be configured into a backbone area (area 0).
  - Make sure the backbone area is connected with all areas.
  - A virtual connection cannot go through stub area.
- 2 Global troubleshooting: If the previous steps are correct but OSPF still cannot find the remote route, check the following features of the configuration.
- If two or more areas are configured for one router, at least one area must be configured as a backbone area (the area-id of one area must be 0 or a virtual link must be configured).

As shown in the following diagram, only one area is configured on Router A and Router D and two areas are configured respectively for Router B (area0, area1) and Router C (area1, area2). One area in Router B is 0, which satisfies the requirement. However, none of the two areas in Router C is 0. In such a case, a virtual link must be set up between Router C and Router B.

Make sure area 2 and area 0 (backbone area) are connected.

**Figure 151** OSPF Area Schematic Diagram



- The virtual link cannot go through a stub area and the backbone area (area 0) cannot be configured as stub area. Therefore, if a virtual link is configured between Router B and Router C, area 1 cannot be configured as a stub area, nor can area 0. In the above diagram, only area 2 can be configured as a stub area.
- The router in the stub area (Router D) cannot receive an external route.
- Make sure the backbone areas are connected.



# 30

## CONFIGURING BGP

This chapter covers the following topics:

- BGP Overview
- Configuring BGP
- Displaying and Debugging BGP
- BGP Configuration Example

---

### BGP Overview

Border Gateway Protocol (BGP) is an inter-AS dynamic route discovery protocol. Its primary function is to exchange loop-free routing information between ASs automatically and to construct the topology diagram of an AS through the exchange of path reachability information, including AS numbers. It constructs the topological diagrams of the ASs to eliminate route loops and carry out user configured strategies. The BGP protocol is usually used between ISPs.

The current version of BGP is BGP-4. It applies to the distributed structure and supports classless interdomain routing (CIDR). BGP-4 has become the standard of Internet external routing protocol. It features the following:

- BGP is an external routing protocol, oriented to control route spreading and select best route rather than find and calculate route. This is different from the internal routing protocol.
- Completely resolves the route loop problem by carrying AS path information.
- Uses TCP as the transmission layer protocol, improving the reliability of the protocol.
- BGP-4 supports classless interdomain routing (CIDR), or supernetting. CIDR judges the IP address in a totally new way. It no longer recognizes network class A, network class B, or network class C. For example, with CIDR, an illegal class C network address 192.213.0.0 (255.255.0.0) is indicated as 192.213.0.0/16, which is a legal supernet. /16 means that the subnet mask is 16bit starting from the left of the address. The introduction of CIDR simplifies the route aggregation. Route aggregation is the combination of several routes. Thus one route instead of several routes are distributed and the routing table is simplified.
- When a route is updated, BGP only sends the incremental route. In this way, BGP occupies much less bandwidth in transmitting routes. It applies to the transmission of a large amount of routing information on the Internet.
- For political and economic reasons, each AS must filter, select and control the routes. BGP-4 provides abundant routing strategies for easy expansion of BGP to support new developments of the Internet.

The BGP system runs on a specific router as a high layer protocol. At system startup, the whole BGP routing table is transmitted for the exchange of routing information. Later on, only an update message is transmitted for updating the routing table. In the system, keep-alive messages are received and transmitted to check whether the connection between routers is normal.

The router transmitting the BGP message is called the BGP speaker. It receives and generates new routing information from time to time and advertises to other BGP speakers. When a BGP speaker receives a new route advertisement from other ASs, if this route is better than the existing route, or if there is no acceptable route currently, the BGP speaker broadcasts this route to all other BGP speakers in the AS. BGP speakers are peers to each other and several related peers form a peer group.

BGP runs on the router in two modes:

- IBGP (Internal BGP)
- EBGP (External BGP)

IBGP is run when routers in an autonomous system exchange network reachable information. When routers of different ASs exchange network reachable information, they use EBGP.

The BGP protocol system is driven by messages that can be divided into 4 categories:

- Open message. This is the first transmitted message after the connection is created. It is used to create a connection between BGP peers
- Update message is the most important message in BGP system, and is used to switch routing information among the peers. Update message consists of three parts: unreachable route, path attributes and Network Layer Reachability Information (NLRI).
- Notification message notifies errors.
- Keep-alive message is used to check the validity of the connection.

---

## Configuring BGP

A BGP configuration includes tasks described in the following sections:

- Enabling BGP
- Configuring Networks for BGP Distribution
- Configuring Peers

A BGP advanced configuration includes:

- Setting the MED for the AS
- Allow Comparing Path MED
- Configuring the Local Preference
- Configuring BGP Timers
- Configuring a BGP Peer Group
- Creating Aggregate Addresses
- Configure BGP Route Reflector

- Configuring a BGP Community
- Configuring a BGP AS Confederation Attribute
- Configuring Route Dampening
- Configuring Synchronization of BGP and IGP
- Configuring the Interactions between BGP and an IGP
- Defining an Access List Entry, an AS Path-list Entry, a Routing Policy
- Configuring a Route Filter for BGP
- Resetting BGP Connections

### Enabling BGP

Specify the local AS number when BGP is enabled. After BGP is enabled, the local router continuously monitors whether any incoming BGP connection request is received from the peer routers. To make the local router send BGP connection requests to the peer routers, use the **peer** command. When BGP is turned off, BGP protocol closes all BGP connections that have been created.

Perform the following configurations in system view.

**Table 508** Enable BGP

| Operation                              | Command                  |
|----------------------------------------|--------------------------|
| Enable BGP and enter into the BGP view | <b>bgp [ as-number ]</b> |
| Turn off the BGP                       | <b>undo bgp</b>          |

By default, BGP is disabled.

### Configuring Networks for BGP Distribution

Perform the following configurations in BGP view.

**Table 509** Configure Networks for BGP Distribution

| Operation                                      | Command                                                                      |
|------------------------------------------------|------------------------------------------------------------------------------|
| Specify a list of networks associated with BGP | <b>network ip-address [ mask address-mask ] [ route-policy policy-name ]</b> |
| Delete a list of networks associated with BGP  | <b>undo network ip-address [ mask address-mask ]</b>                         |

By default, no network is configured for BGP distribution.

### Configuring Peers

The routers that exchange BGP packets are called peers to each other. Peers can be directly connected routers or indirectly connected routers but should be connected by other directly connected router or routers.

BGP peer basic configuration includes setting the AS number of the peer.

Perform the following peer configuration in BGP view.

**Table 510** Configure AS Number of the Peer

| Operation                       | Command                                      |
|---------------------------------|----------------------------------------------|
| Configure AS number of the peer | <b>peer peer-address as-number as-number</b> |

|                   |                                                         |
|-------------------|---------------------------------------------------------|
| Delete a BGP peer | <code>undo peer peer-address as-number as-number</code> |
|-------------------|---------------------------------------------------------|

BGP peer advanced configuration includes the following steps:

- 1 Configure the connection between EBGP peers that are connected indirectly.

**Table 511** Configure Connection Between EBGP Peers Connected Indirectly

| Operation                                                    | Command                                                            |
|--------------------------------------------------------------|--------------------------------------------------------------------|
| Configure connection between EBGP peers connected indirectly | <code>peer peer-address ebgp-max-hop [ max-hop-count ]</code>      |
| Return to the default BGP connections to external peers      | <code>undo peer peer-address ebgp-max-hop [ max-hop-count ]</code> |

By default, the BGP connection can be established with a directly connected peer router.

- 2 Configure the BGP version of the peer.

**Table 512** Configure the BGP Version of the Peer

| Operation                               | Command                                               |
|-----------------------------------------|-------------------------------------------------------|
| Configure the BGP version of the peer   | <code>peer peer-address version version-number</code> |
| Unconfigure the BGP version of the peer | <code>undo peer peer-address version</code>           |

By default, software accepts BGP Version 4.

- 3 Set the timers for the BGP peer.

**Table 513** Set the Timers for BGP Peer

| Operation                                    | Command                                                                    |
|----------------------------------------------|----------------------------------------------------------------------------|
| Set the timers for BGP peer                  | <code>peer peer-address timers keepalive-interval holdtime-interval</code> |
| Set the timers for BGP peer to default value | <code>undo peer peer-address timers</code>                                 |

By default, the value of `keepalive-interval` is 60 seconds, the value of `holdtime-interval` is 180 seconds.



**Caution:** The timer configured with this command is of higher preference than that configured with the `timers` command.

- 4 Configure the BGP route-update interval.

**Table 514** Configure BGP Route-update Interval

| Operation                           | Command                                                      |
|-------------------------------------|--------------------------------------------------------------|
| Configure BGP route-update interval | <code>peer peer-address route-update-interval seconds</code> |
| Restore BGP route-update interval   | <code>undo peer peer-address route-update-interval</code>    |

By default, the BGP route-update interval is 5 seconds.

- 5 Configure to send community attribute to the peer.

**Table 515** Configure to Send Community Attribute to the Peer

| Operation                                         | Command                                                  |
|---------------------------------------------------|----------------------------------------------------------|
| Configure to send community attribute to the peer | <b>peer <i>peer-address</i> advertise-community</b>      |
| Cancel sending community attribute to the peer    | <b>undo peer <i>peer-address</i> advertise-community</b> |

By default, the community attributes are not sent to the peer.

## 6 Configure the peer to be the client of the route reflector.

**Table 516** Configure the Peer to be the Client of the Route Reflector

| Operation                                                                            | Command                                             |
|--------------------------------------------------------------------------------------|-----------------------------------------------------|
| Configure the peer to be the client of the route reflector                           | <b>peer <i>peer-address</i> reflect-client</b>      |
| Cancel the configuration of making the peer as the client of the BGP route reflector | <b>undo peer <i>peer-address</i> reflect-client</b> |

## 7 Configure to distribute default route to the peer.

**Table 517** Configure to Distribute Default Router to the Peer

| Operation                                             | Command                                                      |
|-------------------------------------------------------|--------------------------------------------------------------|
| Configure to distribute default route to the peer     | <b>peer <i>peer-address</i> default-route-advertise</b>      |
| Configure not to distribute default route to the peer | <b>undo peer <i>peer-address</i> default-route-advertise</b> |

By default, the local router does not advertise the default route to any peer. A next hop should be sent to the peer unconditionally as the default route.

## 8 Set the own IP address as the next hop when the peer distributes routes.

Set the router's own IP address as the next hop when the peer distributes routes.

**Table 518** Set the Own IP Address as the Next Hop When the Peer Distributes Route

| Operation                                                                     | Command                                             |
|-------------------------------------------------------------------------------|-----------------------------------------------------|
| Set the own IP address as the next hop when the peer distributes route        | <b>peer <i>peer-address</i> next-hop-local</b>      |
| Not to Set the own IP address as the next hop when the peer distributes route | <b>undo peer <i>peer-address</i> next-hop-local</b> |

By default, its own address is not the next hop when the peer distributes routes.

## 9 Create a routing policy for the peer.

**Table 519** Create a Routing Policy for the Peer

| Operation                                          | Command                                                                                  |
|----------------------------------------------------|------------------------------------------------------------------------------------------|
| Create a routing policy for the peer               | <b>peer <i>peer-address</i> route-policy <i>policy-name</i> { import   export }</b>      |
| Remove a routing policy to import or export routes | <b>undo peer <i>peer-address</i> route-policy <i>policy-name</i> { import   export }</b> |

By default, the route from the peer or peer group is not designated with any route policy.

- 10 Create an filtering policy based on access list for the peer.

**Table 520** Create a Filtering Policy Based on Access List for the Peer

| Operation                                                     | Command                                                                          |
|---------------------------------------------------------------|----------------------------------------------------------------------------------|
| Create an filter policy based on access list for the peer     | <code>peer peer-address filter-policy acl-number { import   export }</code>      |
| Remove an filter policy based on the access list for the peer | <code>undo peer peer-address filter-policy acl-number { import   export }</code> |

By default, no route filtering policy based on IP ACL for a peer is set.

- 11 Create BGP route filtering based on the AS path for the peer. By default, a BGP filter is disabled.

**Table 521** Create a BGP Route Filtering Based on AS Path for the Peer

| Operation                                                  | Command                                                                        |
|------------------------------------------------------------|--------------------------------------------------------------------------------|
| Create a BGP route filtering based on AS path for the peer | <code>peer peer-address acl aspath-list-number { import   export }</code>      |
| Delete a BGP route filtering based on AS path for the peer | <code>undo peer peer-address acl aspath-list-number { import   export }</code> |

### Setting the MED for the AS

The multi-exit discriminator (MED) is the external metric of a route. It is different from the local preference attribute. MED is switched between ASs and the MED that has entered the AS does not leave the AS. AS uses local attributes for its own out-site selection processing while MED attribute is used to select the best route. The route with smallest MED value is selected. When a router running BGP gets routes with the same destination address but a different next hop through different external peers, it makes a preference selection based on the MED values.

To operate the MED attribute, an access control list is used to indicate what network will be operated.

Perform the following configurations in BGP view.

**Table 522** Configure the BGP MED Metric

| Operation                        | Command                       |
|----------------------------------|-------------------------------|
| Configure MED for an AS          | <code>default-med med</code>  |
| Restore the default MED of an AS | <code>undo default-med</code> |

### Allow Comparing Path MED

This command is used to compare MED values from different AS neighboring routes and to select the best route. The route with smaller MED value is selected.

Perform the following configurations in BGP view.

**Table 523** Allow Comparing Path MED

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                             |                                      |
|-----------------------------|--------------------------------------|
| Allow comparing path MED    | <b>compare-different-as-med</b>      |
| Prohibit comparing path MED | <b>undo compare-different-as-med</b> |

By default, MED values from different AS neighboring routes are not compared when determining the best route.

This configuration should not be used unless it is certain that different ASs uses the same IGP and routing modes.

### Configuring the Local Preference

Configuring different local preferences affects BGP routing selection. When a router running BGP gets routes with the same destination address but different next hops through different internal peers, it selects the route of the highest local preference to this destination.

Perform the following configurations in BGP view.

**Table 524** Configure the Local Preference

| Operation                                               | Command                               |
|---------------------------------------------------------|---------------------------------------|
| Configure the local preference                          | <b>default local-preference value</b> |
| Restore the local preference value to its default value | <b>undo default local-preference</b>  |

By default, the value of local preference is 100.

### Configuring BGP Timers

The interval of sending keepalive messages required by RFC and BGP holdtime are important parameters in BGP protocol.

When a router has created a BGP connection successfully with the other router, it sends keepalive messages to this router with the time interval set by the **keepalive-interval** attribute to indicate whether the connection channel is normal. Generally, the time interval for sending a keepalive message is one third of the value for the **holdtime** attribute.

The value of the holdtime-interval attribute is the time interval for continuously receiving keepalive and update messages. If a keepalive or update message is received, the holding timer is reset. If a router has not received any messages from the opposite router for a specific period of holding time, this BGP connection is considered broken and is cut off. The router can negotiate with the interconnected router to set a shorter holding time.

Perform the following configurations in BGP view.

**Table 525** Configure the Keepalive Timer and Holdtime Timer for BGP

| Operation                                                | Command                                            |
|----------------------------------------------------------|----------------------------------------------------|
| Configure the keepalive timer and holdtime timer for BGP | <b>timers keepalive-interval holdtime-interval</b> |
| Restore BGP network timers to their default value        | <b>undo timers</b>                                 |

By default, the value for the **keepalive-interval** attribute is 60 seconds and may have a value ranging from 1 to 4294967295 seconds. The default value for the

**holdtime-interval** attribute is 180 seconds and may have a time interval ranging from 3 to 42949675 seconds.

## Configuring a BGP Peer Group

The BGP peer group command can be used for user configuration. When starting several peers of the same configuration, you can first create and configure one peer group, then add other peer groups into this group to get the same configuration.

Configuring a basic BGP peer group includes creating a peer group and adding a peer to the group.

Perform the following peer group configuration in BGP view.

### 1 Create a peer group

By default, a IBGP peer is added to the default peer group and no configuration is necessary. The configuration of route updating strategy to any IBGP peer is only applicable to other IBGP peers in the group. If the router is not configured as a route reflector, all IBGP peers are in one group. Otherwise, all route reflection clients are in one group and non-clients are in another group.

The members of an external peer group must be in the same network segment, otherwise some EBGp peers may discard the route updating information you have sent.

All peers in this group must be configured with an AS number, if this group is not configured with an AS number. If you add an AS number to the peer group, any peer in this group cannot be configured with an AS number different from this peer group AS number.

The members of the peer group cannot be configured with a route updating strategy different from that of the group but different access strategy is permitted.

**Table 526** Create a Peer Group

| Operation                                             | Command                           |
|-------------------------------------------------------|-----------------------------------|
| Create a peer group                                   | <b>peer group-name group</b>      |
| Delete a specified peer group                         | <b>undo peer group-name group</b> |
| Reset the connection of all members in the peer group | <b>reset bgp group group-name</b> |

By default, no peer group is created.

### 2 Add a peer to the BGP peer group

Add one BGP peer into the peer group to create a peer group. When the configuration of the peer group is changed, the configuration of each peer should also be changed accordingly. IBGP peer and EBGp peer cannot be in the same group.

**Table 527** Add a Peer to the BGP Peer Group

| Operation                               | Command                                        |
|-----------------------------------------|------------------------------------------------|
| Add a peer to the BGP peer group        | <b>peer peer-address group group-name</b>      |
| Delete a member from the BGP peer group | <b>undo peer peer-address group group-name</b> |

By default, there is no BGP peer in a peer group.

To configure an advanced BGP peer group configuration:

1 Configure the AS number of BGP peer group

**Table 528** Configure AS Number of BGP Peer Group

| Operation                             | Command                                                              |
|---------------------------------------|----------------------------------------------------------------------|
| Configure AS number of BGP peer group | <b>peer</b> <i>group-name</i> <b>as-number</b> <i>as-number</i>      |
| Remove AS number of BGP peer group    | <b>undo peer</b> <i>group-name</i> <b>as-number</b> <i>as-number</i> |

By default, there is no AS number for BGP peer group.

2 Configure connection between peers indirectly connected

**Table 529** Configure Connection Between Peers Indirectly Connected

| Operation                                                    | Command                                                          |
|--------------------------------------------------------------|------------------------------------------------------------------|
| Configure connection between peers indirectly connected      | <b>peer</b> <i>group-name</i> <b>ebgp-max-hop</b> [ <i>tth</i> ] |
| Return to the default BGP connections to external peer group | <b>undo peer</b> <i>group-name</i> <b>ebgp-max-hop</b>           |

By default, it only allows direct-connection peer.

The maximum hop value is *tth*. The default value is 64, ranging from 1 to 255.

3 Set the timers of BGP peer group

**Table 530** Set the Timers of BGP Peer Group

| Operation                                             | Command                                                                                        |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Set the timers of BGP peer group                      | <b>peer</b> <i>group-name</i> <b>timers</b> <i>keepalive-interval</i> <i>holdtime-interval</i> |
| Restore the timers of BGP peer group to default value | <b>undo peer</b> <i>group-name</i> <b>timers</b>                                               |

By default, the interval of sending keepalive packet is 60 seconds, the interval of holdtime is 180 seconds,

Note that the timers configured with this command are of higher preference than the values configured with the **timers** command.

4 Configure the BGP routing update sending interval

**Table 531** Configure BGP Routing Update Sending Interval

| Operation                                     | Command                                                                   |
|-----------------------------------------------|---------------------------------------------------------------------------|
| Configure BGP routing update sending interval | <b>peer</b> <i>group-name</i> <b>route-update-interval</b> <i>seconds</i> |
| Restore BGP routing update sending interval   | <b>undo peer</b> <i>group-name</i> <b>route-update-interval</b>           |

By default, the BGP routing update sending interval is 5 seconds

5 Configure to send the community attribute to a BGP peer group

**Table 532** Configure to Send Community Attribute to a BGP Peer Group

| Operation                                                 | Command                                                       |
|-----------------------------------------------------------|---------------------------------------------------------------|
| Configure to send community attribute to a BGP peer group | <b>peer</b> <i>group-name</i> <b>advertise-community</b>      |
| Delete the BGP community en to the peer group.            | <b>undo peer</b> <i>group-name</i> <b>advertise-community</b> |

By default, send no community attribute to any peer group.

## 6 Configure a peer group as the client of a BGP reflector

In general, the AS requires that all the IBGP routers should be connected to one another, and the routes sent by the IBGP neighbors is not advertised, to prevent route loop. However, if the route reflector is used, not all IBGP speakers are required to be fully connected. This technique requires configuring an internal BGP peer as a router reflector. Other internal peers are not necessarily mesh connected but set up an IBGP session with the route reflector and learn routes through the route reflector. Using `peer reflect-client` command, you can configure internal neighbors which can communicate with the route reflector. These neighbors are the client-group members of the route reflector. Other neighbors are the non-client-group members.

Generally, it is unnecessary to configure this command for the peer entity since the IBGP peer is in its default group. You should use the `peer peer-address reflect-client` command to configure the route reflector client.

**Table 533** Configure Peer Group as the Client of BGP Reflector

| Operation                                           | Command                                          |
|-----------------------------------------------------|--------------------------------------------------|
| Configure peer group as the client of BGP reflector | <code>peer group-name reflect-client</code>      |
| Disable peer group as the client of BGP reflector   | <code>undo peer group-name reflect-client</code> |

## 7 Configure to send the default route to the peer group

**Table 534** Configure to Send the Default Route to the Peer Group

| Operation                                         | Command                                                   |
|---------------------------------------------------|-----------------------------------------------------------|
| Configure to send the default route to peer group | <code>peer group-name default-route-advertise</code>      |
| Do not allow to send default route to the peers   | <code>undo peer group-name default-route-advertise</code> |

By default, the local router does not advertise the default route to any peer group. A next hop should be sent to the peer unconditionally as the default route.

## 8 Set the router's own IP address as the next hop when the peer group distributes route information.

Cancel the processing of next hop when sending a route to the peer and take the self-address as the next hop.

**Table 535** Set the Own IP address as Next Hop When Peer Group Distributes Route

| Operation                                                                   | Command                                          |
|-----------------------------------------------------------------------------|--------------------------------------------------|
| Set the own IP address as next hop when peer group distributes route        | <code>peer group-name next-hop-local</code>      |
| Not to set the own IP address as next hop when peer group distributes route | <code>undo peer group-name next-hop-local</code> |

By default, the router's own IP address is not set as the next hop when the peer group distributes routes.

## 9 Create a routing policy for the peer group

**Table 536** Create Routing Policy for Peer Group

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                                                    |                                                                                |
|----------------------------------------------------|--------------------------------------------------------------------------------|
| Create routing policy for peer group               | <code>peer group-name route-policy policy-name { import   export }</code>      |
| Remove a routing policy to import or export routes | <code>undo peer group-name route-policy policy-name { import   export }</code> |

By default, the route from the peer or peer group is not designated with any route policy.

## 10 Create a filtering policy based on the access list for the peer group

**Table 537** Create a Filtering Policy Based on Access List for Peer Group

| Operation                                                      | Command                                                                        |
|----------------------------------------------------------------|--------------------------------------------------------------------------------|
| Create an filtering policy based on access list for peer group | <code>peer group-name filter-policy acl-number { import   export }</code>      |
| Delete an filtering policy based on access list for peer group | <code>undo peer group-name filter-policy acl-number { import   export }</code> |

By default, no route filtering policy based on IP ACL for peer group is set.

## 11 Create a BGP route filtering based on the AS path for the peer group

**Table 538** Create a BGP Route Filtering Based on AS Path for Peer Group

| Operation                                                    | Command                                                                      |
|--------------------------------------------------------------|------------------------------------------------------------------------------|
| Create a BGP route filtering based on AS path for peer group | <code>peer group-name acl aspath-list-number { import   export }</code>      |
| Delete a BGP route filtering based on AS path for peer group | <code>undo peer group-name acl aspath-list-number { import   export }</code> |

By default, a BGP filtering is disabled.

## 12 Configure the BGP version of peer group

**Table 539** Configure BGP Version of Peer Group

| Operation                                          | Command                                             |
|----------------------------------------------------|-----------------------------------------------------|
| Configure the BGP version of peer group            | <code>peer group-name version version-number</code> |
| Restore the default BGP version for the peer group | <code>undo peer group-name version</code>           |

By default, software accepts BGP Version 4.

## Creating Aggregate Addresses

CIDR supports manual route aggregation. Manual aggregation, using the `aggregate` command adds a piece of routing aggregate information to the BGP routing table. The parameters can be set at the same time when manual aggregation mode is configured.

Perform the following configurations in BGP view.

**Table 540** Create an Aggregate Addresses

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                                                                          |                                                                                                                                                                     |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add a piece of routing aggregate information to the BGP routing table    | <code>aggregate address mask [ as-set ] [ detail-suppressed ] [ suppress-policy policy-name ] [ origin-policy policy-name ] [ attribute-policy policy-name ]</code> |
| Delete a piece of routing aggregate information to the BGP routing table | <code>undo aggregate address mask</code>                                                                                                                            |

By default, an aggregate is disabled.

**Configure BGP Route Reflector**

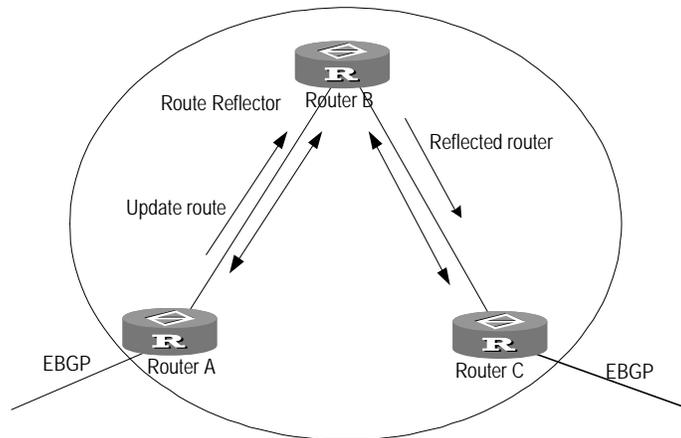
To guarantee the connectivity between the IBGP peers, an all-closed network should exist between IBGP peers. In some networks, the internal BGP network can become very large (with more than one hundred sessions in each router), resulting in huge overhead. The route reflector designates a central router as the core of the internal sessions. Multiple BGP routers can become peers with this central router, and then multiple route reflectors can be peers with each other.

Since the route reflector is the center of other routers, other routers are called client routers from the viewpoint of the reflector. The client routers are peers of the route reflector and exchange routing information. The route reflector forwards (reflects) information among the client routers in turn.

As shown in the following diagram, Router A receives an update from an external peer and transfers it to Router B. Router B is a route reflector, which has two clients: Router A and Router C.

Router B can reflect the routing update from client Router A to client Router C. In this instance, the session between Router A and Router C is unnecessary because the route reflector forwards the BGP information to Router C.

**Figure 152** Schematic diagram of route reflector



The route reflector divides the IBGP peers into two types: client and non-client. Using the peer reflect-client command, you can configure the internal neighbors that can communicate with the route reflector. The neighbors are called the client group members of the route reflector, and other neighbors that are not configured as the non-clients are the non-client group members of the route reflector.

The non-clients must form an all-closed network with the reflector, as they follow the basic rules of IBGP. A client should not be peer of other internal speakers outside its cluster. The reflecting function is achieved only on the route reflector. All the clients and non-clients are normal BGP peers irrelevant to the function. A client is a client only because the route reflector regards it as the client.

When the router reflector receives several routes to one destination, it chooses the best one based on the usual BGP routing strategy process. The best route transfers inside AS according to following rules:

- If the route is received from non-client peers, it only reflects to clients.
- If the route is received from client peers, it reflects to all the clients and non-clients except this route's sender.
- If an EBGP peer receives the route, it is reflected to all clients and non-client peers that can be reflected.

## 1 Configure the route reflection between clients.

Perform the following configurations in BGP view.

**Table 541** Configure the Route Reflection Between Clients

| Operation                                                                         | Command                             |
|-----------------------------------------------------------------------------------|-------------------------------------|
| Enable route reflection function between the clients within the reflection group  | <b>reflect between-clients</b>      |
| Disable route reflection function between the clients within the reflection group | <b>undo reflect between-clients</b> |

By default, the route reflection function is disabled between the clients within the reflection group.

Note that the route reflector configuration between the clients is invalid if the clients are fully connected.

## 2 Configure the cluster ID.

As the route reflector is imported, the route selection circle can occur in an AS, and the route that leaves a cluster during update may try to reenter this cluster. The traditional AS routing method cannot detect the internal circle of the AS, because the update has not left the AS yet. BGP provides two methods to avoid an AS internal loop when you configure the route reflector:

### a Configure an originator-ID for the route reflector:

The originator-ID is a 4-bit, optional, non-transitional BGP attribute created by the route reflector. It carries the router ID of the originator. If the configuration is improper, and the routing update returns to the originator, the originator will discard it.

You don't need to configure this parameter, and it functions automatically when the BGP protocol is started.

### b Configure the cluster-ID of the route reflector:

Generally, a cluster has only one route reflector. To avoid routing update information failure due to the route reflector failure, multiple route reflectors are recommended for a cluster. If more than one route reflector exists in a cluster, all the route reflectors must be configured with the same cluster ID.

Perform the following configurations in BGP view.

**Table 542** Configure the Cluster ID

| Operation                                   | Command                                   |
|---------------------------------------------|-------------------------------------------|
| Configure Cluster-ID of the Route-Reflector | <b>reflect cluster-id cluster-id</b>      |
| Remove Cluster-ID of the Route-Reflector    | <b>undo reflect cluster-id cluster-id</b> |

By default, the router ID of the route reflector is used as the cluster ID.

### Configuring a BGP Community

In BGP range, a community is a logical area formed by a group of destinations which share common attributes for applying the route policy. A community is not limited to a network or an AS, and has no physical boundary.

The community attribute is an optional and transitional attribute. Some communities are commonly recognized and globally functional. These communities are called standard communities. Sometimes the extended community attribute can be defined for special purposes.

The community attribute list is used to identify the community information. It can be a standard-community-list and an extended-community-list.

In addition, one route can have more than one community attribute. The speaker with multiple community attributes in a route can work according to one, several or all attributes. The community attribute can be added or modified before the router transfers a route to other peers.

Perform the following configurations in system view.

**Table 543** Configure BGP Community

| Operation                               | Command                                                                                                                                                         |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create a standard-community-list        | <b>ip community-list<br/>standard-community-list-number {<br/>permit   deny } { aa:nn   internet  <br/>no-export-subconfed   no-advertise  <br/>no-export }</b> |
| Specify a extended-community-list entry | <b>ip community-list<br/>extended-community-list-number {<br/>permit   deny } as-regular-expression</b>                                                         |
| Delete the specified community list     | <b>undo ip community-list<br/>{standard-community-list-number  <br/>extended-community-list-number }</b>                                                        |

By default, no community list is created.

### Configuring a BGP AS Confederation Attribute

Confederation is another method to solve the problem of a sudden increase of IBGP closed networks inside an AS. An AS is divided into multiple sub-ASs and the IBGP peers inside the sub-ASs are fully connected, and each sub-AS connects with other sub-ASs inside the confederation. Among the subsystem, the peers perform EBGP sessions, but they can exchange routing information just like IBGP peers. All the important information such as the next hop, MED value and the local priority will not be lost when passing through the AS.

The disadvantage is that when a non-confederation scheme changes to a confederation scheme, it is required to reconfigure the router and to modify the logical topology. In addition, if the BGP strategy is not manually configured, the best path may not be selected through the confederation.

### 1 Configure a Confederation

You can use different IGP for each sub-AS. Externally, a sub-AS is an integer and the confederation ID is the identification of the sub-AS.

Perform the following configurations in BGP view.

**Table 544** Configure a Confederation

| Operation                  | Command                           |
|----------------------------|-----------------------------------|
| Specify a Confederation id | <b>confederation id as-number</b> |
| Remove a Confederation id  | <b>undo confederation id</b>      |

By default, no BGP confederation identifier is specified.

### 2 Configure the sub-system of e confederation

The configured sub-AS is inside a confederation and each sub-AS uses fully closed network. Use **confederation id** command to specify the confederation ID of the AS. If the confederation ID is not configured, this configuration item is invalid.

Perform the following configurations in BGP view.

**Table 545** Configure the Sub-system of E Confederation

| Operation                                   | Command                                                       |
|---------------------------------------------|---------------------------------------------------------------|
| Configure the sub-system of e confederation | <b>confederation peer-as as-number [ as-number ] ...</b>      |
| Delete an AS from the confederation         | <b>undo confederation peer-as as-number [ as-number ] ...</b> |

By default, no confederation peers are specified.

### 3 Configure the non-RFC standard AS confederation attributes.

The creation of an AS confederation in the devices from some other providers may not be consistent with the RFC1965 standard. All the routers in the confederation must be configured as using non-RFC1965 standard AS confederation attributes to create interconnections with the router using non-RFC1965 standard AS confederation.

Perform the following configurations in BGP view.

**Table 546** Configure to Use the Non-RFC Standard AS Confederation Attributes.

| Operation                                                   | Command                                          |
|-------------------------------------------------------------|--------------------------------------------------|
| Configure the non-RFC standard AS confederation attributes. | <b>confederation nonstandard-compatible</b>      |
| Remove the non-RFC standard AS confederation attributes.    | <b>undo confederation nonstandard-compatible</b> |

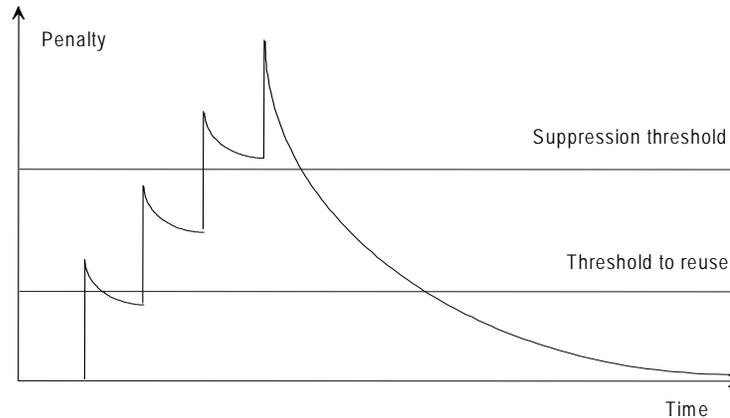
By default, 3Com routers use the RFC1965 standard AS confederation attributes.

## Configuring Route Dampening

Route instability is frequently indicated when a route disappears that used to exist in the routing table. This route may reappear and disappear frequently, which is called routing flapping. When there is route flapping, the UPDATE and WITHDRAWN messages are broadcast repeatedly over the network, occupying bandwidth and processing time of the routers. The administrator should take action to prevent route flapping. Route dampening is a technology to control routing flapping.

There are two types of routes, stable routes and unstable routes. Stable routes remain in the route table continuously, while unstable routes should be suppressed by route dampening. The unstable route is penalized by not allowing it to advertise when its penalty level reaches a threshold. The penalty is exponentially decreased as time goes by. Once it is lower than a certain threshold, the route is unsuppressed and is advertised again, as shown in the following diagram.

**Figure 153** Schematic diagram of route dampening



Configure the following parameters to adjust the performance of route dampening:

- **Penalty:** Increases upon each route flap, decays as time goes by.
  - **Reachable-half-life:** Time duration before they reachable route penalty is reduced to half.
  - **Unreachable-half-time:** Time duration before the unreachable route penalty is reduced to half.
  - **Ceiling-max-suppress:** The maximum value of the penalty.
  - **Suppress-limit:** The route advertisement is suppressed when the penalty reaches this threshold.
  - **Reuse-limit:** The route advertisement is unsuppressed when the penalty is lower than this value.
- 1 Configure route dampening.

Perform the following configurations in BGP view.

The parameters are mutually dependent. To configure any parameter, all other parameters should also be specified.

**Table 547** Configure Route Dampening

| Operation                                                                      | Command                                                                                                                                                      |
|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Put BGP route attenuation in effect or modify BGP route attenuation parameter  | <b>dampening</b> [ <i>half-life-reachable</i> <i>half-life-unreachable</i> <i>reuse</i> <i>suppress</i> <i>ceiling</i> ] [ <i>route-policy policy-name</i> ] |
| Clear route routing dampening information and de-suppress the suppressed route | <b>reset dampening</b> [ <i>network-address</i> [ <i>mask</i> ] ]                                                                                            |
| Disable the route dampening                                                    | <b>undo dampening</b>                                                                                                                                        |

By default, route dampening is disabled.

## 2 Display route flap information.

Perform the following configurations in system view.

**Table 548** Display Route Flap Information

| Operation                                                                               | Command                                                                                               |
|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Display BGP dampened routes                                                             | <b>display bgp routing-table dampened</b>                                                             |
| Display flap information of all routes                                                  | <b>display bgp routing-table flap-information</b>                                                     |
| Display the route flap statistics of routes with AS path comply with regular expression | <b>display bgp routing-table flap-information regular-expression</b> <i>as-regular-expression</i>     |
| Reset BGP flap information matching AS path regular expression                          | <b>reset bgp flap-information</b> <i>regular-expression</i> [ <i>as-regular-expression</i> ]          |
| Display the route flap statistics of routes that passed AS filter-list                  | <b>display bgp routing-table flap-information acl</b> [ <i>aspath-list-number</i> ]                   |
| Clear BGP flap information matching the specified filter list                           | <b>reset bgp flap-information acl</b> [ <i>aspath-list-number</i> ]                                   |
| Display the route flap statistics of routes with designated destination address         | <b>display bgp routing-table flap-information network-address</b> <i>mask</i> [ <i>longer-match</i> ] |
| Clear the route flap statistics of routes with designated destination address           | <b>reset bgp flap-information</b> <i>network-address</i>                                              |
| Clear the route flap statistics of routes received from the specified peer.             | <b>reset bgp network-address</b> <i>flap-information</i>                                              |

## Configuring Synchronization of BGP and IGP

BGP protocol prescribes that a BGP router does not advertise the destination known through internal BGP peers to external peers unless the destination can be known also through IGP. If a router can know the destination through IGP, then the route can be distributed in the AS because an internal connection has been ensured.

One major task of the BGP protocol is to distribute the network reachable information of the local AS to other ASs. Therefore, BGP needs to distribute the route information by synchronization with IGP (such as RIP and OSPF), Synchronization means that BGP cannot distribute transition information to other ASs until IGP broadcasts the route information successfully within its AS. That is to say, before a router receives an updated destination information from an IBGP

peer and advertises it to other EBGP peers, it will try to check whether this destination can be reached through its AS.

Perform the following configurations in BGP view.

**Table 549** Configure Synchronization of BGP and IGP

| Operation                           | Command                     |
|-------------------------------------|-----------------------------|
| Synchronize BGP with IGP            | <b>synchronization</b>      |
| Prohibit synchronizing BGP with IGP | <b>undo synchronization</b> |

By default, BGP synchronizes with IGP.

3Com routers provide the ability to cancel BGP and IGP synchronization so the route from IBGP can be distributed without continuously checking if the IGP route still exists.

The synchronization of a border router can be shut down safely in the following cases:

- All the routers of an AS can form an IBGP totally-closed network. In such a case, a route known from any border router's EBGP can be automatically transferred to any other router through IBGP so that the connection of the AS is insured.
- When AS is not a transitional AS.

### Configuring the Interactions between BGP and an IGP

BGP can import route information that is found by running IGP in another AS to its own AS.

Perform the following configurations in BGP view.

**Table 550** Configure Route Import for BGP

| Operation                         | Command                                                               |
|-----------------------------------|-----------------------------------------------------------------------|
| Configure route import for BGP    | <b>import-route protocol [ med med ] [ route-policy policy-name ]</b> |
| Cancel route distribution for BGP | <b>undo import-route protocol</b>                                     |

By default, BGP does not import routes from other domains into the routing table.

The **protocol** attribute specifies the source routing domain that can be imported. At present, BGP can import routes domain such as connected, static, RIP, OSPF and OSPF-ASE.

See “Configure Route Import” in “Configuration of IP Routing Policy” for the details of routing import.

The **import-route** command cannot import the default route into BGP, so you must use the **default-information** command to import the default route into BGP.

Perform the following configurations in BGP view.

**Table 551** Allow the Import of Network 0.0.0.0 into the BGP

| Operation                                          | Command                         |
|----------------------------------------------------|---------------------------------|
| Allow the import of network 0.0.0.0 into the BGP   | <b>default-information</b>      |
| Disable the import of network 0.0.0.0 into the BGP | <b>undo default-information</b> |

By default, the import of network 0.0.0.0 into BGP is disabled.

### Defining an Access List Entry, an AS Path-list Entry, a Routing Policy

This section describes the configuration of an access list, an AS path list, and a routing policy.

#### Define an access list entry

See "Access Control List" in [\\*\\*\\*\\*need proper ref here 3Com Router Operation Manual \(Security Configuration\)\\*\\*\\*\\*\\*](#). for more details.

#### Define an AS Path-list entry

There is an AS path field in the routing information packet of the BGP protocol. When the BGP protocol operates with the switching routing information, the path of the routing information crossing the AS is recorded in this field. **aspath-list** is identified with *aspath-list-number*. When defining **aspath-list**, you can specify an aspath regular expression used to match the aspath field in the routing information. Use **aspath-list** to match the aspath field in the BGP routing information, filtering the information that does not meet the conditions. You can define multiple aspath-lists for one list number so that one list number represents a group of aspath-lists. Each AS path list is identified with numbers.

Perform the following configurations in system view.

**Table 552** Define a BGP-related ACL Entry

| Operation                      | Command                                                                                        |
|--------------------------------|------------------------------------------------------------------------------------------------|
| Define a BGP-related ACL entry | <b>ip as-path acl <i>aspath-list-number</i> { permit   deny } <i>as-regular-expression</i></b> |
| Remove a BGP-related ACL entry | <b>undo ip as-path acl <i>aspath-list-number</i></b>                                           |

By default, no access list entry is defined.

In the matching process, many *aspath-list-number* use Boolean "OR" operation so that if the routing information passes one item, information is filtered by the as-path list identified with this list number.

#### Define a routing policy

A routing policy is an important way for BGP to implement the route strategy. According to the matching result of the route attribute, BGP decides on the operations to be applied on a route attribute. In each routing policy, there can be several matching rules, labeled with a serial number. When importing a route, it is compared to a rule by number, from small to large. When the first matched rule is found, the matching process is completed. If no matched rules are found, router reception and transmission is canceled.

Perform the following configurations in system view.

**Table 553** Define a Routing Policy

| Operation                                                      | Command                                                                                   |
|----------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Define a routing policy and enter into the Routing policy view | <code>route-policy <i>policy-name</i> { permit   deny } [ <i>seq-number</i> ]</code>      |
| Remove a specified routing policy                              | <code>undo route-policy <i>policy-name</i> [ permit   deny ] [ <i>seq-number</i> ]</code> |

### Define a match rule

Perform the following configurations in BGP Routing policy view.

**Table 554** Define a Match Rules

| Operation                                                                                        | Command                                                                                                                           |
|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Specify a BGP AS path list to be matched in routing policy                                       | <code>if-match as-path <i>aspath-list-number</i></code>                                                                           |
| Delete a BGP AS path list to be matched in routing policy                                        | <code>undo if-match as-path</code>                                                                                                |
| Specify BGP community list number to be matched in routing policy.                               | <code>if-match community { <i>standard-community-list-number</i> [ exact-match ]   <i>extended-community-list-number</i> }</code> |
| Delete BGP community list                                                                        | <code>undo if-match community</code>                                                                                              |
| Define the matched routing access control list and prefix list in routing policy.                | <code>if-match ip address { <i>acl-number</i>   ip-prefix <i>prefix-list-name</i> }</code>                                        |
| Remove a standard access list or a prefix list                                                   | <code>undo if-match ip address [ ip-prefix ]</code>                                                                               |
| Define matched the type of interface                                                             | <code>if-match interface [ <i>type number</i> ]</code>                                                                            |
| Remove the matched interface                                                                     | <code>undo if-match interface</code>                                                                                              |
| Specify the next hop to be matched in Route-policy by an access list or an prefix list specified | <code>if-match ip next-hop { <i>acl-number</i>   ip-prefix <i>prefix-list-name</i> }</code>                                       |
| Remove the destination address of the matched route                                              | <code>undo if-match ip next-hop [ ip-prefix ]</code>                                                                              |
| Define matched the specified cost                                                                | <code>if-match cost <i>cost</i></code>                                                                                            |
| Delete the specified cost                                                                        | <code>undo if-match cost</code>                                                                                                   |

By default, AS regular expression, community list, interface type, IP address range, and metric value are not matched.

See “Define matching rules” of “Configuration of IP Routing Policy” for details.

### Define an apply clause

Perform the following configurations in Routing policy view.

**Table 555** Define An Apply Clause

| Operation                                  | Command                                              |
|--------------------------------------------|------------------------------------------------------|
| Set the BGP AS path access list            | <code>apply as-path <i>aspath-list-number</i></code> |
| Delete BGP AS-path attribute to BGP routes | <code>undo apply as-path</code>                      |

| Operation                                                          | Command                                                                                                                             |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Set the communities attributes                                     | <code>apply community { { [aa:nn ] [ no-export-subconfed ] [ no-advertise ] [ no-export ] } [ additive ]   none   additive }</code> |
| Delete the communities attributes                                  | <code>undo apply community</code>                                                                                                   |
| Set the next hop of BGP routing information                        | <code>apply ip next-hop ip-address</code>                                                                                           |
| delete the next hop of BGP routing                                 | <code>undo apply ip next-hop</code>                                                                                                 |
| Set the local preference value of source route                     | <code>apply local-preference value</code>                                                                                           |
| Cancel the local preference value of source route                  | <code>undo apply local-preference</code>                                                                                            |
| Apply cost to the imported routes                                  | <code>apply cost cost</code>                                                                                                        |
| Restore the destination routing protocol's cost value              | <code>undo apply cost</code>                                                                                                        |
| Set the origin attribute of the original route in the Route-policy | <code>apply origin { igp   egp as-number   incomplete }</code>                                                                      |
| Remove the origin attribute                                        | <code>undo apply origin</code>                                                                                                      |

By default, AS serial number, BGP community attribute, next hop, local preference, metric value, and origin attributes are not applied.

See " Define Apply Clause " of " Configuration of IP Routing Policy" for details.

### Configuring a Route Filter for BGP

Perform the following configurations in BGP view.

Configure a route filter for information received by BGP

**Table 556** Filter Routing Information Received from BGP

| Operation                                                                                                                  | Command                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Filter routing information received from a specified gateway                                                               | <code>filter-policy gateway prefix-list-name import</code>                                       |
| Change or cancel filtering the routing information received from a specified gateway                                       | <code>undo filter-policy gateway prefix-list-name import</code>                                  |
| Filter the routing information received                                                                                    | <code>filter-policy {acl-number   ip-prefix prefix-list-name } import</code>                     |
| Change or cancel filtering routing information received                                                                    | <code>undo filter-policy {acl-number   ip-prefix prefix-list-name } import</code>                |
| Configure to filter the routing information received from the specified address and that matching <i>prefix-list</i> .     | <code>filter-policy ip-prefix prefix-list-name { gateway prefix-list-name   import }</code>      |
| Configure not to filter the routing information received from the specified address and that matching <i>prefix-list</i> . | <code>undo filter-policy ip-prefix prefix-list-name { gateway prefix-list-name   import }</code> |

**Configure Filtering Route Information being Advertised by BGP****Table 557** Filter Routing Information Being Advertised by BGP

| Operation                                                    | Command                                                                                        |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Filter routing information being advertised by BGP           | <code>filter-policy {acl-number   ip-prefix prefix-list-name } export [ protocol ]</code>      |
| Cancel filtering routing information being advertised by BGP | <code>undo filter-policy {acl-number   ip-prefix prefix-list-name } export [ protocol ]</code> |

By default, BGP does not filter any route information that is received or advertised.

`protocol` specifies the routing domain that can will be filtered. At present, BGP can filter route domains such as connected, static, OSPF and OSPF-ASE.

See “Configure Route Filter” of “Configuration of IP Routing Policy” for details.

**Resetting BGP Connections**

After modifying a BGP configuration, you must turn off the current BGP connections and reset BGP connections to make the new configuration effective.

Perform the following configurations in system view.

**Table 558** Reset BGP Connections

| Operation                                                                                | Command                                                       |
|------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Reset BGP connection                                                                     | <code>reset bgp { all   peer-id }</code>                      |
| Clear routing flapping attenuation information and cancel the dampening over the routes. | <code>reset bgp dampening [ network-address [ mask ] ]</code> |
| Reset the BGP connection of a specified peer or all members of a peer group              | <code>reset bgp group group-name</code>                       |

**Displaying and Debugging BGP****Table 559** Display and Debug BGP

| Operation                                                                         | Command                                                                                                                             |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Display BGP path information                                                      | <code>display bgp paths as-regular-expression</code>                                                                                |
| Display AS filtered path information in BGP                                       | <code>display ip as-path-acl acl-number</code>                                                                                      |
| Display the routing information of the specified IP address in the routing table. | <code>display bgp routing-table ip-address [ mask ]</code>                                                                          |
| Display CIDR route                                                                | <code>display bgp routing-table cidr</code>                                                                                         |
| Display routing information of the specified BGP community                        | <code>display bgp routing-table community [ [aa:nn ] [ no-export-subconfed ] [ no-advertise] [ no-export ] ] [ exact-match ]</code> |
| Display routing information of permitted in the specified BGP community list      | <code>display bgp routing-table comm-list community-list-number [ exact-match]</code>                                               |
| Display Dampening route                                                           | <code>display bgp routing-table dampened</code>                                                                                     |
| Display the route matching the specified access list                              | <code>display bgp routing-table acl acl-number</code>                                                                               |

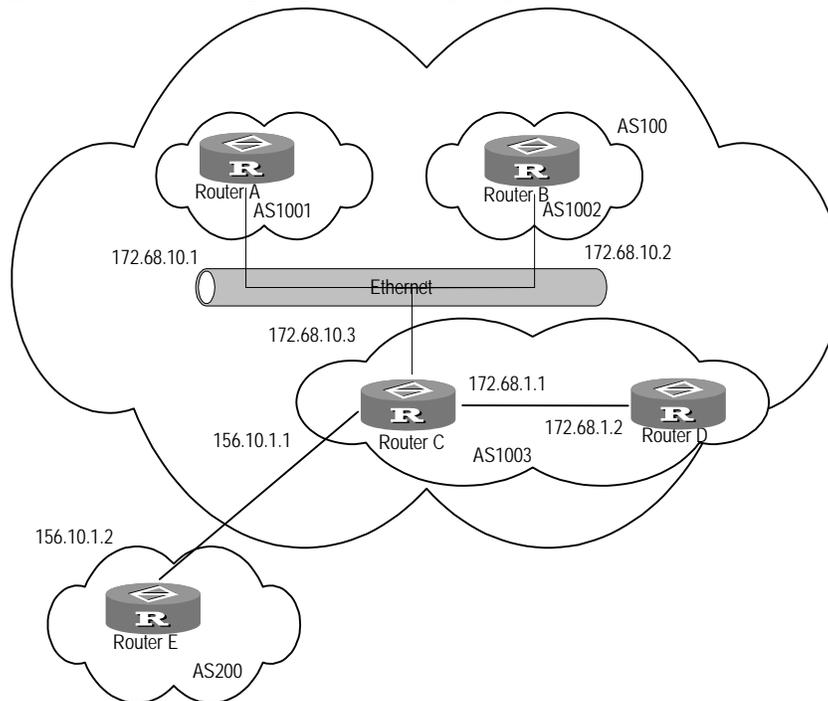
| Operation                                           | Command                                                                                                                                                                       |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display route flap information                      | <code>display bgp routing-table flap-information [ { regular-expression as-regular-expression }   { acl acl-number }   { network-address [ mask [ longer-match ] ] } ]</code> |
| Display the route with inconsistent source AS       | <code>display bgp routing-table different-origin-as</code>                                                                                                                    |
| Display peer information                            | <code>display bgp peer [ peer-address ]</code>                                                                                                                                |
| Display routing information distributed through BGP | <code>display bgp routing-table network</code>                                                                                                                                |
| Display peer group information                      | <code>display bgp group [ group-name ]</code>                                                                                                                                 |
| -table regular-express                              | <code>display bgp routing-table regular-expression as-regular-expression</code>                                                                                               |
| Display BGP route summary information               | <code>display bgp summary</code>                                                                                                                                              |
| Display the configured routing policy information   | <code>display route-policy policy-name</code>                                                                                                                                 |
| Enable BGP packet debugging.                        | <code>debugging bgp { all   event   { keepalive   open   packet   update } [ receive   send ] [ verbose ] }</code>                                                            |
| Disable BGP packet debugging                        | <code>undo debugging bgp { all   event   keepalive   open   packet   update }</code>                                                                                          |

## BGP Configuration Example

This section describes several different configurations of BGP with a suggested procedure for each configuration.

### Configuring the AS Confederation Attribute

As shown in the following diagram, AS 100 is divided into 3 sub-ASs: 1001, 1002, 1003, which are configured with EBGP, confederation EBGP and IBGP.

**Figure 154** Networking diagram of configuring AS confederation**1** Configure Router A:

```
[RouterA] bgp 1001
[RouterA-bgp] undo synchronization
[RouterA-bgp] confederation id 100
[RouterA-bgp] confederation peer-as 1002 1003
[RouterA-bgp] peer 172.68.10.2 as-number 1002
[RouterA-bgp] peer 172.68.10.3 as-number 1003
```

**2** Configure Router B:

```
[RouterB] bgp 1002
[RouterA-bgp] undo synchronization
[RouterB-bgp] confederation id 100
[RouterB-bgp] confederation peer-as 1001 1003
[RouterB-bgp] peer 172.68.10.1 as-number 1001
[RouterB-bgp] peer 172.68.10.3 as-number 1003
```

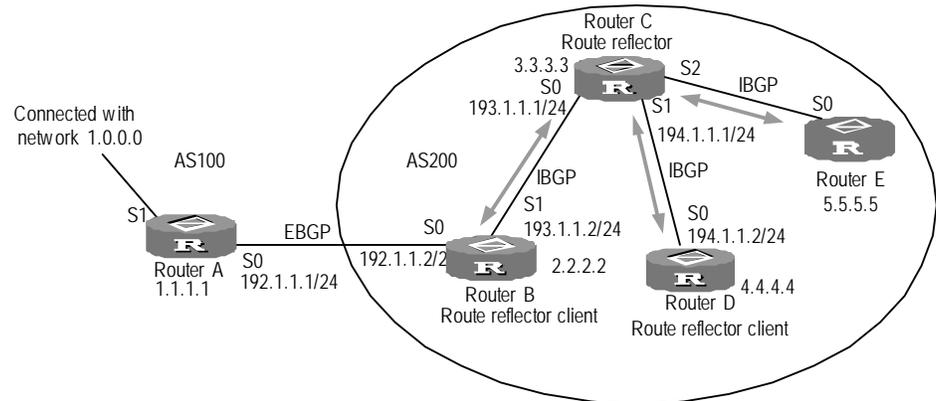
**3** Configure Router C:

```
[RouterC] bgp 1003
[RouterA-bgp] undo synchronization
[RouterC-bgp] confederation id 100
[RouterC-bgp] confederation peer-as 1001 1002
[RouterC-bgp] peer 172.68.10.1 as-number 1001
[RouterC-bgp] peer 172.68.10.2 as-number 1002
[RouterC-bgp] peer 156.10.1.2 as-number 200
[RouterC-bgp] peer 172.68.1.2 as-number 1003
```

**Configuring BGP Route Reflector**

Router B receives a BGP update message and forwards the update to Router C, which is configured as a route reflector and has two clients: Router B and Router D. When Router C receives routing update from Router B, it reflects the information to Router D. Therefore, an IBGP connection is not necessary between Router B and Router D, because Router C will reflect the information to Router D.

Figure 155 Networking diagram of configuring route reflector



### 1 Configure Router A:

```
[RouterA] bgp 100
[RouterA-bgp] undo synchronization
[RouterA-bgp] peer 192.1.1.2 as-number 200
[RouterA-bgp] interface serial 0
[RouterA-Serial0] ip address 192.1.1.1 255.255.255.0
```

### 2 Configure Router B:

#### a Configure BGP peers

```
[RouterB] bgp 200
[RouterA-bgp] undo synchronization
[RouterB-bgp] peer 192.1.1.1 as-number 100
[RouterB-bgp] peer 193.1.1.1 as-number 200
```

#### b Enable OSPF

```
[RouterB] ospf enable
```

#### c Configure Serial 0

```
[RouterB-ospf] interface serial 0
[RouterB-Serial0] ip address 192.1.1.2 255.255.255.0
```

#### d Configure Serial 1

```
[RouterB-Serial0] interface serial 1
[RouterB-Serial1] ip address 193.1.1.2 255.255.255.0
[RouterB-Serial1] ospf enable area 0
```

### 3 Configure Router C:

#### a Configure BGP peers and route reflector clients

```
[RouterC] bgp 200
[RouterA-bgp] undo synchronization
[RouterC-bgp] peer 193.1.1.2 as-number 200 reflect-client
[RouterC-bgp] peer 193.1.1.2 reflect-client
[RouterC-bgp] peer 194.1.1.2 as-number 200 reflect-client
[RouterC-bgp] peer 194.1.1.2 reflect-client
```

#### b Enable OSPF

```
[RouterC] ospf enable
```

#### c Configure Serial 0

```
[RouterC-ospf] interface serial 0
```

```
[RouterC-Serial0] ip address 193.1.1.1 255.255.255.0
```

**d** Configure Serial 1

```
[RouterC-Serial0] interface serial 1
[RouterC-Serial1] ip address 194.1.1.1 255.255.255.0
[RouterC-Serial1] ospf enable area 0
```

**4** Configure Router D:

**a** Configure BGP peers

```
[RouterD] bgp 200
[RouterA-bgp] undo synchronization
[RouterD-bgp] peer 194.1.1.1 as-number 200
```

**b** Enable OSPF

```
[RouterD] ospf enable
```

**c** Configure Serial 0

```
[RouterD-ospf] interface serial 0
[RouterD-Serial0] ip address 194.1.1.2 255.255.255.0
[RouterD-Serial0] ospf enable area 0
```

View BGP routing table on Router B with **display bgp routing-table** command. Note that Router B knows that network 1.0.0.0 exists.

```
[RouterB] display bgp routing-table
network next hop metric localpref
1.0.0.0 192.1.1.1 0
```

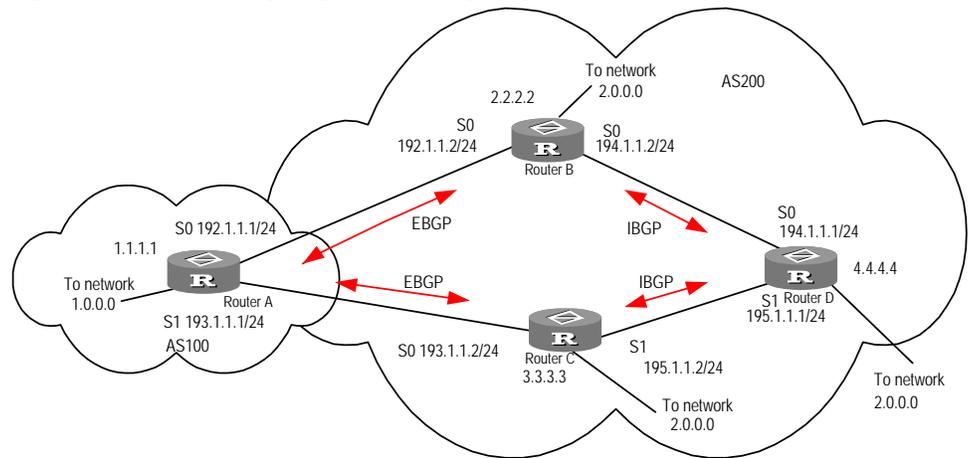
View BGP routing table on Router C with **display bgp routing-table** command. Note that Router C knows that network 1.0.0.0 exists.

```
[RouterD] display bgp routing-table
network next hop metric llocalpref
1.0.0.0 194.1.1.1 0 100
```

### Configuring BGP Path Selection

This example describes how the administrator manages the routing with the BGP attribute. All routers are configured with BGP. OSPF is used by IGP in AS200. Router A is in AS100, functioning as the BGP peer of Router B and Router C in AS200. When Router B and Router C run IBGP to Router D, Router D is also in AS200.

Figure 156 Networking diagram of configuring BGP path selection



### 1 Configure Router A:

```
[RouterA] interface serial 0
[RouterA-Serial0] ip address 192.1.1.1 255.255.255.0
[RouterA] interface serial 1
[RouterA-Serial1] ip address 193.1.1.1 255.255.255.0
[RouterA-Serial1] quit
```

#### a Start BGP

```
[RouterA] bgp 100
[RouterA-bgp] undo synchronization
```

#### b Specify BGP transmission network

```
[RouterA-bgp] network 1.0.0.0 mask 255.0.0.0
[RouterA-bgp] network 2.0.0.0 mask 255.0.0.0
```

#### c Configure peer

```
[RouterA-bgp] peer 192.1.1.2 as-number 200
[RouterA-bgp] peer 193.1.1.2 as-number 200
```

#### d Configure MED attribute of Router A

- Add access list to Router A and enable network 1.0.0.0.

```
[RouterA-bgp] acl 1
[RouterA-acl-1] rule permit source 1.0.0.0 0.255.255.255
```

- Define two routing diagram, namely set\_med\_50 and set\_med\_100. The first routing diagram is network 1.0.0.0. The MED attribute is 50, and the second MED attribute is 100.

```
[RouterA-acl-1] route-policy set_med_50 permit 1
[RouterA-route-policy] if-match ip address 1
[RouterA-route-policy] apply cost 50
[RouterA-route-policy] quit
[RouterA] route-policy set_med_100 permit 1
[RouterA-route-policy] if-match ip address 1
```

- [RouterA-route-policy] apply cost 100 Apply the routing diagram set\_med\_50 to the exit routing update of Router C (193.1.1.2). Apply the routing diagram set\_med\_100 to exit routing update of Router B (192.1.1.2).

```
[RouterA] bgp 100
[RouterA-bgp] peer 193.1.1.2 route-policy set_med_50 export
[RouterA-bgp] peer 192.1.1.2 route-policy set_med_100 export
```

**2** Configure Router B:

```
[RouterB] interface serial 0
[RouterB-Serial0] ip address 192.1.1.2 255.255.255.0
[RouterB] interface serial 1
[RouterB-Serial1] ip address 194.1.1.2 255.255.255.0
[RouterB] ospf enable
[RouterB-ospf] network 194.1.1.0 0.0.0.255 area 0
[RouterB-ospf] network 192.1.1.0 0.0.0.255 area 0
[RouterB] bgp 200
[RouterB-bgp] undo synchronization
[RouterB-bgp] peer 192.1.1.1 as-number 100
[RouterB-bgp] peer 194.1.1.1 as-number 200
[RouterB-bgp] peer 195.1.1.1.2 as-number 200
```

**3** Configure Router C:

```
[RouterC] interface serial 0
[RouterC -Serial] ip address 193.1.1.2 255.255.255.0
[RouterC] interface serial 1
[RouterC-Serial1] ip address 195.1.1.2 255.255.255.0
[RouterC] ospf enable
[RouterC-ospf] network 193.1.1.0 0.0.0.255 area 0
[RouterC-ospf] network 195.1.1.0 0.0.0.255 area 0
[RouterC] bgp 200
[RouterC-bgp] undo synchronization
[RouterC-bgp] peer 193.1.1.1 as-number 100
[RouterC-bgp] peer 194.1.1.2 as-number 200
[RouterC-bgp] peer 195.1.1.1 as-number 200
```

Set the local preference attribute of Router C.

- Add access list 1 to Router C and enable network 1.0.0.0.

```
[RouterC-bgp] acl 1
[RouterC-acl-1] rule permit source 1.0.0.0 0.255.255.255
```

- Define a routing diagram named localpref. In the diagram, the local preference of the route matching access list 1 is set to 200 and the local preference of the route not matching access list 1 is 100.

```
[RouterC-acl-1]route-policy localpref permit 1
[RouterC-route-policy] if-match ip address 1
[RouterC-route-policy] apply local-preference 200
[RouterC-route-policy] route-policy localpref permit 2
[RouterC-route-policy] apply local-preference 100
```

- Apply this routing diagram to the entry traffic from BGP peer 193.1.1.2 (Router A).

```
[RouterC] bgp200
[RouterC-bgp] peer 193.1.1.1 route-policy localpref import
```

**4** Configure Router D:

```
[RouterD] interface serial 0
[RouterD-Serial0] ip address 194.1.1.1 255.255.255.0
[RouterD] interface serial 1
[RouterD-Serial1] ip address 195.1.1.1 255.255.255.0
[RouterD] ospf enable
[RouterD-ospf]network 194.1.1.0 0.0.0.255 area 0
[RouterD-ospf]network 195.1.1.0 0.0.0.255 area 0
```

```
[RouterD-ospf] network 4.0.0.0 0.0.0.255 area 0
[RouterD] bgp 200
[RouterD-bgp] undo synchronization
[RouterD-bgp] peer 194.1.1.2 as-number 100
[RouterD-bgp] peer 194.1.1.2 as-number 200
```

To make the configuration effective, use the `reset bgp all` command to reset all BGP neighbors.



This chapter covers the following topics:

- IP Routing Policy Overview
- Configure IP Routing Policy
- Displaying and Debugging IP Routing Policy
- Configuring IP Routing Policy
- Troubleshooting IP Routing Policy

---

### IP Routing Policy Overview

During the information exchange with a peer router, the routing protocol may need to receive or distribute only part of the route information that complies with specific conditions; and to import only part of the route information learned by other protocols that satisfy the preset conditions. In addition, some attributes of the imported route information are set in order to satisfy the requirements of the protocol. The route strategy also provides measures for the routing protocol to implement these functions.

The route strategy consists of a series of rules, classified into three types and used for route information filtering in route advertisement, route receiving, and route import. Since defining a strategy is similar to defining a group of filters that are used during receiving or advertising route information or before the route information exchange between different protocols, route strategy is also called route filtering.

A common filter is the basis for route strategy implementation. The user defines some matching conditions as necessary, which are referred to when making the routing strategies. Apply these conditions to different objects such as the destination address of the routing information, and the router address publishing the routing information, to implement route information filtering.

A routing strategy provides five filters:

- 1 Routing policy
- 2 Access list
- 3 Aspath-list
- 4 Community-list
- 5 Prefix-list

These filters serve as the reference for the protocols to work out routing strategies.

- Routing Policy** A routing policy matches attributes of the given routing information and sets some attributes of the routing information when the conditions are matched. A routing policy contains several "if-match" clauses and "apply" clauses. The "if-match" clauses specify the matching conditions. The "apply" clauses specify the configuration commands that are executed when the filtering conditions specified by if-match clauses are satisfied.
- Access List** An access list can be divided into a standard access list and an extended access list. The standard access list is usually used for filtering routing information. When you define an access list, you need to specify the network segment range of an IP address, to match the destination network segment address or next hop address of the routing information and to filter the routing information not satisfying the conditions. If an extended access list is used, only the source address matching field is used to match the destination network segment of the routing information, while the IP address range used to match packet destination address specified in the extended access list should be ignored.
- Prefix-list** Prefix-list functions are similar to the functions of an access list, which may not be easily understood when used for routing information filtering, because it is in the format of packet filtering. `ip ip-prefix` is more flexible and comprehensible. When applied to routing information filtering, its matching object is the destination address information of the routing information. It can also be directly used to the router object (gateway), so that the local routing protocol can only receive the routing information distributed by specific routers. The addresses of these filters must be filtered by prefix-list. In this case, the matching object of `ip ip-prefix` is the source address of the IP header of the route packet.
- A prefix-list is identified with the list name and consists of several parts, with *sequence-number* specifying the matching order of these parts. In each part, you can specify a matching range in the form of the network prefix. Different parts of different *sequence-numbers* are matched using Boolean "OR" operations. When the routing information matches a specific part of *prefix-list*, it is considered successfully filtered through the *prefix-list*.
- Aspath-list** Aspath-list is only used for the BGP protocol. There is an aspath field in the routing information packet of the BGP protocol. When the BGP protocol operates with the switching routing information, the path of the routing information crossing the AS is recorded in this field. Aspath-list is identified with *aspath-list-number*. When defining aspath-list, you can specify an aspath regular expression to match the aspath field in the routing information. You can use aspath-list to match the aspath field in the BGP routing information, and filter information that does not satisfy the conditions. Each list number can be defined with multiple aspath-lists, because one list number represents a group of aspath-lists. The matching process for *acl-numbers* uses Boolean "OR" operations, so a match with any one of the list is considered successful filtering of the routing information through the aspath list identified with this list number.
- The definition of *access-path-list* is implemented in the BGP configuration. See the description of the `ip as-path acl` command in "Define an AS Path-list entry".
- Community-list** Community-list is only used for the BGP protocol. In the routing information packet of the BGP protocol, there is a community attribute field, used to identify a

community. Actually, it is a method of grouping according to the destination address where the packets are sent. After grouping, the whole group of routing information should be distributed, received or imported. The community-list is an access list based on community information, used for the BGP protocol. Its matching object is the community field of BGP routing information.

Community-list definition is already implemented in BGP configuration. See the description of the `ip community-list` command in “Configuring a BGP Community”.

## Configure IP Routing Policy

Configuring an IP routing policy includes tasks that are described in the following sections:

- Defining a Routing Policy
- Define a Matching Rules
- Defining an Apply Clause
- Configuring Route Import
- Defining an IP Prefix List
- Configuring Route Filter

## Defining a Routing Policy

A routing policy consists of several parts and each part has its own `if-match` clauses and applies clauses, with `sequence-number` specifying the matching order of these parts.

Perform the following configurations in system view.

**Table 560** Define a Routing Policy

| Operation                                                       | Command                                                                    |
|-----------------------------------------------------------------|----------------------------------------------------------------------------|
| Define a routing policy and enter into the routing policy view. | <code>route-policy policy-name { permit   deny } { seq-number }</code>     |
| Delete a routing policy                                         | <code>undo route-policy policy-name [ permit   deny ] [seq-number ]</code> |

By default, no routing policy is defined.

**permit** specifies the matching mode of the defined routing policy node as permit mode. When the route item satisfies all if-match clauses of the node, it is permitted to pass the filtering of this node and execute apply clauses of this node. If the route item does not satisfy the if-match clauses of this node, the next node of this routing policy is tested.

**deny** specifies the matching mode of the defined routing policy node as deny mode. When the route item satisfies all if-match clauses of this node, it is rejected and the next node is not tested.

Please note that the parts of different `seq-number` use Boolean “OR” operations. Namely, route information matches every part in turn. Through a certain part of routing policy defines filtering through this routing policy.

**Define a Matching Rules** The **if-match** clause defines matching rules to meet the filtering conditions of the routing information of the current routing policy. The matched objects are the attributes of this routing information.

Perform the following configurations in routing policy view.

**Table 561** Configure a Matching Rules

| Operation                                                                                 | Command                                                                                                                                         |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Specify the AS number to be matched at the beginning of the AS path in the route-policy.  | <b>if-match as-path aspath-list-number</b>                                                                                                      |
| Remove the AS number to be matched from the beginning of the AS path in the route-policy. | <b>undo if-match as-path</b>                                                                                                                    |
| Specify the BGP community attributes to be matched in the route-policy.                   | <b>if-match community-list</b><br><b>{standard-community-list-number [</b><br><b>exact-match ]  </b><br><b>extended-community-list-number }</b> |
| Remove the BGP community attributes to be matched from the route-policy.                  | <b>undo if-match community-list</b>                                                                                                             |
| Specify the ACL and prefix list to be matched in the route-policy.                        | <b>if-match ip address { acl-number  </b><br><b>ip-prefix prefix-list-name }</b>                                                                |
| Remove the ACL and prefix list to be matched from the route-policy.                       | <b>undo if-match ip address [ ip-prefix</b><br><b>]</b>                                                                                         |
| Specify the interface to be matched in the route-policy.                                  | <b>if-match interface [ type number ]</b>                                                                                                       |
| Remove the interface to be matched from the route-policy.                                 | <b>undo if-match interface</b>                                                                                                                  |
| Specify the route-policy-matching next-hop of the routing information.                    | <b>if-match ip next-hop { acl-number  </b><br><b>ip-prefix prefix-list-name }</b>                                                               |
| Remove the route-policy-matching next-hop of the routing information.                     | <b>undo if-match ip next-hop [ ip-prefix</b><br><b>]</b>                                                                                        |
| Specify the cost of the routing information to be matched in the route-policy.            | <b>if-match cost cost</b>                                                                                                                       |
| Remove the cost of the routing information to be matched in the route-policy              | <b>undo if-match cost</b>                                                                                                                       |
| Specify the tag of OSPF routing information to be matched in the route-policy.            | <b>if-match tag tag-value</b>                                                                                                                   |
| Delete the tag of OSPF routing information to be matched in the route-policy.             | <b>undo if-match tag</b>                                                                                                                        |
| Specify the matched OSPF route type (i.e. internal or external) in the routing policy.    | <b>if-match route-type { internal  </b><br><b>external }</b>                                                                                    |
| Delete the matched OSPF route type in the routing policy                                  | <b>undo if-match route-type</b>                                                                                                                 |

By default, AS regular expression, community list, interface type, IP address range, metric value, OSPF tag field and OSPF routing information type are not matched.

Note that:

- For one routing policy node, the if-match clauses of the same part use Boolean “AND” operations in the matching process so the routing information cannot

be filtered through the routing policy unless it matches all if-match clauses of this part and it can execute the operation of the apply sub-clause.

- If an if-match clause is not specified, all routing information is filtered through the policy of this node.

### Defining an Apply Clause

The **apply** clause specifies the configuration commands that are executed after the filtering conditions specified by the **if-match** clause are satisfied. The commands are used to modify attributes of the routing information.

Perform the following configurations in Routing policy view.

**Table 562** Define a Setting Clause

| Operation                                                              | Command                                                                                                   |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Specify the AS number ahead of the original AS path in Routing policy. | <b>apply as-path aspath-list-number</b>                                                                   |
| Cancel the AS number ahead of the original AS path in Routing policy.  | <b>undo apply as-path</b>                                                                                 |
| Set BGP community attribute in Routing policy                          | <b>apply community { { aa:nn   no-export-subconfed   no-advertise   no-export } [ additive ]   none }</b> |
| Cancel BGP community attribute in Routing policy                       | <b>undo apply community</b>                                                                               |
| Set the next hop address of BGP routing information.                   | <b>apply ip next-hop ip-address</b>                                                                       |
| Cancel the next hop address of BGP routing information.                | <b>undo apply ip next-hop</b>                                                                             |
| Set the local preference of BGP routing information.                   | <b>apply local-preference value</b>                                                                       |
| Cancel the local preference of BGP routing information.                | <b>undo apply local-preference</b>                                                                        |
| Set the cost of routing information.                                   | <b>apply cost cost</b>                                                                                    |
| Cancel the cost of routing information.                                | <b>undo apply cost</b>                                                                                    |
| Set the origin attribute of the original route in the Route-policy     | <b>apply origin { igp   egp as-number   incomplete }</b>                                                  |
| Remove the origin attribute of the original route in the Route-policy. | <b>undo apply origin</b>                                                                                  |
| Set the OSPF tag value                                                 | <b>apply tag tag-value</b>                                                                                |
| Cancel the OSPF tag value                                              | <b>undo apply tag</b>                                                                                     |

By default, AS number, BGP community attribute, next hop, local preference, metric value, origin attribute and routing information tag field are not set.

### Configuring Route Import

Different routing protocols can import and share the routing information. When the routing information of other protocols is imported, the inappropriate routing information can be filtered. The metric of distributed destination routing protocol cannot exchange with that of the imported original routing protocol. At this time, a route metric should be specified for the imported route.

Perform the following configurations in RIP view, OSPF view, or BGP view.

**Table 563** Configure Route Import

| Operation                      | Command                                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------|
| Configure route import in RIP  | <code>import-route protocol [ cost cost ] [ route-policy route-policy-name ]</code>                          |
| Cancel route import            | <code>undo import-route protocol</code>                                                                      |
| Configure route import in OSPF | <code>import-route protocol [ cost cost ] [ type 1   2 ] [ tag tag-value ]</code>                            |
| Cancel route import            | <code>undo import-route protocol [ cost cost ] [ type 1   2 ] [ tag tag-value ]</code>                       |
| Configure route import in BGP  | <code>import-route protocol [ med med ] [ tag tag-value ] [ type 1   2 ] [ route-policy policy-name ]</code> |
| Cancel route import            | <code>undo import-route protocol</code>                                                                      |

By default, a protocol does not import routes from other domains into the its routing table.

**protocol** specifies the source routing domain that can be imported. At present, it can import routes domain such as direct, static, RIP, OSPF, OSPF-ASE and BGP.

Software supports importing route information found by the ollowing protocols into the route table:

- direct: network segment (or host) route directly connected to the router's interface
- static: static route
- RIP: routes discovered by rip
- OSPF: routes discovered by ospf
- OSPF-ASE: external routes discovered by ospf
- BGP: routes discovered by bgp

**med med** or **cost cost**: specifies the metric value of the imported routes.

**bandwidth** is the route bandwidth, ranging from 1 to 4294967295 kbyte/s.

**delay** is the route time delay, each unit stands for 10μs, ranging from 1 to 16777215

**reliability** is the channel reliability, ranging 0 to 255. 255 stands for 100% creditable.

**loading** is the channel seizure rate, ranging 1 to 255, 255 stands for 100% seized.

**mtu** is the maximum transfer unit of route, ranging from 1 to 65535 byte.

**route-policy policy-name** specifies imported routes which matches the specified routing policy name. This item can be used in the routing protocol configuration except in the OSPF view.

**tag tag-value** sets the tag value of the imported route when ospf is importing other protocol routes.

**type** is the type of ospf external route corresponding to the imported route when ospf is importing other protocol routes. **type 1** refers to external route type 1 and **type 2** refers to external route type 2.

The metric value of the imported route can be set as the following:

- 1 Specify the metric value with the **apply cost** command.
- 2 Filter the route with routing policy and set attributes for the route matching the conditions.
- 3 If neither of the above is specified, the imported route uses the default metric value. The default metric can be specified with the **default-med** command.

When both routing policy and med value are specified, the routing information matching the routing policy will use the metric specified by the **apply** command of a routing policy.

## Defining an IP Prefix List

An IP prefix list is identified with the list name and consists of several parts, with the *sequence-number* specifying the matching order of these parts. In each part, you can specify an individual matching range in the form of network prefix.

It should be noted that:

- In the process of matching, different parts of different *sequence-numbers* use Boolean “OR” operations and the routing information matches different parts in turn. Matched with a specific part of the IP prefix list is considered as successfully filter through this IP prefix list

Perform the following configurations in system view.

**Table 564** Define an IP Prefix List

| Operation                | Command                                                                                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Define an IP prefix list | <b>ip ip-prefix <i>prefix-list-name</i> [ index <i>index-number</i> ] { permit   deny } <i>network/len</i> [ greater-equal <i>ge-value</i> ] [ less-equal <i>le-value</i> ]</b> |
| Cancel an IP prefix list | <b>undo ip ip-prefix <i>prefix-list-name</i> [ index <i>seq-number</i> ] [ permit   deny ]</b>                                                                                  |

By default, no IP prefix list is defined.

## Configuring Route Filter

In some cases, only the routing information that meets the condition should be distributed or imported, to prevent the neighboring routers from receiving private information of other routes. A prefix-list or access list in the route strategy is used to filter the routing information.

Perform the following configurations in RIP view, OSPF view, or BGP view.

- 1 Configure filtering route information received
 

Define a strategic rule and quote an ACL or prefix-list to filter the routing information that does not meet the requirements when receiving routes. Specify an IP prefix list through **gateway** keywords, filtering the address of the information router to receive only the updating messages from specific neighboring routers.

**Table 565** Configure Filtering Route Information Received

| Operation                                                                                                                                          | Command                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Filter the route information received from a specified gateway                                                                                     | <code>filter-policy gateway<br/>prefix-list-name import</code>                                     |
| Change or cancel filtering the route information received from a specified gateway                                                                 | <code>undo filter-policy gateway<br/>prefix-list-name import</code>                                |
| Filter the route information received                                                                                                              | <code>filter-policy {acl-number  <br/>ip-prefix prefix-list-name } import</code>                   |
| Change or cancel filtering route information received                                                                                              | <code>undo filter-policy {acl-number  <br/>ip-prefix prefix-list-name } import</code>              |
| Filter routing information received from a specified gateway and the routing information received according to prefix-list                         | <code>filter-policy ip-prefix<br/>prefix-list-name gateway<br/>prefix-list-name import</code>      |
| Change or cancel filtering the routing information received from a specified gateway and the routing information received according to prefix-list | <code>undo filter-policy ip-prefix<br/>prefix-list-name gateway<br/>prefix-list-name import</code> |

## 2 Configure filtering the route information being advertised

Define a strategic rule and quote an ACL or prefix-list to filter the routing information that does not meet the requirements when receiving routes. Specify the *protocol* to filter only the distributed *protocol* routing information.

**Table 566** Configure Filtering Route Information Being Advertised

| Operation                                                     | Command                                                                                             |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Filter the route information being advertised                 | <code>filter-policy {acl-number  <br/>ip-prefix prefix-list-name } export [ protocol ]</code>       |
| Change or cancel filtering route information being advertised | <code>undo filter-policy { acl-number  <br/>ip-prefix prefix-list-name } export [ protocol ]</code> |

By default, no route information received or being advertised is filtered.

*protocol* specifies the routing domain that can will be filtered. At present, it can filter routes domain as follows:

- direct: the network segment (host) route directly connected with the local interface.
- static: static route
- RIP: route discovered by RIP protocol+
- OSPF: route discovered by OSPF protocol
- OSPF-ASE: external route discovered by OSPF protocol
- BGP: route discovered by BGP protocol

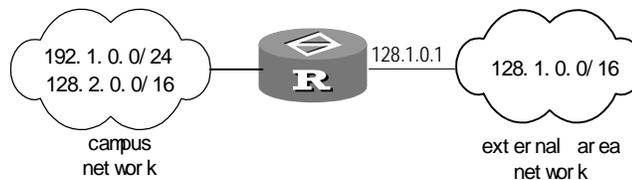
**Table 567** Display and Debug of IP Routing Policy

| Operation                          | Command                                                |
|------------------------------------|--------------------------------------------------------|
| Display routing policy             | <code>display route-policy [ policy-name ]</code>      |
| Display IP prefix list information | <code>display ip ip-prefix [ prefix-list-name ]</code> |

## Configuring IP Routing Policy

This example explains how an OSPF protocol selectively imports an RIP route.

As shown in the following figure, the router connects a campus network which uses RIP as its internal routing protocol and an external area network which uses OSPF routing protocol. The router advertises some routing information of the campus network around the external area network. To implement this, the OSPF protocol imports a routing policy to perform route filtering in order to import the RIP information. The routing policy consists of two nodes, and the routing information of 192.1.0.0/24 and 128.2.0.0/16 is advertised by the OSPF protocol with different weighting values.

**Figure 157** Networking diagram of OSPF importing route distributed by RIP

### 1 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
```

### 2 Configure Routing policy

```
[Router]route-policy r1 permit 10
[Router-route-policy]if-match ip address ip-prefix p1
[Router-route-policy]route-policy r1 permit 20
[Router-route-policy]if-match ip address ip-prefix p2
[Router-route-policy]quit
```

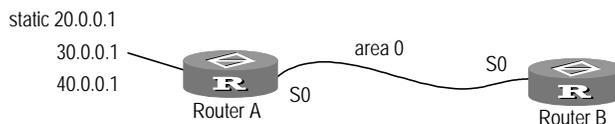
### 3 Configure OSPF

```
[Router]ospf enable
[Router-ospf]import-route rip route-policy r1
[Router-ospf]interface ethernet 0
[Router-Ethernet0]ip address 128.1.0.1 255.255.255.0
[Router-Ethernet0]ospf enable area 0
```

## Configuring Filtering Route Information for OSPF

### I. Networking requirements

- Router A is connected to Router B, and the link layer encapsulates PPP protocol.
- Router A receives three static routes and the next hop is an Ethernet interface.
- Router B is configured with filtering rules, making the 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 those of network segment 30.0.0.0 are filtered.

**Figure 158** Networking diagram of configuring OSPF route filtering**1** Configure Router A:**a** Configure static routes:

```
[RouterA] ip route-static 20.0.0.1 32 ethernet 0
[RouterA] ip route-static 30.0.0.1 32 ethernet 0
[RouterA] ip route-static 40.0.0.1 32 ethernet 0
```

**b** Start OSPF protocol.

```
[RouterA] router id 1.1.1.1
[RouterA] ospf enable
```

**c** Import static route

```
[RouterA-ospf] import-route static
```

**d** Configure Serial 0, and specify id of area including the interface.

```
[RouterA-ospf] interface serial 0
[RouterA-Serial0] ip address 10.0.0.1 255.0.0.0
[RouterA-Serial0] link-protocol ppp
[RouterA-Serial0] interface serial 0
[RouterA-Serial0] ospf enable area 0
```

**2** Configure Router B:**a** Configure an access list:

```
[RouterB] acl 1
[RouterB-acl-1] rule deny source 30.0.0.0 255.255.255.0
[RouterB-acl-1] permit any
[RouterB-acl-1] quit
```

**b** Start OSPF protocol and configure the area number of this interface

```
[RouterB] router id 2.2.2.2
[RouterB] ospf enable
```

**c** Configure filtering route information received for OSPF

```
[RouterB-ospf] filter-policy 1 import
```

**d** Configure IP address of Serial0, encapsulated to PPP protocol.

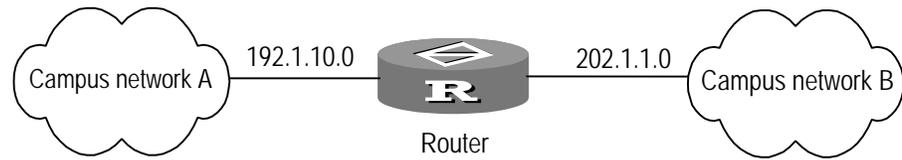
```
[RouterB-ospf] interface serial 0
[RouterB-Serial0] link-protocol ppp
[RouterB-Serial0] ip address 10.0.0.2 255.0.0.0
[RouterB-Serial0] ospf enable area 0
```

**Configuring Filtering Route Information**

This example describes how OSPF imports RIP route selectively.

The router connects campus network A and campus network B, both of which use RIP as the internal routing protocol. The router needs to distribute the routes 192.1.1.0/24 and 192.1.2.0/24 of campus A in the local network. To achieve this function, RIP protocol on the router defines a filter-policy to filter the routing information, perform the route filtering function through quoting a prefix list.

**Figure 159** Networking diagram of filtering the distributed routing information



**1** Configure ip-prefix

```
[Router] ip ip-prefix p1 permit 192.1.1.0/24
```

**2** Configure RIP protocol

```
[Router] rip
[Router-rip] network 192.1.0.0
[Router-rip] network 202.1.1.0
[Router-rip] filter-policy ip-prefix p1 export
```

**Troubleshooting IP Routing Policy**

**Routing information cannot be filtered when the routing protocol is in normal operation**

Check the following:

- At least one node in the routing policy should be in permit matching mode. When a routing policy is used to filter routing information or a specific routing information does not pass the filtering of a node, the routing information is considered not passing the filtering of this routing policy. When all nodes of the routing policy are in deny mode, no routing information will pass the filtering of this routing policy.
- At least one item in the prefix-list should be in permit matching mode. The list items in deny mode can be defined to fast filtering routing information that does not meet the conditions. But if all list items are in deny mode, no route will pass the filtering of this prefix-list. Define a permit 0.0.0.0/0 list item after multiple items are defined in deny modes, so that all other routes will pass the filtering.

**When an ACL is quoted for filtering routing information and ACL definition is modified, the route strategy is not updated.**

In this case, reconfigure by quoting the strategy and rule of this ACL to inform the protocol of the ACL change. If other filters are quoted, this operation is not necessary and the protocols are informed of the change of the router.



This chapter covers the following topics:

- IP Policy Routing Overview
- Configuring IP Policy Routing
- Displaying and Debugging IP Policy Routing
- IP Policy Routing Configuration Example

---

### IP Policy Routing Overview

IP policy routing is a mechanism in which messages are transmitted and forwarded by strategy without going through the routing table. When a router is forwarding a packet by policy routing, it is first filtered by a route policy which decides the packets to be forwarded and to which router.

The user configures the IP policy for routing. It is composed of a group of `if-match` clauses and a group of `apply` clauses. Only when all `if-match` clauses of policy routings are fully satisfied are the `apply` clauses in the policy routings executed in sequence, to affect the message forwarding.

At present, two `if-match` clauses, `if-match length` and `if-match ip address`, are provided.

`Apply` clause defines the operation of the strategy. there are five `apply` clauses: `apply ip precedence`, `apply interface`, `apply ip next-hop`, `apply default interface`, `apply ip default next-hop`. They are executed in sequence until the operation can proceed.

There are two kinds of policy routings: interface policy routing and local policy routing. Interface policy routing is configured in interface view and performs strategic routing for messages from this interface. Local policy routing is configured in system view and performs policy routing for messages generated by this host. Generally, the local policy routing must not be configured.

The policy routing can be used for security and load balancing.

---

### Configuring IP Policy Routing

IP policy routing configuration includes:

- Creating a Routing Policy
- Define Match Rules
- Define Apply Clause
- Enabling and Disabling Local Policy Routing
- Enabling and Disabling Interface Policy Routing

### Creating a Routing Policy

The strategy specified with the strategy name may have several strategy points and each strategy point is specified with *sequence-num*. The smaller the *sequence-num*, the higher the preference and the defined strategy will be executed first. This strategy can be used to import routes and perform policy routing when IP messages are forwarded. When a routing policy is recreated, the configuration information of the new routing policy overwrites that of the old routing policy. The contents of the strategy is specified by if-match and apply clauses.

See “Configuring IP Routing Policy” for details.

Perform the following configurations in system view.

**Table 568** Create a Routing Policy

| Operation                                                      | Command                                                                   |
|----------------------------------------------------------------|---------------------------------------------------------------------------|
| Create a routing policy and enter into the Routing policy view | <code>route-policy policy-name { permit   deny } { seq-number }</code>    |
| Delete a routing policy                                        | <code>no route-policy policy-name [ permit   deny ] [ seq-number ]</code> |

**permit** means policy routing for the messages meets the conditions and **deny** means no policy routing for the message meets the conditions.

By default, no strategy is created.

### Define Match Rules

IP policy routing provides two if-match clauses that allow matching strategy according to IP message length and IP address. One strategy includes multiple if-match clauses, which can be used in combination.

Perform the following configurations in Routing policy view.

**Table 569** Define Match Rules

| Operation                                              | Command                                      |
|--------------------------------------------------------|----------------------------------------------|
| Specify IP message matching the length                 | <code>if-match length min-len max-len</code> |
| Remove IP message matching the length                  | <code>no if-match length</code>              |
| Specify IP address matching the specified access lists | <code>if-match ip address acl-number</code>  |
| Remove IP address matching the specified access lists  | <code>undo if-match ip address</code>        |

By default, no if-match clause is defined.

### Define Apply Clause

IP policy routing provides 5 apply clauses. One strategy includes multiple apply clauses, which can be used in combination.

Perform the following configurations in Routing policy view.

**Table 570** Define Apply Clause

| Operation              | Command                                     |
|------------------------|---------------------------------------------|
| Set message precedence | <code>apply ip precedence precedence</code> |

| Operation                                                      | Command                                           |
|----------------------------------------------------------------|---------------------------------------------------|
| Cancel apply clauses setting message precedence                | <code>undo apply ip precedence</code>             |
| Set message transmitting interface                             | <code>apply interface type number</code>          |
| Cancel apply clauses setting message transmitting interface    | <code>no apply interface</code>                   |
| Set message default transmitting interface                     | <code>apply default interface type number</code>  |
| Cancel apply clauses setting message default sending interface | <code>undo apply default interface</code>         |
| Set message next-hop                                           | <code>apply ip next-hop ip-address</code>         |
| Cancel apply clauses setting message next-hop                  | <code>undo apply ip next-hop</code>               |
| Set message default next-hop                                   | <code>apply ip default next-hop ip-address</code> |
| Cancel apply clauses setting message default next-hop          | <code>undo apply ip default next-hop</code>       |

You can specify multiple next-hops or send the message to multiple interfaces. Generally, only the first parameter works. If the first parameter is mismatched, the second parameter will take effect, and so on.

By default, no apply clause is defined.

### Enabling and Disabling Local Policy Routing

Perform the following configurations in system view.

**Table 571** Enable/Disable the Local Policy Routing

| Operation                    | Command                                               |
|------------------------------|-------------------------------------------------------|
| Enable local policy routing  | <code>ip local policy route-policy policy-name</code> |
| Disable local policy routing | <code>undo ip local policy route-policy</code>        |

By default, local policy routing is disabled. Only one local policy route can be configured.

### Enabling and Disabling Interface Policy Routing

Perform the following configurations in interface view

**Table 572** Enable/Disable Interface Policy Routing

| Operation                        | Command                                         |
|----------------------------------|-------------------------------------------------|
| Enable interface policy routing  | <code>ip policy route-policy policy-name</code> |
| Disable interface policy routing | <code>undo ip policy route-policy</code>        |

By default, interface policy routing is disabled.

### Displaying and Debugging IP Policy Routing

Perform the following configurations in all views.

**Table 573** Display and Debug IP Policy Routing

| Operation                                                  | Command                                  |
|------------------------------------------------------------|------------------------------------------|
| Turn on the debugging information switch of policy routing | <code>debugging ip policy-routing</code> |

## IP Policy Routing Configuration Example

This section describes two different configurations for IP policy routing with a suggested procedure for each configuration.

### Configure Policy Routing Based on Source Address

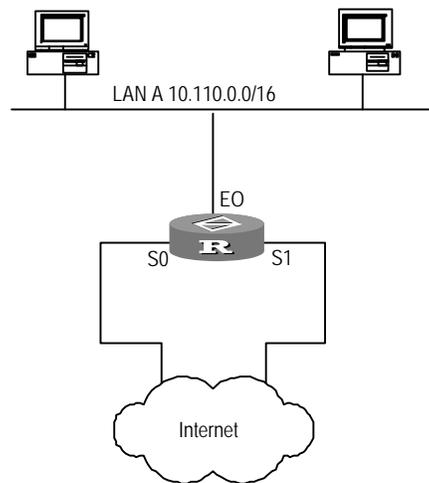
Define a policy named "aaa" that includes two nodes, through which all TCP messages are transferred from serial interface 0 and the others are transferred from serial interface 1.

- Node 10 indicates that messages matched with access list 102 will be sent to serial interface 0.
- Node 20 indicates that all the other messages will be sent to serial interface 1.

The messages from Ethernet 0 attempt to match if-match clauses of nodes 10 and 20, in turn. If nodes in permit mode are matched, the corresponding apply clauses are executed. If nodes in deny modes are matched, exit from policy routing.

LAN A is connected with the Internet through the 3Com router, requiring that TCP messages be transmitted through path 1 and other messages be transmitted through path 2.

**Figure 160** Networking diagram of configuring policy routing based on source address



- 1 Define access list:

```
[Router]acl 101
[Router-acl-101]rule deny tcp source any destination any
[Router-acl-101]acl 102
[Router-acl-102]rule permit tcp source any destination any
```

- 2 Define a node 10, indicating messages matching access list 102 will be sent to serial interface 1

```
[Router-acl-101]route-policy aaa permit 10
[Router-route-policy]if-match ip address 102
[Router-route-policy]apply interface serial 1
```

- 3 Define node 20, indicating all the other messages will be sent to serial interface 0

```
[Router-route-policy]route-policy aaa permit 20
[Router-route-policy]if-match ip address 101
[Router-route-policy]apply interface serial 0
```

## 4 Adopt policy aaa in Ethernet interface

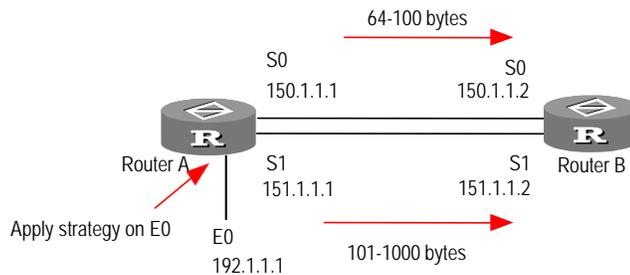
```
[Router-route-policy] interface ethernet 0
[Router-Ethernet0] ip policy route-policy aaa
```

## Configure Policy Routing Based on Message Size

Router A sends the messages of 64-100 bytes through S0, messages of 101-1000 bytes through S1 and those of other sizes must be routed normally.

Apply IP policy routing lab1 on E0 of Router A. This strategy sets message of 64-100 bytes to 150.1.1.2 as the IP address of next forwarding and set message of 101-1000 bytes to 151.1.1.2 as the IP address of next forwarding. All messages of other levels must be routed in the method based on the destination address

**Figure 161** Networking diagram of configuring policy routing based on message size



## 1 Configure Router A:

```
[RouterA] interface ethernet 0
[RouterA-Ethernet0] ip address 192.1.1.1 255.255.255.0
[RouterA-Ethernet0] ip policy route-policy lab1
[RouterA-Ethernet0] interface serial 0
[RouterA-Serial0] ip address 150.1.1.1 255.255.255.0
[RouterA-Serial0] interface serial 1
[RouterA-Serial1] ip address 151.1.1.1 255.255.255.0
[RouterA-Serial1] quit
[RouterA] rip
[RouterA-rip] network 192.1.1.0
[RouterA-rip] network 150.1.1.0
[RouterA-rip] network 151.1.1.0
[RouterA-rip] route-policy lab1 permit 10
[RouterA-route-policy] if-match length 64 100
[RouterA-route-policy] apply ip next-hop 150.1.1.2
[RouterA-route-policy] route-policy lab1 permit 20
[RouterA-route-policy] if-match length 101 1000
[RouterA-route-policy] apply ip next-hop 151.1.1.2
```

## 2 Configure Router B:

```
[RouterB] interface serial 0
[RouterB-Serial0] ip address 150.1.1.2 255.255.255.0
[RouterB-Serial0] interface serial 1
[RouterB-Serial1] ip address 151.1.1.2 255.255.255.0
[RouterB-Serial1] quit
[RouterB] rip
[RouterB-rip] network 150.1.1.0
[RouterB-rip] network 151.1.1.0
```

Monitor policy routing with debug ip policy command on Router A. Note: the messages of 64 bytes match the entry item whose serial number 10 as shown in the routing diagram lab1, therefore they are forwarded to 150.1.1.2.

```
[RouterA] debugging ip policy-routing
```

```
IP: s=151.1.1.1(local),d=152.1.1.1, len 64, policy match
```

```
IP: route map lab1, item 10, permit
```

```
IP: s=151.1.1.1(local),d=152.1.1.1, len 64, policy routed
```

```
IP: local to serial 150.1.1.2
```

On Router A, change the message size to 101 bytes and monitor policy routing with debug ip policy command. Note: the messages of 101 bytes match the entry item whose serial number 20 as shown in the routing diagram lab1. They are sent to 151.1.1.2.

```
[RouterA] debugging ip policy-routing
```

```
IP: s=151.1.1.1(local),d=152.1.1.1, len 101, policy match
```

```
IP: route map lab1, item 20, permit
```

```
IP: s=151.1.1.1(local),d=152.1.1.1, len 101, 64, policy routed
```

```
IP: local to serial 151.1.1.2
```

On Router A, change the message size to 1001 bytes and monitor policy routing with debug ip policy command. Note that this message does not match any entry item in lab1, so it is forwarded in regular mode.

```
[RouterA] debugging ip policy-routing
```

```
IP:s=151.1.1.1(local),d=152.1.1.1, len 1001, policy rejected-normal forwarding
```

```
IP:s=151.1.1.1(local),d=152.1.1.1, len 1001, policy rejected-normal forwarding
```

# VII

# MULTICAST

- Chapter 33 IP Multicast
- Chapter 34 Configuring IGMP
- Chapter 35 Configuring PIM-DM
- Chapter 36 Configuring PIM-SM



This chapter covers the following topics:

- IP Multicast Overview
- IP Multicast Addresses
- IP Multicast Features
- IP Multicast Routing Protocols
- IP Multicast Packet Forwarding
- IP Multicast Application

---

**IP Multicast Overview**

When the destination addresses carrying information (data, voice, and video) transmit with only a few subscribers in the network, multiple transmission methods such as unicast and broadcast can be employed. Unicast transmission means establishing a separate data transmission channel for each subscriber, while broadcast transmission means sending the message to all the subscribers in the network no matter whether they need it or not. If 200 subscribers in network require receiving the same message, traditionally there are two solutions for this. One is to send such message 200 times to ensure that all the subscribers are able to get it. The other one is to transmit the data within the whole network to enable subscribers to get the necessary data directly from the network by adopting the broadcast method.

Using the unicast method to transmit to 200 subscribers results in wasted bandwidth. Using the broadcast method risks information security and confidentiality. IP multicast technology solves both of these problems. The multicast source sends the information only once. The transmitted information is duplicated and distributed continuously at key network nodes. In this way, the information can be sent accurately and efficiently to each subscriber who requires it.

In simple terms, IP multicast is a bandwidth-saving technology. It sends a single information flow to several receivers simultaneously to reduce network traffic. In case a router does not support multicast in the network, the router can employ the tunnel method to encapsulate the multicast packets in the unicast packets, and send them to the adjacent multicast router. Adjacent multicast routers drop the unicast IP header, and then continue the multicast transmission to avoid causing a change to the network structure.

---

**IP Multicast Addresses**

IP multicasting uses Class D addressing. Each multicast address stands for a multicast group, not for a host. Because the maximum four-digit number of a

Class D address is 1110, the range of the multicast addresses is from 224.0.0.0 to 239.255.255.255.

The multicast group can be either permanent or temporary. The permanent group has a constant group address assigned by IANA, while the number of members in the group can be random, even zero. Temporary multicast groups can use that group address, which is not reserved, but the number of members in the temporary multicast group cannot be zero.

The range and meaning of Class D address are as follows:

**Table 574** Range and Meaning of Class D Addresses

| Class D address range        | Meaning                                                          |
|------------------------------|------------------------------------------------------------------|
| 224.0.0.0 to 224.0.0.255     | Reserved multicast address (Permanent group address)             |
| 224.0.1.0 to 238.255.255.255 | Subscriber available multicast address (Temporary group address) |
| 239.0.0.0 to 239.255.255.255 | The multicast address not managed or at specific locations       |

The reserved multicast addresses, which are frequently used, are as follows:

**Table 575** List for Reserved Multicast Addresses

| Class D address range | Meaning                        |
|-----------------------|--------------------------------|
| 224.0.0.0             | Reference addresses (reserved) |
| 224.0.0.1             | All systems on this subnet     |
| 224.0.0.2             | All routers on this subnet     |
| 224.0.0.3             | Not for distribution           |
| 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                  |
| 224.0.0.11            | Active agents                  |
| 224.0.0.12            | DHCP Server/trunk agent        |
| 224.0.0.13            | All the PIM routers            |
| 224.0.0.14            | RSVP encapsulation             |
| 224.0.0.15            | All the CBT routers            |
| 224.0.0.16            | Assigned SBM                   |
| 224.0.0.17            | All the SBMS                   |
| 224.0.0.18            | VRRP                           |
| .....                 | .....                          |

The multicast protocol changes the Class D address into the hardware/media address. For example, in an Ethernet MAC address, the range of the reserved corresponding Ethernet addresses that IANA obtains the IEEE-802 MAC is from 01-00-5e-00-00-00 to 01-00-5E-ff-ff-ff.

## IP Multicast Features

In simple TCP/IP routing, the path of a data packet transmission is from the source address to the destination address following the principle of hop-by-hop. But in

the IP multicast environment, the destination address of a data packet is not one address but a group, forming a group address. All the information receivers are added to a group, and once they access the group, data flowing to the destination address begin to transmit to the receivers of that particular group. All the group members can receive the data packet. Therefore, to get the data packet, they have to become group members first. The data packet transmitter is not required to be a group member. In the multicast environment, data will be sent to all the group members, and the subscribers who are not group members will not receive the data packets.

Generally, IP multicast has the following features:

- The membership of the host group is dynamic. There is no restriction on the location or the number of members in the host group. Independent hosts access or leave the multicast group at any time. These members can be anywhere on the Internet. One host can be a member of several multicast groups simultaneously.
- One host can send data packets to a multicast group even though it is not a group member. When sending the message to all the IP hosts in a multicast group, it is necessary to send a message to the group address only, just like unicast.
- There is no need for the router to save the membership for all the hosts. It is only necessary to know whether there is any host belonging to a certain multicast group on the network segment. The physical interface is located on the network segment. The host can only save the multicast groups it has joined.

---

## IP Multicast Routing Protocols

The multicast protocol includes two parts. One part is the Internet Group Management Protocol (IGMP) acting as the IP multicast basic signaling protocol. The other part includes the multicast routing protocols such as DVMRP, PIM-SM, PIM-DM, which implement IP multicast flow routing.

### Internet Group Management Protocol (IGMP)

IGMP is a simple protocol for the support of multicast transmission. IGMP is a simple leave/join protocol that allows end-user nodes and their multicast-enabled routers to exchange messages that describe the wishes of hosts to participate in multicast groups. It defines the multicast membership establishment and maintenance mechanism between hosts and routers, and it is the foundation of the entire IP multicast.

IGMP informs routers about the group members, and enables routers to know the information about other members within the group through the hosts directly connected to them. Application programs can learn that information coming from one data source goes to a specific group. If a LAN subscriber announces that it has joined a certain multicast group via IGMP, the multicast routers in the LAN propagate this information by the multicast routing protocol, and finally add this LAN as a branch to the multicast tree. When the host, as a member of a certain group, begins to receive information, the routers periodically carry out queries on this group, and check whether the group members are still participating. As long as there is a host still participating, routers can continue to receive data. Only after all the subscribers in the LAN exit this multicast group, are the related branches deleted from the multicast tree.

**Multicast Routing Protocol**

The group address in the multicast protocol is a virtual address. Therefore, unlike unicast, data packets cannot be routed directly from the data source to the specific destination address. The multicast application program sends the data packet to a group of receivers instead of a single receiver .

Multicast routing establishes a cyclic data transmission path from one data source end to multiple receiving ends. The task of the multicast routing protocol is to establish a distribution tree structure. The multicast routers can adopt many methods to establish a data transmission path distribution tree. Protocol Independent Multicast (PIM) is the protocol that allows multicast routers to identify other multicast routers that will receive the packets. Depending on actual network conditions, the multicast routing protocol can be divided into two kinds - dense mode and sparse mode.

**Protocol Independent Multicast--Dense Mode (PIM-DM)**

The dense mode of the multicast routing protocol is suitable for small networks with abundant bandwidth. Suppose that each subnet in the network has at least a pair of receiving sites interested in multicast. Therefore, multicast data packets are distributed to all the sites in the network. Together with this process there is consumption of the related resources (bandwidth and the CPU of the router). To decrease the consumption of these precious network resources, the dense mode of the multicast routing protocol "prunes" the branches that do not have multicast data forwarding, and retains only the branches that contain the receiving sites.

To enable the receiving sites with the multicast forwarding demand in the pruned branches to receive multicast data flow, the pruned branches can return to forwarding state periodically. To reduce the time delay for the pruned branch to recover to the forwarding state, the dense mode of the multicast routing protocol adopts a grafting mechanism to actively add to the multicast distribution tree. This cyclic diffusion and pruning phenomenon is the feature of the dense mode of the multicast routing protocol. Generally, the data packet forwarding path in the dense mode is an "active tree" with the source being its root and the group members being its leaves.

The typical routing protocol in the dense mode includes Protocol-Independent Multicast-Dense Mode (PIM-DM) and Distance Vector Multicast Routing Protocol (DVMRP).

**Protocol Independent Multicast-Sparse Mode (PIM-SM)**

Dense mode uses the flood-prune technology, which is not applicable for a WAN. In a WAN, multicast receivers are sparse and the sparse mode is used. In sparse mode, all hosts do not need to receive multicast packets unless there is an explicit request for the packets by default. A multicast router must send a *join* message to the rendezvous point (RP), which is created in the network as the virtual place for data exchange. The RP corresponds to the group that receives the multicast data traffic from the specified group. The join message passes routers and finally reaches the root, the RP. The path that the join message used becomes a branch of the shared tree. In PIM sparse mode, multicast packets are sent to the RP first and then are forwarded along the shared tree rooted at the RP and with members as the branches. To prevent the branches of the shared tree from being deleted because they are not updated, PIM sparse mode sends join messages to branches periodically to maintain the multicast distribution tree.

The transmitting end is first registered at the RP if it needs to send data to a specific address, and then sends the data to the RP. Once data reaches the RP, multicast data packets are duplicated and sent to receivers who are interested in getting them along the distribution tree path. The duplication only occurs at the crotch of the distribution tree. This process can automatically repeat until the data packets finally arrive at the destination point.

---

**IP Multicast Packet Forwarding**

In the multicast model, the source host sends information to any host group represented by the multicast group addresses in the destination address segment of the IP information packet. In contrast to the unicast model, the multicast model cannot base forwarding decisions on the destination addresses contained in the information packet. Instead, it must forward the multicast information packet to multiple external interfaces to send it to all the receiving sites. Therefore, the multicast forwarding process is more complicated than the unicast forwarding process.

To guarantee that all the multicast information reaches routers by the shortest route, the multicast model must use the unicast routing table or the independent multicast routing table and check the multicast information packet receiving interfaces. This checking mechanism is the basis for most multicast routing protocols to carry out the multicast forwarding reverse path forwarding (RPF) check. The multicast module checks the source address in the received multicast data packet. If the active tree is adopted, this source address is that of the host sending the multicast data packet. If the shared tree is adopted, this source address is the root address of the shared tree. Thus, the multicast module can determine whether the input interface of the arrived data packet is on the shortest path from the receiving site to the source address. When the multicast data arrives at the router, if the examination has passed, the information packet is forwarded according to the multicast forwarding items. Otherwise, the information is discarded.

---

**IP Multicast Application**

IP multicast allows the internal data of the company to be distributed to a large number of subscribers. For example, for a company with many chain stores, multicast can be used to send its price information to the cash register in each chain store. The real-time information can be sent to multicast subscribers by media over the Internet, such as the current remote employee management and education.

The traditional data broadcast is based on the broadcast transmission form, which requires much Internet bandwidth. Using multicast technology, TV and wireless sites can not only multicast data to Internet subscribers who really need them, but can also reduce the cost of network maintenance to a large extent.



# 34

## CONFIGURING IGMP

This chapter covers the following topics:

- IGMP Overview
- Configuring IGMP
- Displaying and Debugging IGMP
- IGMP Configuration Example

---

### IGMP Overview

The Internet Group Management Protocol (IGMP) is a protocol that is responsible for the IP multicast member management among the TCP/IP protocol family. It is the basis for IP multicast, and it is used to establish and maintain multicast membership between the IP hosts and the multicast routers directly adjacent to the hosts. IGMP does not include the propagation and maintenance of the membership relationship information between multicast routers, which is accomplished by each multicast routing protocol. IGMP operates on a physical network, such as a single Ethernet segment.

At present, IGMP Version 1 and IGMP Version 2 are extensively used. IGMP Version 2 specifies the following three kinds of messages:

- **Membership Query Message:** According to different group addresses, it can be classified into a general query message or a group-specific query message, used to learn if a particular group has any members attached on a network. For a group-specific query message, the router is used to check whether there is any subscriber in a connecting network who wants to make the query message valid, and the target group address must be zero or a valid multicast group address. IGMP Version 2 allows routers to send group-specific query messages.
- **Membership Report Message:** When the host receives a general query or a group-specific membership query message, it first identifies the combination with the interface sending the query message and sets a host group delay timer for each member group. If the remaining time of this timer is larger than the maximum response time set in the query message, it is changed to the maximum response time value. The host broadcasts the membership report to this router before the time runs out. Once the router receives the membership report, it adds the group to the membership list of the network it belongs to, and starts the group membership interval timer. If the router does not receive any membership report with the maximum query response timeout, it becomes clear that there is no local group member, and it does not transmit the received multicast message to the network it connects to.
- **Leave Group Message:** IGMP Version 2 allows a host to send a leave group message to all routers when it leaves a multicast group (the target group address is 224.0.0.2).

IGMP is asymmetric between hosts and routers. The host responds to the IGMP query message of the multicast router, and makes a response in the membership report message. The router periodically sends a general query message. Then it determines, based on the response message received, whether a specific group has a host access on its own subnet. Meanwhile, when a router exits from a group, it sends a message to the multicast router when it exits. When it receives the message, the multicast router sends a packet to inquire about the group to ensure that the member has already gone.

## Configuring IGMP

To configure the IGMP protocol, the multicast routing function is first enabled, and then each feature of the IGMP protocol can be configured.

IGMP configuration includes tasks that are covered in the following sections:

- Enabling Multicast Routing
- Configuring Router Interfaces as Group Members
- Configuring the Version Number of IGMP at the Router Interface
- Configuring the Time Interval of IGMP Host Sending Query Messages
- Configuring IGMP Maximum Query Response Time
- Configuring Subnet Querier Survival Time

### Enabling Multicast Routing

Start the IGMP protocol on all interfaces to enable routers to send multicast messages. Only after enabling multicast routing can all the other configurations related to the multicast be valid.

Make the following configuration in system view.

**Table 576** Enable/disable Multicast Routing

| Operation                 | Command                              |
|---------------------------|--------------------------------------|
| Enable multicast routing  | <b>multicast routing-enable</b>      |
| Disable multicast routing | <b>undo multicast routing-enable</b> |

By default, the system disables multicast routing.

### Configuring Router Interfaces as Group Members

Configuring router interfaces as group members can not only enable routers to access the multicast group by simulating host behaviors, but also enables the static multicast group to access the multicast group.

Make the following configuration in the interface view.

**Table 577** Configure Router Interfaces to be Group Members

| Operation                                      | Command                                   |
|------------------------------------------------|-------------------------------------------|
| Configure router interface to be group members | <b>igmp host-join groups-address</b>      |
| Delete router interface from group members     | <b>undo igmp host-join groups-address</b> |

By default, the router interface has no group member.

### Configuring the Version Number of IGMP at the Router Interface

IGMP Version 2 is able to configure query message timeout and the maximum query response time. All the systems in the same subnet must run the same IGMP version because the routers are not able to check the version number of IGMP currently running on the interface.

Make the following configuration in the interface view.

**Table 578** Configure the IGMP Version Number Run at Router Interface

| Operation                                                                             | Command                       |
|---------------------------------------------------------------------------------------|-------------------------------|
| Configure the version number of IGMP operating at router interface                    | <b>igmp version { 1   2 }</b> |
| Restore the default value of the version number of IGMP operating at router interface | <b>undo igmp version</b>      |

By default, IGMP Version 2 is operates at the router interface.

If the host does not support IGMP Version 2, then the router must be configured to use IGMP Version 1.

### Configuring the Time Interval of IGMP Host Sending Query Messages

The router periodically sends membership query messages to the network it connects to. The query interval timer sets the time interval. Subscribers can change the time interval of the IGMP host that sends query messages by configuring the query interval timer.

Make the following configuration in the interface view.

**Table 579** Configure the Time Interval of IGMP Host Sending Query Messages

| Operation                                                                          | Command                                |
|------------------------------------------------------------------------------------|----------------------------------------|
| Configure the time interval of IGMP host sending query messages                    | <b>igmp timer query <i>seconds</i></b> |
| Restore the default value of the time interval of IGMP host sending query messages | <b>undo igmp timer query</b>           |

By default, the interval for sending query messages is 125 seconds.

### Configuring IGMP Maximum Query Response Time

After the host receives the query message periodically sent by the router, it starts delay timers for each of the multicast groups it joins. A random number between zero and the maximum response time will be adopted to serve as the initial value. The maximum response time is the query message assigned maximum response time (the maximum response time of IGMP Version 1 is fixed at 10 seconds). The host broadcasts the membership report to the router before the timer times out. If the router does not receive a membership report when the maximum query response time times out, it assumes that there is no local group member, and it does not send the received multicast message to the network it connects to.

Make the following configuration in interface view.

**Table 580** Configure IGMP Maximum Query Response Time

| Operation                                  | Command                                      |
|--------------------------------------------|----------------------------------------------|
| Configure IGMP maximum query response time | <b>igmp max-response-time <i>seconds</i></b> |

|                                                               |                                          |
|---------------------------------------------------------------|------------------------------------------|
| Restore the default value of IGMP maximum query response time | <code>undo igmp max-response-time</code> |
|---------------------------------------------------------------|------------------------------------------|

The default maximum query response time is 10 seconds but ranges from 1 to 25 seconds.

This configuration can only be carried out if the current router interface is operating IGMP Version 2.

### Configuring Subnet Querier Survival Time

When there are several routers operating IGMP in a subnet, one router is chosen to serve as a querier to take charge of sending query messages to other routers in the network segment. In the network initialization, all the routers in the network segment act as querier by default, and send general query messages to all the multicast hosts in the subnet the routers connect to. Meanwhile, they compare the receiving IP address of the query message interface with the sending IP address of the query message interface. The router with the minimum IP address in the subnet will be chosen as querier, and the other routers become non-queriers.

All the non-queriers start the other querier present interval timer. Before the timer times out, if the query message from the querier is received, the timer resets. If the timer times out, all the routers reset as querier. The querier selection process restarts.

Make the following configuration in the interface view.

**Table 581** Configure Subnet Querier Survival Time

| Operation                                                     | Command                                         |
|---------------------------------------------------------------|-------------------------------------------------|
| Configure subnet Querier survival time                        | <code>igmp timer querier-present seconds</code> |
| Restore the default value of the subnet Querier survival time | <code>undo igmp timer querier-present</code>    |

By default, subnet querier timeout is 250 seconds.

This configuration can only be carried out if the current router interface is operating IGMP Version 2.

### Displaying and Debugging IGMP

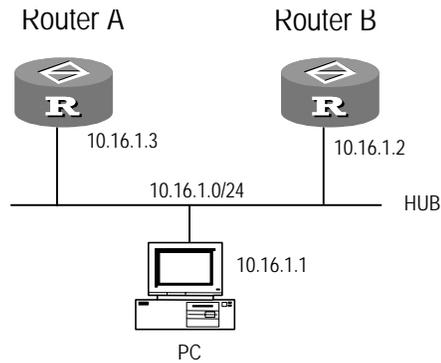
**Table 582** Display and Debug IGMP

| Operation                                                           | Command                                                                   |
|---------------------------------------------------------------------|---------------------------------------------------------------------------|
| Display the group membership status in the direct connecting subnet | <code>display igmp group [ group-address / interface type number ]</code> |
| Display IGMP interface configuration information                    | <code>display igmp interface [ type number ]</code>                       |
| Turn on the switch of IGMP debugging information                    | <code>debugging igmp { all   event   host   packet   timer }</code>       |

After the previous configuration, execute the **display** command in all views to display IGMP configuration, and to verify the effect of the configuration. Execute the **debugging** command in system view to debug IGMP.

### IGMP Configuration Example

Router A, Router B and a PC connect to one another through a Hub, and their interfaces are all fast Ethernet (FE).

**Figure 162** IGMP network diagram

- 1 Configure the IP addresses of the interfaces of Router A, Router B and the PC.

```
[RouterA] interface e0
[RouterA-Ethernet0] ip address 10.16.1.3 24
[RouterB] interface e0
[RouterB-Ethernet0] ip address 10.16.1.2 24
```

- 2 Execute the **multicast routing-enable** command on 3Com A and 3Com B to enable multicast routing.

```
[RouterA] multicast routing-enable
[RouterB] multicast routing-enable
```



This chapter covers the following topics:

- PIM-DM Overview
- PIM-DM Configuration
- Displaying and Debugging PIM-DM
- PIM-DM Configuration Example

---

### PIM-DM Overview

Protocol Independent Multicast--Dense Mode (PIM-DM) is applicable to the following conditions:

- The transmitter and the receiver are close to each other, and there are a large number of multicast group receiving members in the network.
- Multicast packet traffic is large.
- Multicast packet traffic is continuous.

PIM-DM constructs a multicast distribution tree from the source PIM router to all the other nodes employing unicast routing table. When sending a multicast packet, PIM-DM assumes that all the hosts in the network are ready for receiving the multicast packet. The multicast source begins distributing multicast packets to the downstream nodes of the network. The nodes without multicast group members will send prune message to the upstream router and inform it that there is no need for it to distribute data to the downstream nodes any more. When new members appear in the prune area, PIM-DM sends graft message to enable the pruned path to restore to distribution status. This mechanism is called broadcast-prune process.

The PIM-DM broadcast-prune mechanism continues periodically. PIM-DM adopts reverse path forwarding (RPF) technology in the broadcast-prune process. When a multicast packet arrives, the router first judges the correctness of the arriving path. If the arriving port is the one directed to the multicast source according to the unicast routing instruction, the multicast packet is considered to be from the correct path. Otherwise, the multicast packet will be considered a redundant packet and will be discarded.

PIM-DM includes the following kinds of messages:

- PIM Hello Message: PIM hello message is periodically sent neighbor interface in the same network segment to establish a relationship with the PIM-DM neighbors by the router interface operating the PIM-DM protocol. In addition, a designated router (DR) is required, in the IGMPv1, to send a host-query message. Meanwhile, the hello message takes charge of choosing a DR for the router

operating IGMPv1 (each PIM router periodically broadcasts a hello message, and the router with higher IP address is chosen to be the DR).

- **Graft Message:** The host informs the router which multicast groups it wants to join by a IGMP membership report message. At this time, the port sends a graft message to the upstream router. After the upstream router receives a graft message, it adds this port to the forwarding list of the multicast group.
- **Graft ACK Message:** After the upstream router receives the graft message, it needs to send graft acknowledgement (ACK) message to the downstream router sending the graft message.
- **Prune Message:** If the router interface forwarding list is empty, or the interface forwarding list becomes empty, the prune message will be sent to the upstream router to inform it to delete the downstream router from its interface neighbor list.
- **Assert Message:** A shared network segment can have two upstream routers simultaneously. If both of them forward multicast packets to it, the downstream routers of this network segment will probably receive two same multicast packets. In order to avoid this condition, PIM-DM adopts the assert message mechanism. If a router receives multicast packets at the forwarding port of a shared LAN, it requires all the routers operating PIM-DM (group address is 224.0.0.13) to send an assert message. The downstream routers determine the winner by comparing the specific domains of the assert message according to the relevant series of rules. The router with little message preference wins. If the preference is the same, the router with the smaller message metric value wins. If the message metric value is the same, the router with the bigger IP address wins. The winner serves as the transmitter of the network segment, while the loser sends an output interface prune message.

PIM-DM itself does not have a routing discovery mechanism, so it has to depend on a specific unicast routing protocol. Thus the protocol implementation is quite simple.

## PIM-DM Configuration

PIM-DM configuration includes tasks that are described in the following sections:

- Enabling Multicast Routing
- Starting the PIM-DM Protocol
- Configuring the Time Interval for Hello Messages

### Enabling Multicast Routing

Only after the multicast routing is enabled, can routers receive multicast packets.

Make the following configuration in the system view.

**Table 583** Enable Multicast Routing

| Operation                 | Command                              |
|---------------------------|--------------------------------------|
| Enable multicast routing  | <b>multicast routing-enable</b>      |
| Disable multicast routing | <b>undo multicast routing-enable</b> |

By default, the system disables the multicast routing.

### Starting the PIM-DM Protocol

You must start the PIM-DM protocol at each interface. By default, the system disables the PIM-DM protocol.

Make the following configuration in the interface view.

**Table 584** Start/Disable PIM-DM Protocol

| Operation               | Command                  |
|-------------------------|--------------------------|
| Start PIM-DM protocol   | <code>pim dm</code>      |
| Disable PIM-DM protocol | <code>undo pim dm</code> |

### Configuring the Time Interval for Hello Messages

After the interface starts PIM-DM protocol, it will periodically send to all the PIM routers (group address is 224.0.0.13) hello messages to find neighbors. PIM query-interval timer determines the time interval. If the interface receives the hello message, it means that there are adjacent PIM routers for this interface, and this interface adds the neighbor to its interface neighbor list. If the interface does not receive any hello message from the neighbors in the interface neighbor list within a specific period, it is assumed that the neighbor has left the multicast network. The time interval of sending hello message can be configured according to the bandwidth and the type of the network to which the interface connects.

Make the following configuration in the interface view.

**Table 585** Configure the Time Interval of Interface Sending Hello Messages

| Operation                                                                          | Command                              |
|------------------------------------------------------------------------------------|--------------------------------------|
| Set the time interval of interface sending hello messages                          | <code>pim timer hello seconds</code> |
| Restore the default value of the time interval of interface sending hello messages | <code>undo pim timer hello</code>    |

By default, the time interval of interface sending hello messages is 30 seconds.

### Displaying and Debugging PIM-DM

**Table 586** Display and Debug PIM-DM

| Operation                                                              | Command                                                                                                                    |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Display multicast forwarding list information                          | <code>display multicast forwarding-table [ group-address   source-address ]</code>                                         |
| Display multicast core routing table                                   | <code>display multicast routing-table [ group-address   source-address ]</code>                                            |
| Display IP multicast forwarding table information                      | <code>display multicast forwarding-table</code>                                                                            |
| Display PIM protocol interface information                             | <code>display pim interface [ type number ]</code>                                                                         |
| Display PIM protocol multicast routing table information               | <code>display pim routing-table [ *g [ group-address ]   **rp [ rp-address ]   { group-address   source-address } ]</code> |
| Display PIM adjacent routers information                               | <code>display pim neighbor [ interface type number ]</code>                                                                |
| Turn on the switch of multicast forwarding table debugging information | <code>debugging multicast forwarding</code>                                                                                |
| Turn on the switch of PIM general debugging information                | <code>debugging pim common { all   event   packet   timer }</code>                                                         |

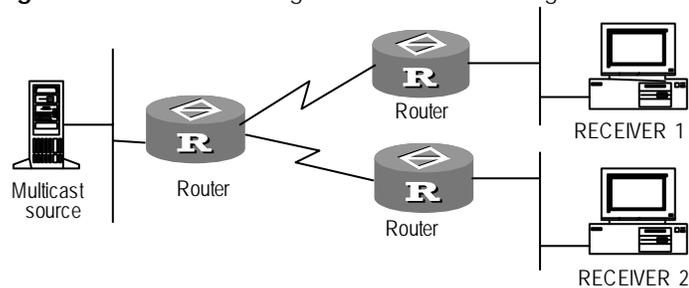
|                                                    |                                                                                                                                           |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Turn on the switch of PIM-DM debugging information | <pre>debugging pim dm { alert   all   mrt   timer   warning   { recv   send } { all   assert   graft   graft-ack   join   prune } }</pre> |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|

After making the previous configuration, execute the **display** command in all views to display the running of the PIM-DM configuration, and to verify the effect of the configuration. Execute the **debugging** command in system view to debug PIM-DM.

## PIM-DM Configuration Example

In this example, the multicast source server is the multicast source, while RECEIVER 1 and RECEIVER 2 are the two receivers of this multicast group.

**Figure 163** PIM-DM configuration and networking



### 1 Enable multicast routing protocol

```
[Router] multicast routing-enable
```

### 2 Enable PIM-DM protocol

```
[Router] interface Ethernet 0
[Router-Ethernet0] pim dm
[Router-Ethernet0] interface serial 0
[Router-Serial0] pim dm
[Router-Serial0] interface serial 1
[Router-Serial1] pim dm
```

# 36

## CONFIGURING PIM-SM

This chapter covers the following topics:

- PIM-SM Overview
- PIM-SM Configuration
- Displaying and Debugging PIM-SM
- PIM-SM Configuration Example
- Troubleshooting PIM-SM

---

### PIM-SM Overview

Protocol Independent Multicast--Sparse Mode (PIM-SM) is used in the following conditions:

- The distribution of the group members is relatively separate and the range is comparatively wide.
- The network bandwidth resource is limited.

PIM-SM is independent of any specific unicast routing protocol. PIM -SM is called protocol independent because it can use the route information entered by any routing protocol, such as unicast protocols like OSPF, RIP, or multicasting protocols like DVRMP in the multicasting routing information base (RIB). It supposes that all the routers will not send multicast packets to the multicast group unless there is an explicit transmission request. PIM-SM informs all the PIM-SM routers of multicast information by configuring a rendezvous point (RP) and a bootstrap router (BSR). And it reduces data messages and controls the network bandwidth occupied by the messages occupy by allowing routers to explicitly join and leave multicast groups. PIM-SM constructs an RP path tree (RPT) with the RP its root so as to make the multicast packets transmitted along with the RPT.

When a host joins a multicast group, the directly connected router sends a joining message to the RP PIM. The first hop router of the transmitter registers the transmitter at RP. The receiver's DR adds the receiver to the RPT. Using the RPT with the RP its root not only reduces the protocol state that routers need maintenance, which improves the scalability of the protocol and reduces the router's processing cost, but also supports a large number of simultaneous multicast groups. When the data traffic flow reaches a certain degree, the data will switch from the RPT to the shortest path tree based on source so as to reduce the network delay.

PIM-SM mainly includes the following kinds of messages:

- PIM Hello Message: A PIM hello message is periodically sent to the other neighbor interface by a router interface that operates PIM-DM protocol in the same network segment. It establishes neighborhood with the PIM-DM

neighbors. The hello message also takes charge of choosing a DR for the router operating IGMPv1.

- Register Message: When the DR receives the multicast message sent by the host in the local network, it encapsulates it in the register message and unicasts it to the RP to distribute the message along the RP tree. The source address in the IP header of the register message is DR address, and the destination address is RP address.
- Register-Stop Message: It is unicast to the transmitter of the register message by RP to inform the transmitter to stop sending register messages.
- Join/Prune Message: This message is sent in the direction of the source or RP. The join message establishes the RPT or SPT. When the receiver leaves the group, the prune message is used to prune the RPT or SPT. The join message and the prune message are placed in one message, but either of such two kinds of messages can be empty.
- Bootstrap Message: The router sends this message from all the interfaces except on that interface receiving this kind of message. This kind of message is generated in BSR, and is forwarded by all the routers. It is used to inform all the routers of the RP-Set information collected by BSR.
- Assert Message: When there are multiple routers in the multiple access network, and the output interface for the routing item of a router receives multicast message, this kind of message is used to specify the transmitter.
- Candidate-RP-Advertisement Message: This message is unicast to BSR by the candidate RP to report the service group address set of this candidate RP.

## PIM-SM Configuration

PIM-SM configuration includes tasks that are described in the following sections:

- Enabling Multicast Routing
- Starting the PIM-SM Protocol
- Configuring the Candidate BSR
- Configuring the Candidate RP
- Configuring the PIM-SM Domain Boundary
- Configuring the Time Interval for Sending a Hello Message
- Configuring the Threshold of the Shortest Path

### Enabling Multicast Routing

Make the following configuration in the system view.

**Table 587** Enable/Disable Multicast Routing

| Operation                 | Command                              |
|---------------------------|--------------------------------------|
| Enable multicast routing  | <b>multicast routing-enable</b>      |
| Disable multicast routing | <b>undo multicast routing-enable</b> |

By default, the system disables multicast routing.

### Starting the PIM-SM Protocol

The PIM-SM protocol is configured at each interface in turn. In normal conditions, the PIM-SM protocol should be started at all interfaces.

Make the following configuration in the interface view.

**Table 588** Enable/Disable PIM-SM Protocol

| Operation               | Command            |
|-------------------------|--------------------|
| Enable PIM-SM protocol  | <b>pim sm</b>      |
| Disable PIM-SM protocol | <b>undo pim sm</b> |

By default, the interface disables PIM-SM protocol.

Note that PIM-SM only runs on specific interfaces. One interface can only run one multicast routing protocol at one time.

### Configuring the Candidate BSR

In a PIM-SM domain, there must be a unique bootstrap router to enable PIM-SM router to function normally. BSR takes charge of collecting and sending RP information. Several candidate bootstrap routers (C-BSR) generate one publicly acknowledged BSR by bootstrap message selection. Before the BSR information is known, C-BSRs view themselves as BSRs. They periodically broadcast bootstrap messages in PIM-SM domain (the broadcast address is 224.0.0.13). Such a message contains BSR address and priority.

BSR manages RP, and it collects and distributes the RP information in the whole network. RP is generated from the BSR election.

Make the following configuration in the system view.

**Table 589** Configure Candidate BSR

| Operation                                     | Command                                                                    |
|-----------------------------------------------|----------------------------------------------------------------------------|
| Configure an interface to be candidate BSR    | <b>c-bsr interface-type interface-number hash-mask-length [ priority ]</b> |
| Disable an interface from being candidate BSR | <b>undo c-bsr</b>                                                          |

By default, no interface is configured to be a candidate BSR.



Use the **pim** command in system view to enter PIM view.

### Configuring the Candidate RP

In the PIM-SM protocol, the shared tree (RP Path Tree) constructed by the routing multicast data regards the rendezvous point (RP) as its root, and the group members as its leaves. RP is generated from BSR selection. After the BSR is selected, all the C-RPs periodically unicast to BSR C-RP advertisements. BSR then selects the RP, and propagates it to the whole network. There may be several RPs, and each has different group service range. In this way, all the routers can get RP information.

In configuring candidate RP, we can specify the RP group service range. It can serve all the multicast groups, or just part of the groups.

Make the following configuration in the system view.

**Table 590** Configure Candidate RP

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                                              |                                                                                                        |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Configure an interface to be candidate RP    | <b>c-rp interface-type interface-number</b><br>[ <b>accept-policy acl-number</b> [ <b>priority</b> ] ] |
| Disable an interface from being candidate RP | <b>undo c-rp interface-type interface-number</b>                                                       |

By default, no interface is configured to be candidate RP.



Use **pim** command in system view to enter PIM view.

Generally, only one C-BSR and one C-RP are configured in the network, and usually it is the same router. Only one C-BSR can be configured for a single router. The latter configured C-BSR replaces the formerly configured C-BSR. Subscribers are recommended to configure the C-RP and C-BSR at the loopback interface of the same router. This reduces the network oscillation caused by physical interface alternating UP/DOWN, because the router loopback interface is always UP.

### Configuring the PIM-SM Domain Boundary

When the scale of a network is large, the network needs to be divided into several multicast domains. A different multicast domain can be in charge of a different RP. After the PIM domain boundary has been configured, the BSR message and RP message do not break through this boundary, but the other PIM messages are able to pass through the domain boundary.

Make the following configuration in the interface view.

**Table 591** Configure PIM-SM Domain Boundary

| Operation                  | Command                      |
|----------------------------|------------------------------|
| Set PIM domain boundary    | <b>pim bsr-boundary</b>      |
| Delete PIM domain boundary | <b>undo pim bsr-boundary</b> |

By default, no PIM-SM domain boundary is configured.

### Configuring the Time Interval for Sending a Hello Message

After the interface starts PIM-SM protocol, it will periodically transmits a hello message to all the PIM routers (group address is 224.0.0.13) to find PIM neighbors. the query interval timer determines this time interval. If the interface receives the Hello message, it means that there are adjacent PIM routers for this interface, and this interface can add the neighbor to its interface neighbor list. If the interface does not receive a hello message from the neighbors in the interface neighbor list within a specific period, it is assumed that the neighbor must have left the multicast network. The time interval for sending a hello message can be configured according to the bandwidth and the type of the network the interface connects to.

Make the following configuration in the interface view.

**Table 592** Configure the Time Interval of Interface Sending Hello Message

| Operation                                                                         | Command                        |
|-----------------------------------------------------------------------------------|--------------------------------|
| Configure the time interval of interface sending Hello message                    | <b>pim timer hello seconds</b> |
| Restore the default value of the time interval of interface sending Hello message | <b>undo pim timer hello</b>    |

By default, the time interval of interface sending Hello message is 30 seconds.

**Configuring the Threshold of the Shortest Path**

The PIM-SM router first forwards multicast data packets by the shared tree. But if the multicast data rate exceeds a certain threshold value, the router for the last hop of multicast packets starts the switch from the shared tree to the shortest path tree.

Make the following configuration in the system view.

**Table 593** Configure the Threshold of the Shortest Path Switching From the Shared Tree to Source

| Operation                                                                                         | Command                                                                                    |
|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Configure the threshold value of the shortest path switching from the shared tree to source       | <code>spt-switch-threshold { traffic-rate   infinity } [ accept-policy acl-number ]</code> |
| Restore the default threshold value of the shortest path switching from the shared tree to source | <code>undo spt-switch-threshold [ accept-policy acl-number ]</code>                        |

By default, the threshold value of the shortest path switches from the shared tree to source is zero. That is to say, after the router receives the first multicast data packet in the last hop, it switches immediately to the shortest path tree.

Use the `pim` command in system view to enter PIM view.

**Displaying and Debugging PIM-SM**

**Table 594** Display and Debug PIM-SM

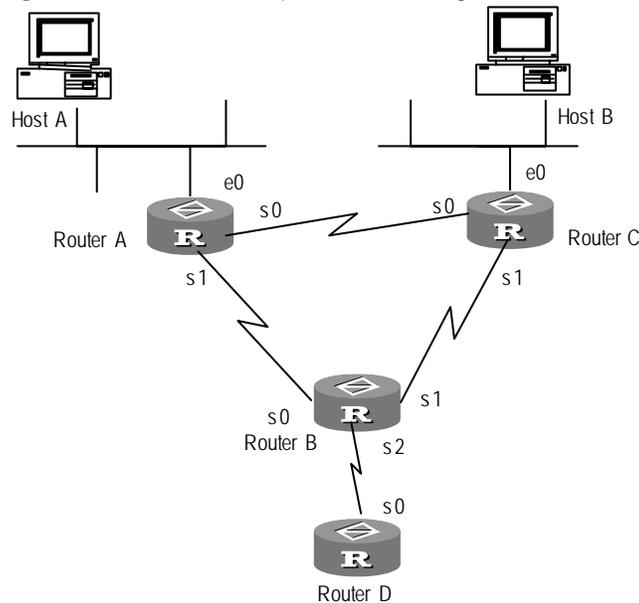
| Operation                                                              | Command                                                                                                                                    |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Display multicast forwarding list information                          | <code>display multicast forwarding-table [ group-address ] [ source-address ]</code>                                                       |
| Display multicast core routing table                                   | <code>display multicast routing-table [ group-address ] [ source-address ]</code>                                                          |
| Display BSR information                                                | <code>display pim bsr-info</code>                                                                                                          |
| Display PIM protocol interface information                             | <code>display pim interface [ type number ]</code>                                                                                         |
| Display PIM protocol multicast routing table information               | <code>display pim routing-table [ *g [ group-address ]   **rp [ rp-address ]   { group-address   source-address } ]</code>                 |
| Display PIM adjacent routers information                               | <code>display pim neighbor [ interface type number ]</code>                                                                                |
| Display corresponding RP information of the multicast group            | <code>display pim rp-info [ group-address ]</code>                                                                                         |
| Turn on the switch of multicast forwarding table debugging information | <code>debugging multicast forwarding</code>                                                                                                |
| Turn on the switch of PIM debugging information                        | <code>debugging pim common { all   event   packet   timer }</code>                                                                         |
| Turn on the switch of PIM-SM debugging information                     | <code>debugging pim sm { all   mbr   mrt   timer   warning   { recv   send } { assert   bootstarp   crpadv   jp   reg   regstop } }</code> |

After the above configuration, execute the **display** command in all views to display PIM-SM configuration, and to verify the effect of the configuration. Executethe **debugging** command in system view for the debugging of PIM-SM.

## PIM-SM Configuration Example

In the actual network, because different manufacturers provide routing equipment, the routing protocols are different. Because the PIM protocol is independent of any specific unicast protocol, there is no need to pay attention to the unicast protocol. The the purpose of this example, the routers are mutually accessible.

**Figure 164** PIM-SM comprehensive configuration networking diagram



### 1 Configure Router A

#### a Enable PIM-SM protocol

```
[RouterA] multicast routing-enable
[RouterA] interface ethernet 0
[RouterA-Ethernet0] pim sm
[RouterA-Ethernet0] interface serial 0
[RouterA-Serial0] pim sm
[RouterA-Serial0] interface serial 1
[RouterA-Serial1] pim sm
```

#### b Configure the threshold value of the multicast group switching from the shared tree to the shortest path tree to be 10kbps.

```
[RouterA] acl 5
[RouterA-acl-5] rule permit source 225.0.0.0 255.0.0.0
[RouterA-acl-5] pim
[RouterA-pim] spt-switch-threshold 10 accept-policy 5
```

### 2 Configure Router B

#### a Enable PIM-SM protocol

```
[RouterB] multicast routing-enable
[RouterB] interface serial 0
[RouterB-Serial0] pim sm
[RouterB] interface serial 1
```

```
[RouterB-Serial1] pim sm
[RouterB] interface serial 2
[RouterB-Serial2] pim sm
```

**b** Configure the candidate BSR

```
[RouterB-pim] c-bsr serial 0 30 2
```

**c** Configure the candidate RP

```
[RouterB-pim] acl 5
[RouterB-acl-5] rule permit source 225.0.0.0 255.0.0.0
[RouterB-acl-5] pim
[RouterB-pim] c-rp serial 0 accept-policy 5
```

**d** Configure PIM domain boundary

```
[RouterB-Serial2] pim bsr-boundary
```

When the Serial 2 has been configured to be BSR, Router D will not be able to receive the BSR information sent by Router B, which will be excluded from this PIM domain.

**3** Configure the Router C

**a** Enable PIM-SM protocol

```
[RouterC] multicast routing-enable
[RouterC] interface ethernet 0
[RouterC-Ethernet0] pim sm
[RouterC] interface serial 0
[RouterC-Serial0] pim sm
[RouterC] interface serial 1
[RouterC-Serial1] pim sm
```

Suppose Host A is the receiver of 225.0.0.1. Host B now begins sending data with the destination address 225.0.0.1. Router A receives the multicast data sent by Host B via Router B. When the multicast data rate of Host B exceeds 10kbps, Router A will be added to the shortest path tree, and the multicast data message sent by Host B will be received directly from Router C.

---

## Troubleshooting PIM-SM

### The router cannot correctly establish the multicast routing table.

Follow these steps:

- Use the PIM-SM protocol to configure RP and BSR. First, use the **display pim bsr-info** command to check whether there is BSR information. If there is no such information, check whether there is unicast routing to the BSR. Then, use the **display pim rp-info** command to check whether the RP information is correct. If there is no RP information, check the unicast routing again.
- The **display pim neighbor** command can be used to check whether the neighbors have discovered each other.



# VIII

# SECURITY

- Chapter 37    Configuring Terminal Access Security
- Chapter 38    Configuring AAA and RADIUS Protocol
- Chapter 39    Configuring Firewall
- Chapter 40    Configuring IPSec
- Chapter 41    Configuring IKE



# 37

## CONFIGURING TERMINAL ACCESS SECURITY

This chapter provides an overview to the security features provided for terminal access of 3Com routers and covers the following topics:

- Terminal Access Security Overview
- Configuring Terminal Access Security
- EXEC Configuration Example

---

### Terminal Access Security Overview

3Com routers adopt cascade protection for the command line interface, and divide terminal access users into three types:

- Administrators
- Operators
- Guests

A guest user can only log onto the router to execute the interconnectivity test commands, such as ping, tracet, pad. An operator user can only view the running and debugging information of the router. An administrator user can not only view all the router information, but can also configure and maintain the router. All users need to authenticate the usernames and passwords when visiting the router.

The command line interface (CLI) provides the following features for terminal users:

- For security, password input is not displayed on the terminal screen.
- If an illegal user attempts to break into the system by testing different passwords, access is automatically denied if the wrong password is entered consecutively three times.

Users can set the terminal timeout time. If a terminal user makes no keyboard input within a certain time, the access is disconnected automatically, so as to avoid illegal access to the router.

---

### Configuring Terminal Access Security

Terminal access security includes tasks described in the following sections:

- Configuring a User
- Configuring User Login Authentication

#### Configuring a User

Perform the following configurations in system view.

**Table 595** Configure a User

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                  |                                                                                  |
|------------------|----------------------------------------------------------------------------------|
| Configure a user | <code>local-user user-name service-type type [ password cipher password ]</code> |
| Delete a user    | <code>undo local-user user-name</code>                                           |

By default, no user is configured.

### Configuring User Login Authentication

All users who access a router through a terminal are called terminal users. 3Com routers divide terminal users into five types:

- Asynchronous port terminal user
- X.25 PAD calling user
- Console port user
- Dumb terminal user
- Telnet terminal user

3Com routers now support command line interpreters that access terminals from four types of interfaces:

- Remote X.25 PAD
- Asynchronous dialing port (working in interactive mode)
- Local console port
- Dumb terminal access mode
- Local/remote Telnet terminal

Perform the following configurations in system view.

**Table 596** Configure EXECLogin Authentication

| Operation                                                              | Command                        |
|------------------------------------------------------------------------|--------------------------------|
| Configure login authentication of terminal user from asynchronous port | <code>login async</code>       |
| Cancel login authentication of terminal user from asynchronous port    | <code>undo login async</code>  |
| Configure login authentication of terminal user from Console port      | <code>login con</code>         |
| Cancel login authentication of terminal user from Console port         | <code>undo login con</code>    |
| Configure login authentication to dumb terminal access user            | <code>login hwtty</code>       |
| Cancel terminal user login authentication to dumb terminal access user | <code>undo login hwtty</code>  |
| Configure login authentication to remote X.25 PAD calling user         | <code>login pad</code>         |
| Cancel login authentication to remote X.25 PAD calling user            | <code>undo login pad</code>    |
| Configure login authentication of terminal user via telnet             | <code>login telnet</code>      |
| Cancel login authentication of terminal user via telnet                | <code>undo login telnet</code> |

### EXEC Configuration Example

The following examples demonstrate how to configure login authentication for:

- An administrator user using the console port
- An operator user using telnet

### Configuring Administrator User Login Authentication from a Console Port

In this example, the user name is abc and the password is hello. The RADIUS server first authenticates the user, and then local authentication is used when the former authentication cannot be carried out normally. When logging in the router connected through the console port, only the user whose user name is abc and password is hello can log on successfully. Otherwise, access to the router is denied.

#### 1 Enable AAA

```
[Router] aaa-enable
```

#### 2 Configure the login authentication of entering EXEC from Console port

```
[Router] login con
```

#### 3 Configure the local authentication user name and password of EXEC user type.

```
[Router] local-user abc service-type exec-administrator password
cipher hello
```

#### 4 Configure the default authentication method list of EXEC users

```
[Router] aaa authentication-scheme login default radius local
```

#### 5 Configure RADIUS server and the shared secret

```
[Router] radius server 172.17.0.30 authentication-port 1645
accounting-port 1646
[Router] radius shared-key 3Com
```

### Configuring Operator User Login Authentication Through Telnet

In this example, the user name is abcd and the password is hello. Local authentication is conducted directly and only users who pass the local authentication can log on successfully. Otherwise, access to the router is denied.

#### 1 Enable AAA

```
[Router] aaa-enable
```

#### 2 Configure the login authentication of entering EXEC via Telnet port

```
[Router] login telnet
```

#### 3 Configure the local authentication user name and password of EXEC user type.

```
[Router] local-user abcd service-type exec-operator password cipher
hello
```

#### 4 Configure the authentication method list of EXEC users

```
[Router] aaa authentication-scheme login default local
```



# CONFIGURING AAA AND RADIUS PROTOCOL

This chapter covers the following topics:

- AAA Overview
- RADIUS Overview
- Configuring AAA and RADIUS
- Displaying and Debugging AAA and RADIUS
- AAA and RADIUS Configuration Examples
- Troubleshooting AAA and RADIUS

---

## AAA Overview

AAA implements the following network security services:

- Authenticating user access rights
- Authorizing users for certain types of services
- Accounting for the network resources used by users

Network security refers mainly to access control which determines:

- Users who can access the network server
- Services that the users with access authority can obtain
- Accounting of users using network resources

---

## RADIUS Overview

Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that provides AAA functions and protects networks from being intruded by unauthorized visitors, so it is mainly applied in network environments that require high security and support remote login.

RADIUS consists of three components:

- Protocol: Based on UDP/IP layer, RFC2865 and 2866 define the RADIUS frame relay format and message transmission mechanism, and define 1812 as the authentication port and 1813 as the accounting port.
- Server: A RADIUS server runs on a central computer or workstation, and contains the information for user authentication and network service visits.
- Client: A client is located at the Network Access Server (NAS) side. It can be placed anywhere in the network.

As the RADIUS client, a NAS (such as a 3Com router) is responsible for transmitting user information to a specified RADIUS server and for processing according to the information returned from the server. The RADIUS server is

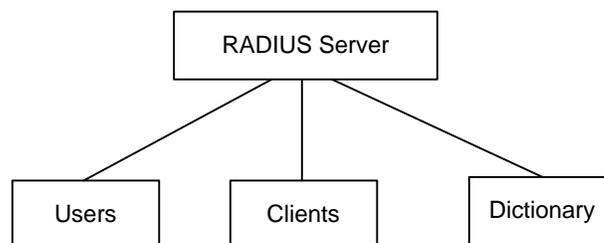
responsible for receiving a user's request for connection, authenticating the user, and returning the required information to NAS.

The RADIUS server maintains three databases:

- Users: stores user information, such as username, password, applied protocols, IP address
- Clients: stores information about the RADIUS client, such as the shared key
- Dictionary: explains the meaning of RADIUS protocol attributes

The following figure shows the three components of a RADIUS server.

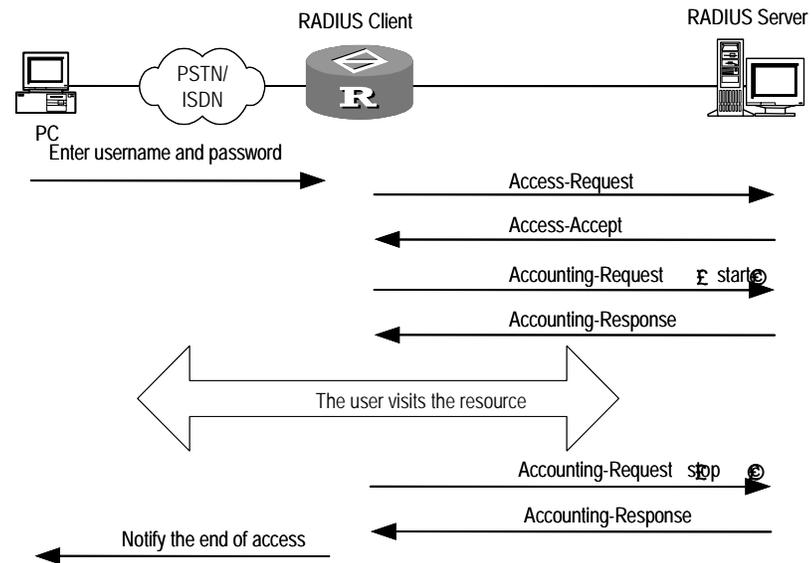
**Figure 165** Components of RADIUS server



In addition, a RADIUS server can act as the client of other AAA servers to perform authentication or accounting. A RADIUS server supports multiple ways to authenticate the user, such as PPP-based PAP, CHAP and UNIX-based login.

### Basic Information Interaction Procedure of RADIUS

The RADIUS server usually uses the agent authentication function of the devices like NAS to authenticate the user. The RADIUS client and server authenticate their interactive messages through shared keys, and the user password is transmitted over the network in ciphertext mode to enhance security. The RADIUS protocol integrates the authentication and authority processes and the response packet carries authority information. The operation process is shown in the following figure.

**Figure 166** Basic message interaction process of RADIUS

The basic operation is described as follows:

- 1 The user enters a username and password.
- 2 Having received the username and password, the RADIUS client sends an authentication request packet (Access-Request) to the RADIUS server.
- 3 The RADIUS server authenticates the user information in the user database. If the authentication succeeds, it sends the user's right information in an authentication response packet (Access-Accept) to the RADIUS client. If the authentication fails, it returns the Access-Request packet.
- 4 According to the authentication result, the RADIUS client accepts or denies the user. If it accepts, the RADIUS client sends an accounting start request packet (Accounting-Request) to the RADIUS server. The value of Status-Type is *start*.
- 5 The RADIUS server returns an accounting start response packet (Accounting-Response).
- 6 The RADIUS client sends an accounting stop request packet (Accounting-Request) to the RADIUS server. The value of Status-Type is *stop*.
- 7 The RADIUS server returns an accounting stop response packet (Accounting-Response).

### Packet Structure of the RADIUS protocol

RADIUS uses UDP to transmit messages. By employing a timer management mechanism, retransmission mechanism, and slave server mechanism, it can ensure that the interactive message between the RADIUS server and client can be processed correctly. Figure 167 illustrates the contents of a RADIUS packet.

**Figure 167** RADIUS packet structure

| Code          | Identifier | Length |
|---------------|------------|--------|
| Authenticator |            |        |
| Attribute     |            |        |

The Identifier field is used to match request packets and response requests. It varies with the Attribute field and the valid received response packets, but remains unchanged during retransmission. The Authenticator field (16 bytes) is used to authenticate the request transmitted by the RADIUS server, and it can also be used on the password hidden algorithm. There are two kinds of Authenticator packets:

- Request Authenticator: Adopts 16-byte random code.
- Response Authenticator: Is the result of performing the MD5 algorithm on Code, Identifier, Request Authenticator, Length, Attribute and shared-key.

The Code field decides the type of RADIUS packets, as shown in Table 597.

**Table 597** The Type of Packets Decided by Code Field

| Code | Packet type         | Explanation of the packet                                                                                                                                                                                                                                                                                    |
|------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Access-Request      | Direction: Client -> Server.<br>The Client transmits the user information to Server to decide whether or not to allow the user to access.<br>The packet must contain User-Name attribute, and may contain such attributes as NAS-IP-Address, User-Password or NAS-Port.                                      |
| 2    | Access-Accept       | Direction: Server->Client.<br>If all the Attribute values in the Access-Request packets are acceptable (i.e., the authentication is successful), this type of packet can be transmitted.                                                                                                                     |
| 3    | Access-Reject       | Direction: Server->Client.<br>If none of the Attribute values in the Access-Request packet is acceptable (i.e., the authentication has failed), this type of packet can be transmitted.                                                                                                                      |
| 4    | Accounting-Request  | Direction: Client->Server.<br>Client transmits the user information to Server and request accounting. The Acct-Status-Type attribute in this packet differentiates accounting start request and accounting stop request. The attributes in this packet is almost the same as those in Access-Request packet. |
| 5    | Accounting-Response | Direction: Server->Client.<br>Server informs Client that the Accounting-Request packet is received and the accounting information is correctly recorded. The packet includes inbound/outbound bytes, inbound/outbound packets and session time on the interface.                                             |

The Attribute field carries special AAA information, and provides the configuration details of request and response packets in the triplet form of type, length, and value. Table 598 lists the explanation of Attribute fields defined by RFC.

**Table 598** Attribute Fields

| 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           |
| 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            |

Attribute field 26 (Vendor-Specific) in the RADIUS protocol can be easily extended, so that the user can define extension attributes. Figure 168 shows the packet structure:

**Figure 168** Fragment of the RADIUS packet that includes extension attribute

| Type                                     | Length | Vendor-ID           |                       |
|------------------------------------------|--------|---------------------|-----------------------|
| Vendor-ID                                |        | type<br>(specified) | length<br>(specified) |
| specified attribute value <sub>i-j</sub> |        |                     |                       |
|                                          |        |                     |                       |

## Configuring AAA and RADIUS

Configuring AAA and RADIUS includes tasks that are described in the following sections:

- Enabling and Disabling AAA
- Configuring the Authentication Method List for Login Users
- Configuring an Authentication Method List for PPP Users
- Configuring the Local-First Authentication of AAA
- Configuring the AAA Accounting Option
- Configuring a Local IP Address Pool

- Assigning an IP Address for a PPP User
- Configuring a Local User Database
- Configure RADIUS Server

### Enabling and Disabling AAA

Please perform the following configurations in the system view.

**Table 599** Enable/Disable AAA

| Operation   | Command         |
|-------------|-----------------|
| Enable AAA  | aaa-enable      |
| Disable AAA | undo aaa-enable |

By default, AAA is disabled.

### Configuring the Authentication Method List for Login Users

An authentication method list defines the authentication methods, including the authentication types, which can be executed, and their execution sequence. This list is used in sequence to authenticate users.

Login users are divided into FTP users and EXEC users. EXEC means logging on the router through Telnet or other methods, such as the console port, asynchronous serial port, telnet, X.25 PAD calling, for router configuration. The two types of users have to be authorized in a local user database with the command **local-user service-type**. If a RADIUS server is used for authentication, the authorization details for the corresponding user (defining user name and password) should be set on the RADIUS server, before it is started.

Perform the following configuration in system view.

**Table 600** Configure AAA Login Authentication

| Operation                                         | Command                                                                                                                                                    |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure login authentication method list of AAA | <b>aaa authentication-scheme login { default   <i>methods-list</i> } [ template <i>server-template-name</i> ] [ <i>method1</i> ] [ <i>method2</i> ]...</b> |
| Delete login authentication method list of AAA    | <b>undo aaa authentication-scheme login { default   <i>methods-list</i> }</b>                                                                              |

By default, the login method list is **aaa authentication-scheme login default local**.

If the user does not define the **methods-list**, the execution sequence of default method list will be used.

*Method* here refers to the authentication method. The Authentication method includes the following:

- **radius** --- authentication with the RADIUS server
- **local** --- local authentication
- **none** --- access authority to all users without authentication

While configuring the authentication method list, at least one authentication method should be designated. If multiple authentication methods are designated, then at the time of login authentication, if there is no response to the preceding

methods the subsequent methods can be used. If authentication again, the authentication is terminated. The **none** method is meaningful only when it is the last item of the method list. Note that only one login method list can be configured, which can use a different name from the previously configured list. The latest configured authentication method list replaces the former one. All the login services using AAA use this method list.

Five legal combinations of the methods are as follows:

- `aaa authentication-scheme login default none`
- `aaa authentication-scheme login default local`
- `aaa authentication-scheme login default radius`
- `aaa authentication-scheme login default radius none`
- `aaa authentication-scheme login default radius local`

### Configuring an Authentication Method List for PPP Users

Perform the following configuration in system view.

**Table 601** Configure PPP Authentication Method List of AAA

| Operation                                       | Command                                                                                           |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Configure PPP authentication method list of AAA | <code>aaa authentication-scheme ppp { default   methods-list } { method1 [ method2 ... ] }</code> |
| Cancel PPP authentication method list of AAA    | <code>undo aaa authentication-scheme ppp { default   methods-list }</code>                        |

By default, the method list combination for the PPP login users is `aaa authentication-scheme ppp default local`.

If users do not define the method *methods-list*, the executing sequence defined in the default method list (defined by **default**) is used.

*Method* here refers to the authentication method. The authentication method includes the following:

- **radius** --- authentication using the RADIUS server
- **local** --- local authentication
- **none** -- access authority to all users without authentication

While configuring the authentication method list, at least one authentication method should be designated. If multiple authentication methods are designated, then in PPP authentication, only when there is no response to the preceding methods, can the subsequent methods be used. If authentication fails after the preceding methods are used, then the authentication is terminated. The **none** method is meaningful only when it is the last item of the method list.

There are five legal combinations of the methods:

- `aaa authentication-scheme ppp default none`
- `aaa authentication-scheme ppp default local`
- `aaa authentication-scheme ppp default radius`
- `aaa authentication-scheme ppp default radius none`

- `aaa authentication-scheme ppp default radius local`

Different PPP authentication method lists can be configured for different interfaces.

### Configuring the Local-First Authentication of AAA

When local-first authentication is configured, the user is authenticated locally first. If local authentication fails, then the authentication method configured in the method list is used instead. Once local-first authentication is configured, it is applied to all users using PPP and login.

Perform the following configurations in system view.

**Table 602** Configure AAA Local-First Authentication

| Operation                          | Command                                                 |
|------------------------------------|---------------------------------------------------------|
| Enable local-first authentication  | <code>aaa authentication-scheme local-first</code>      |
| Disable local-first authentication | <code>undo aaa authentication-scheme local-first</code> |

By default local-first authentication is disabled.

### Configuring the AAA Accounting Option

In case there is no available RADIUS accounting server or if communication with the RADIUS accounting server fails, and if only `aaa accounting-scheme optional` command is configured then the user is be disconnected and can still use the network resources.

Perform the following configurations in system view.

**Table 603** Configure AAA Accounting Option

| Operation                         | Command                                                 |
|-----------------------------------|---------------------------------------------------------|
| Turn on accounting option switch  | <code>aaa accounting-scheme-scheme optional</code>      |
| Turn off accounting option switch | <code>undo aaa accounting-scheme-scheme optional</code> |

By default, the accounting option is disabled and users are charged. When the method list designated by the user is `none`, accounting is unnecessary.

### Configuring a Local IP Address Pool

A local address pool is mainly used to assign an IP address for users who log in remote PPP. If the end IP address of the pool is not specified when the IP address pool is defined, there will be only one IP address in the address pool.

Perform the following configurations in system view.

**Table 604** Configure Local IP Address Pool

| Operation                       | Command                                                             |
|---------------------------------|---------------------------------------------------------------------|
| Configure local IP address pool | <code>ip pool pool-number low-ip-address [ high-ip-address ]</code> |
| Cancel local IP address pool    | <code>undo ip pool pool-number</code>                               |

By default no address pool is defined by the system.

The *pool-number* ranges from 0 to 99. Addresses in each address pool must be consecutive, and each address pool can have at most 256 addresses.

### Assigning an IP Address for a PPP User

For a user accessing the Internet through remote PPP dialing, the system either specifies an address or allocates an unoccupied address selected from a local address pool to the user.

Perform the following configurations in interface view.

**Table 605** Assign IP Address for PPP User

| Operation                      | Command                                                           |
|--------------------------------|-------------------------------------------------------------------|
| Assign IP address for PPP user | <code>remote address { ip-address   pool [ pool-number ] }</code> |
| Cancel IP address of PPP user  | <code>undo remote address</code>                                  |

By default *pool-number* is 0.

### Configuring a Local User Database

When a user dials in to access the network, user information is looked up according to the following steps in the local user database:

- 1 Information about the user is sought in the local database. If the information is present, the login of the user is permitted.
- 2 If the user information is not in the local database and if the RADIUS server authentication is configured, the user information is sent to the RADIUS server for authentication. If authentication succeeds, the user can log on normally. Otherwise, the user is rejected.
- 3 If the user information is not in the local database and the RADIUS server authentication is not configured, the login of the user is rejected.

Various configuration tasks conducted in the local user database can be nested or combined and all local user databases can be configured in one command.

Perform the following configurations in system view.

#### Configure a User and Password

The user and the local authentication password can be configured in the local database

**Table 606** Configure Ordinary User and Password

| Operation                       | Command                                                                         |
|---------------------------------|---------------------------------------------------------------------------------|
| Configure the user and password | <code>local-user user-name [ password { simple   cipher } password ] ...</code> |
| Delete the user                 | <code>undo local-user user-name</code>                                          |

*user-name* can be a 1-32-bit character string or number. *Password* can be a 1-16-bit character string or number.

#### Configure Callback User

In the callback technique, first the client, on the user side, originates a call and requires callback from the server. The server receives the call and decides whether to call back.

The Callback technique enhances security. In the processing of a Callback, the server calls the client according to the call number configured locally. This avoids security risks caused by leakage of user name or password. The server can also classify call-in requests according to its configuration as refuse call, accept call (no call back) or accept callback. This serves to exert different limitations upon different clients and take initiative in ensuring resource access when there are incoming calls.

The callback technique has the following advantages:

- Saves communication expenses, especially when the call charge rates of two directions are different)
- Changes the call charge bearer
- Combines call charge lists

The security devices in 3Com routers support the callback technique that is divided into ISDN caller authentication callback and callback participated in by PPP.

ISDN caller authentication callback does not involve PPP, it directly authenticates whether the call-in number matches with the number configured by the server. Hence, only the server end needs a corresponding configuration and the client needs no modification.

**Table 607** Configure Callback User and the Callback Number

| Operation                                           | Command                                               |
|-----------------------------------------------------|-------------------------------------------------------|
| Configure the callback user and the callback number | <b>local-user user [ callback-number number ] ...</b> |
| Delete the callback user and the callback number    | <b>undo local-user user</b>                           |

A RADIUS server can be configured with *callback-number*, equivalent to *number*, which is defined locally. If **aaa authentication-scheme ppp default radius** is configured then *number*, which is configured locally, is invalid and the number to be transmitted to PPP will be decided by *callback-number* set on RADIUS server. If **aaa authentication-scheme ppp default radius local** is configured, local authentication is used only when the RADIUS server does not respond, and here *number* defined locally can work. If **aaa authentication-scheme ppp default none** is configured, *number* defined locally does not work.

### Configure User with Caller Number

After users with caller numbers are configured, the call-in caller numbers of users calling in can be authenticated in order. At present, only ISDN users can be configured to be such type of users.

**Table 608** Configure User with Caller Number

| Operation                           | Command                                                           |
|-------------------------------------|-------------------------------------------------------------------|
| Configure a user with caller number | <b>local-user user [ call-number number ] [ :sub-number ] ...</b> |
| Delete a user with caller number    | <b>undo local-user user-name</b>                                  |

### Configure FTP User and the Usable Directory

An FTP user and the FTP directory available for the user can be configured in the local database. The function is reserved temporarily for future extension.

**Table 609** Configure FTP User and the Usable Directory

| Operation                                      | Command                                                |
|------------------------------------------------|--------------------------------------------------------|
| Configure an FTP user and the usable directory | <b>local-user user [ ftp-directory directory ] ...</b> |
| Delete an FTP user and the usable directory    | <b>undo local-user user</b>                            |

### Authorize a User with Usable Service Types

The services, which can be used by a user, are authorized in the local database. Presently there are five service types, which are listed as follows:

- **exec** refers to operations that include logging in to the router and configuring it via Telnet or other means (such as Console port, AUX port, X25PAD call, etc).
- **exec-administrator**: Authorized “administrator” user can use EXEC. EXEC refers to the operation of logging into the router by means of Telnet or through console port, AUX port and X.25PAD.
- **exec-guest**: Authorized “guest” user can use EXEC.
- **exec-operator**: Authorized “operator” user can use EXEC.
- **ftp** refers to operations that include logon to the router via file transmission so as to share corresponding services.
- **ppp** refers to remote dial-in service used by the user.

When a single service is authorized to a user, it is only necessary to configure any one of the parameters of **exec**, **ftp**, and **ppp** after the service type. When multiple services are authorized to a user, it is necessary to configure over 2 types of the above-mentioned parameters, other than to use this command repeatedly, because the new service type will overwrite the old one, not to pack the service type.

**Table 610** Configure Authorizing a User with Usable Service Types

| Operation                                         | Command                                                                                                         |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Configure authorizing a user with usable services | <b>local-user user [ service-type { exec-administrator   exec-guest   exec-operator   ftp   ppp } ... ] ...</b> |
| Delete authorizing a user with usable services    | <b>undo local-user user-name</b>                                                                                |

By default users are authorized to use services of PPP type.

## Configure RADIUS Server

Perform the following configurations in system view.

### Configure IP Address, Authentication Port Number and Accounting Port Number of the Server Host

At most 3 RADIUS servers can be configured for a user.

RADIUS follows the principles below to select authentication and accounting server:

- Servers are used in the sequence in which they are configured.

- When the RADIUS server used first does not respond, the succeeding servers are used in sequence.

When the authentication or accounting port number is configured to 0, the client does not use the authentication or accounting function provided by the server.

**Table 611** Configure IP Address, Authentication Port Number and Accounting Port Number

| Operation                                                                                                         | Command                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure IP address (or host name), authentication port number and accounting port number of RADIUS server host. | <b>radius server</b> { <i>hostname</i>   <i>ip-address</i> } [ <b>authentication-port</b> <i>port-number</i> ] [ <b>accounting-port</b> <i>port-number</i> ] |
| Cancel RADIUS server with designated host address or host name                                                    | <b>undo radius server</b> { <i>hostname</i>   <i>ip-address</i> }                                                                                            |

The default authentication port number is 1812. When configured as 0, this server is not used as an authentication server. The default accounting port number is 1813. When configured as 0, this server is not used as an accounting server.

### Configure RADIUS Server Shared Secret

The shared secret is used to encrypt user password and generate a response authenticator. When RADIUS sends authentication messages, MD5 encryption is applied to important information such as passwords, so the security of the authentication information transmission in the network can be insured. To insure the identification validity of the two parties, the secret key of the router must be the same as the one set on the RADIUS server, so that it can pass the authentication of the RADIUS server.

**Table 612** Configure RADIUS Server Shared Secret

| Operation                                | Command                                |
|------------------------------------------|----------------------------------------|
| Configure shared secret of RADIUS server | <b>radius shared-key</b> <i>string</i> |
| Delete shared secret of RADIUS server    | <b>undo radius shared-key</b>          |

By default, no key is configured for the RADIUS server.

### Configure the Time Interval at Which the Request Packet is Sent Before the RADIUS Server Fails

To determine whether a RADIUS server is invalid, the router will send authentication request packets to the RADIUS server periodically.

**Table 613** Configure the Time Interval at Which the Request Packet is Sent Before RADIUS Server Fails

| Operation                                                                                     | Command                                             |
|-----------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Configure the time interval at which the authentication request packet is sent                | <b>radius timer response-timeout</b> <i>seconds</i> |
| Restore default value of the time interval at which the authentication request packet is sent | <b>undo radius timer response-timeout</b>           |

By default, the timeout interval is 10 seconds. The range is from 1 to 65535 seconds.

### Configure the Request Retransmission Times

If the RADIUS server fails to respond, the router sends the authentication request packet again periodically. If no RADIUS server response is received after the configured value of timeout, the authentication request packet needs to be transmitted again. The user can set the maximum number of times for the request retransmission, when the number of request retransmission exceed it, the system will consider the server fails to work normally and set it to *dead*.

**Table 614** Configure the Times of Request Retransmission

| Operation                                                | Command                         |
|----------------------------------------------------------|---------------------------------|
| Configure the times of request retransmission            | <code>radius retry times</code> |
| Restore default value of times of request retransmission | <code>undo radius retry</code>  |

By default, the times of request retransmission are three and the number ranges from 1 to 255.

### Configure the Time Interval at Which the Inquiry Packet is Sent

After the first RADIUS server breaks down (due to line failure between NAS and the server or RADIUS process failure, the system sets this server to "dead", and periodically queries whether it can work normally or not. If the server is found to work normally, then after the currently used server breaks down, the system will automatically uses the first one.

**Table 615** Configure the Time Interval for the Inquiry Packet

| Operation                                                                                       | Command                                 |
|-------------------------------------------------------------------------------------------------|-----------------------------------------|
| Configure the time interval at which the inquiry packet is sent after RADIUS server breaks down | <code>radius timer quiet minutes</code> |
| Restore default value of time interval at which the inquiry packet is sent                      | <code>undo radius timer quiet</code>    |

By default, the inquiry packet is sent at intervals of 5 minutes after the RADIUS server fails, and the interval ranges from 1 to 255 minutes.

### Configure the Time Interval at Which the Real-Time Accounting Packet is Sent to the RADIUS Server

After a user passes authentication, NAS sends the user's real-time accounting information to the RADIUS server periodically. If the real-time accounting request fails, the user is handled according to the `aaa accounting-scheme optional` command. If the `aaa accounting-scheme optional` command has been configured, the user can continue to use the network services, otherwise, NAS disconnects the user.

Usually, the server sends the accounting packet only according to the access time and disconnection time. But for higher reliability, the time interval at which the real-time accounting packet is sent to the RADIUS server can be configured.

**Table 616** Configure the Time Interval

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                                                                                               |                                                                  |
|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Configure the time interval at which the real-time accounting packet is sent to RADIUS server | <b>radius timer</b><br><b>realtime-accounting-scheme minutes</b> |
| Restore default value of the time interval at which the real-time accounting packet is sent   | <b>undo radius timer</b><br><b>realtime-accounting</b>           |

By default, the real-time accounting packet is sent to the RADIUS server at an interval of 0 minutes, indicating that real-time accounting is disabled. The interval ranges from 0 to 32767 minutes.

---

## Displaying and Debugging AAA and RADIUS

Use the **debugging** and **display** commands in all modes.

**Table 617** Display and debug AAA and RADIUS

| Operation                                  | Command                           |
|--------------------------------------------|-----------------------------------|
| Display status of dial-in users            | <b>display aaa user</b>           |
| View local user database                   | <b>display user</b>               |
| Enable RADIUS event debugging              | <b>debugging radius event</b>     |
| Enable RADIUS packet debugging             | <b>debugging radius packet</b>    |
| Enable RADIUS primitive language debugging | <b>debugging radius primitive</b> |

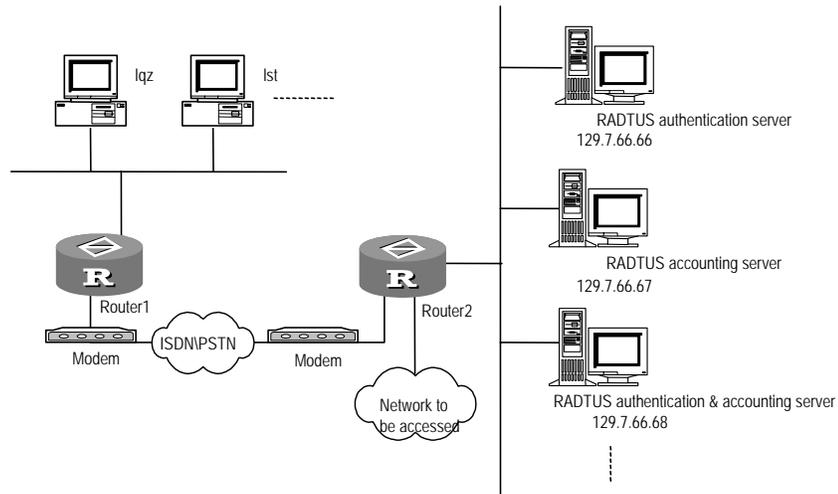
---

## AAA and RADIUS Configuration Examples

This section provides examples of using AAA and Radius within a network, with a suggested procedure for each configuration

### Accessing User Authentication Case 1

The RADIUS server is used for authentication. 129.7.66.66 acts as the first authentication and accounting server, and 129.7.66.67 as the second authentication and accounting server, both using default authentication port number 1812 and default accounting port number 1813.

**Figure 169** Networking diagram of typical AAA and RADIUS configuration

- 1 Enable AAA and configure default authentication method list of PPP user.

```
[Router] aaa-enable
[Router] aaa authentication-scheme ppp default radius
```

- 2 Configure IP address and port of RADIUS server.

```
[Router] radius server 129.7.66.66
[Router] radius server 129.7.66.67
```

- 3 Configure RADIUS server shared secret, retransmission times, and accounting option

```
[Router] radius shared-key this-is-my-secret
[Router] radius retry 2
[Router] aaa accounting-scheme optional
[Router] radius timer response-timeout 5
```

### Accessing User Authentication Case 2

129.7.66.66 acts as the first authentication and accounting server, port numbers being 1000 and 1001 respectively.

129.7.66.67 acts as the second authentication and accounting server, port numbers being 1812 and 1813 respectively.

Authenticate by the local database first, and if there is no response, use the RADIUS server.

Charge all users in real time. The real-time accounting packet is sent at the interval of 5 minutes.

See Figure 169.

- 1 Enable AAA and configure default authentication method list of PPP user.

```
[Router] aaa-enable
[Router] aaa authentication-scheme ppp default radius
```

- 2 Configure local-first authentication

```
[Router] aaa authentication-scheme local-first
```

**3** Configure RADIUS server

```
[Router] radius server 129.7.66.66 authentication-port 1000
accounting-port 1001
[Router] radius server 129.7.66.67
```

**4** Configure RADIUS server shared secret, retransmission times, and time length of timeout timer

```
[Router] radius shared-key this-is-my-secret
[Router] radius retry 2
```

**5** Configure real-time accounting with interval of 5 minutes

```
[Router] radius timer realtime-accounting 5
```

**Authenticating an FTP User**

The authentication server is 129.7.66.66, numbers of ports being 1812 and 1813.

Authenticate and charge FTP users using RADIUS server first, and if there is no response, do not authenticate or charge them.

See Figure 169.

**1** Enable AAA and configure default authentication method list of FTP user.

```
[Router] aaa-enable
[Router] aaa authentication-scheme login default radius none
```

**2** Enable FTP server

```
[Router] ftp-server enable
```

**3** Configure user abc and authorize the user to use FTP service.

```
[Router] local-user abc service-type ftp password simple hello
```

**4** Configure RADIUS server IP address and port, using default port number

```
[Router] radius server 129.7.66.66
```

**5** Configure RADIUS server shared secret, retransmission times, timeout and RADIUS server dead time.

```
[Router] rad shared-key this-is-my-secret
[Router] radius retry 4
[Router] radius timer response-timeout 2
[Router] radius timer quiet 1
```

**Troubleshooting AAA and RADIUS****Local user authentication is always rejected**

Follow the steps below.

- 1** Check whether correct password has been configured in `local-user` command.
- 2** Check whether the authorized service-type is correct.
- 3** When RADIUS server accounting is used, and the command `aaa accounting-scheme optional` is not configured, check whether the RADIUS server can be pinged through. Also check whether the address, port number and key of RADIUS server configured on the router for accounting are identical with those on the RADIUS server in use.
- 4** If the operation above does not work, use the `radius server` command to reconfigure the RADIUS server. Because of the communication failure with the RADIUS server mentioned. RADIUS server is considered by the system as

unavailable. Moreover as the `radius timer quiet` command has not been configured (defaulted as 5 minutes), or a relative long dead-time has been configured, the system does not know that the server has recovered. Use `undo radius server` command to delete the original RADIUS server, and reconfigure it by `radius server` command to activate the server immediately.

- 5 If none of the above operations work, check whether the RADIUS server has been configured correctly, and whether the modification has been activated

### **A user's RADIUS authentication is always rejected**

Follow the steps below.

- 1 Check whether the user name, password and service type are set correctly on RADIUS server.
- 2 Check whether the RADIUS server can be pinged through Check whether the address, port number and key of RADIUS server configured on the router are identical with those of the RADIUS server in use.
- 3 Use the `radius server` command to reconfigure the RADIUS server. Because of the communication failure with the server, RADIUS server may be considered by the system as unavailable by the system. And as the `radius timer quiet` command has not been configured (defaulted as 5 minutes), or a relative long dead-time has been configured, the system does not know that the server has recovered. Use `undo radius server` command to delete the original RADIUS server, and reconfigure it by `radius server` command to activate the server immediately.
- 4 Check whether the RADIUS server has been configured correctly, and whether the modification made just now has been activated.

### **A connected user cannot be seen in `display aaa user`**

Follow the steps below.:

- 1 Check whether AAA has been enabled.
- 2 Check whether the authentication methods contain "`none`", because users using none method will not be displayed in the command `display aaa user`.

### **No authentication is configured, yet users are still authenticated**

Follow the step below:

- 1 AAA has been enabled, and the default authentication method in AAA default authentication method list is "local". To disable the authentication, `aaa authentication-scheme ppp default none` should be configured. Meanwhile, it should be noted that `undo aaa authentication-scheme ppp default` can delete the default method; it can only restore the local authentication.



# 39

## CONFIGURING FIREWALL

This chapter covers the following topics:

- Firewall Overview
- Configure Firewall
- Displaying and Debugging Firewall
- Firewall Configuration Example

---

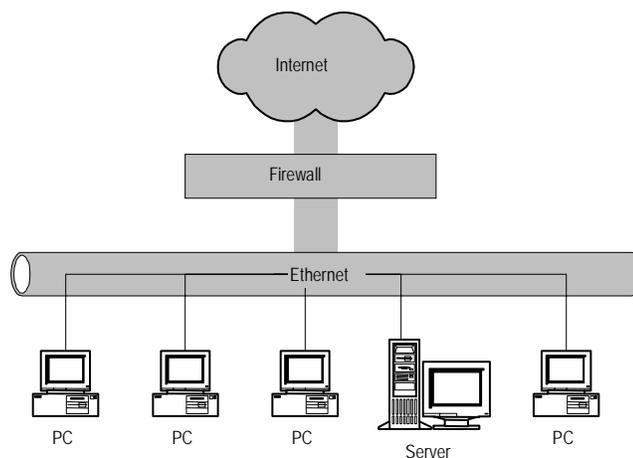
### Firewall Overview

A firewall is used to control the network equipment, which accesses the internal network resources. Setting a firewall at the access entry point of the intranet can control access to the internal network resources by the external network devices. In case of multiple entry points, every access entry point should be configured with a firewall to effectively control the external access. To ensure that all data entering the intranet is detected by the firewall, the firewall should be set at the intranet entry point.

A firewall is used not only to connect the Internet, but also to control the access to some special part of the internal network, such as to protect mainframes and important resources, such as data, in the network. Access to the protected data must be filtered through the firewall even if the access is from inside.

The firewall can screen the information, structure and operation of the intranet from outside by detecting, restricting and modifying data flow overriding the firewall. At present many firewalls also have other characteristics, for example, to identify the user, and conduct security processing (encryption) for information.

**Figure 170** A firewall isolates the internal network from the Internet



### Classification of Firewalls

Usually firewalls are divided into two types: network layer firewalls and application layer firewalls. A network layer firewall mainly obtains the packet head information of data packets, such as protocol number, source address and source port, destination address and destination port, or directly obtains the data of a packet head. But an application layer firewall analyzes the whole information stream.

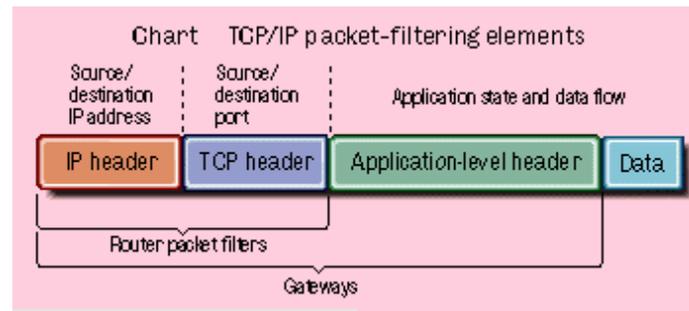
Commonly used firewalls include the following:

- **Application Gateway:** checks the application layer data of all data packets passing through this gateway. For example, the FTP application gateway will be a FTP server to a connected client end, but will be an FTP client to the server end. All FTP data packets transmitted on the connection must pass through this FTP application gateway.
- **Packet Filtering:** filters each data packet using the user-defined items. For example, to check if the source address and destination address of a data packet meet the rules. Packet filtering does not check call status, nor does it analyze the data. If data packets with port 21 or greater than or equal to 1024 are allowed to pass, then once a port meets this condition, the data packet can pass this firewall. If the rules are configured, then many data packets with hidden security troubles can be filtered out on this layer.
- **Proxy:** normally refer to address proxy on a proxy server or a router. It replaces the IP address and port of a host inside the network with the IP address and port of a server or router. For example, the intranet address of an enterprise is 129.0.0.0 network segment, and its formal external IP address is 202.38.160.2-202.38.160.6. When the internal host 129.9.10.100 accesses a certain external server in WWW mode, the IP address and port might become 202.38.160.2:6080 after passing through the proxy server. An address mapping table is maintained in the proxy server. When the external WWW server returns the result, the proxy server will convert this IP address and port into the internal IP address and port 80 of the network. The proxy server is used so that all access between the external network hosts and the internal network occurs through this proxy server. In this way, the access to internal devices that contain important resources can be controlled.

### Packet Filtering

Usually, packet filtering refers to filtering for IP data packets forwarded. For the data packets that need to be forwarded by a router, first the packet header information, including the number of the upper layer protocol carried by the IP layer, the packet's source/destination address and source/destination port is obtained. Then the information is compared with the set rules. Finally, it is decided whether to transfer or discard the data packet according to the comparison result.

Packet filtering (for IP data packets) selects the following elements for judgment (in the figure, the upper layer protocol carried by IP is TCP), as shown in the figure below.

**Figure 171** Packet filtering schematic diagram

The following can be realized by data packet filtering:

- Prohibit logging on with telnet from outside
- Every E-mail is sent by SMTP (Simple Message Transfer Protocol).
- One PC, rather than all other PCs, can send news to us by NNTP (Network News Transfer Protocol).

Packet filtering in 3Com routers security equipment features the following:

- Based on access-list (Access Control List - ACL): ACL is applied not only in packet filtering but also in other features where data streams need to be classified, such as address translation and IPSec.
- Support standard and extended ACL: Set a simple address range with the standard ACL or set the specific protocol, source address range, destination address range, source port range, destination port range, priority and service type with the extended ACL.
- Support time segment: Set ACL functions in a specific period of time, such as 8:00-2:00 of every Monday, or it can be as specific as from a year/month/day to another year/month/day.
- Support ACL automatic sorting: You can select sorting ACLs of a specific category to simplify the configuration and facilitate the maintenance.
- It can be as specific as indicating the input/output direction: For example, a special packet filtering rule can be applied in the output direction of the interface that is connected with WAN or another packet filtering rule is applied in the input direction.
- Support interface based filtering: It can be set to prohibit or permit to forward messages from a specific interface in a specific direction of an interface.
- Support creating a log for message meeting the condition: Record the related information of the message and provide a mechanism to guarantee that excessive resources are not consumed when a large number of logs are triggered in the same way.

**Access Control List** To filter data packets, rules need to be configured. A rule identifies a packet to be considered by an Access Control List.

The access control list is generally employed to configure the rules to filter data packets, and the types of access control lists are as follows:

- Standard access control list

```
acl acl-number [match-order config | auto]
rule { normal | special } { permit | deny } [source source-addr
source-wildcard | any]
```

- Extended access control list

```
acl acl-number [match-order config | auto]
rule { normal | special } { permit | deny } pro-number [source
source-addr source-wildcard | any] [source-port operator port1 [
port2]] [destination dest-addr dest-wildcard | any]
[destination-port operator port1 [port2]] [icmp-type icmp-type
icmp-code] [logging]
```

*Protocol-number* is the type of the protocol carried by IP in the form of name or number. The range of number is from 0 to 255, and the range of name is icmp, igmp, ip, tcp, udp, gre and ospf.

The above command can also be written in following formats due to the different *protocol*.

- 1 Command format when the protocol is ICMP:

```
rule { normal | special } { permit | deny } icmp [source source-addr
source-wildcard | any] [destination dest-addr dest-wildcard | any]
[icmp-type icmp-type icmp-code] [logging]
```

- 2 Command format when the protocol is IGMP, IP, GRE or OSPF:

```
rule { normal | special } { permit | deny } { ip | ospf | igmp | gre
} [source source-addr source-wildcard | any] [destination
dest-addr dest-wildcard | any] [logging]
```

- 3 Command format when the protocol is TCP or UDP:

```
rule { normal | special } { permit | deny } { tcp | udp } [source
source-addr source-wildcard | any] [source-port operator port1 [
port2]] [destination dest-addr dest-wildcard | any]
[destination-port operator port1 [port2]] [logging]
```

Only the TCP and UDP protocols require specifying the port range. Listed below are supported operators and their syntax.

**Table 618** Operators of the Extended Access Control List

| Operator and Syntax                         | Meaning                                 |
|---------------------------------------------|-----------------------------------------|
| <b>equal</b> <i>portnumber</i>              | Equal to 'portnumber'                   |
| <b>greater-than</b> <i>portnumber</i>       | Greater than 'portnumber'               |
| <b>less-than</b> <i>portnumber</i>          | Less than 'portnumber'                  |
| <b>not-equal</b> <i>portnumber</i>          | Not equal to 'portnumber'               |
| <b>range</b> <i>portnumber1 portnumber2</i> | Between 'portnumber1' and 'portnumber2' |

In specifying the *port number*, following mnemonic symbols may be used to stand for the actual meaning.

**Table 619** Mnemonic Symbol of the Port Number

| Protocol | Mnemonic Symbol | 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)             |
|          | chat            | 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           | Nickname (43)                         |
|          | www             | World Wide Web (HTTP, 80)             |

| Protocol | Mnemonic Symbol                          | 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 Securit Attribute Token Map (90) |
|          | echo                                     | Echo (7)                               |
|          | mobileip-ag                              | MobileIP-Agent (434)                   |
|          | mobileip-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) |                                        |

As for the ICMP, you can specify the ICMP packet type. You can use a number (ranging 0 to 255) or a mnemonic symbol to specify the packet type.

**Table 620** Mnemonic Symbol of the ICMP Message Type

| Operator and Syntax  | 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 |

By configuring the firewall and adding appropriate access rules, you can use packet filtering to check IP packets that pass the router. The passing of unexpected packets can thus be prohibited. In this way the packet filtering helps to protect the network security.

### Configure the match sequence of access control list

An access control rule can be composed of several “**permit**” and “**deny**” statements and the range of the data packet specified by each statement varies. The match sequence needs to be configured when matching a data packet and access control rule.

The maximum number of rules configured under an *acl-number* is 500 (that is, 500 rules can be configured in normal time range, and 500 rules can also be configured in special time range), and the number of total rules under all *acl-number* are not more than 500. When there is a conflict among several rules, the system will configure the match rules according to the following principle:

- Rules with the same serial number can be defined. If two rules with the same serial number conflict, use the “depth-first” principle to judge the *source-addr*, *source-wildcard-mask*, *destination-addr*, *destination-wildcard-mask*, protocol number and port number, then determine the sequence of the rule.
- If the ranges defined by the rules are the same, then determine the sequence of the rules according to the time sequence of definition. The system will choose the rule defined earlier.

The “depth-first” principle means matching the access rules with the smallest definition range of data packets. It can be achieved by comparing the wildcards of address. The smaller the wildcards are, the smaller the range specified by the host is. For example, 129.102.1.1.0.0.0.0 specifies a host (the address is 129.102.1.1), while 129.102.1.1.0.0.255.255 specifies a network segment (the range of the address is from 129.102.1.1 to 129.102.255.255), obviously the former is arranged in the front of access control rule.

The special standard is the following:

- For the statement of standard access control rules, compare the wildcards of the source addresses directly, and arrange according configuration sequence if the wildcards are the same.
- For the access control rules based on interface filtering, the rules configured with “**any**” are arranged last, and the rest will be arranged according to the configuration sequence.
- For extended access control rules, compare the wildcards of source addresses. If they are the same, then compare the wildcards of the destination address. If they are still the same, compare the range of port numbers, and the rule with smaller range will be arranged first. If the port numbers are the same, then match the rules according to the user's configuration sequence.

The **display acl acl-number** command can be used to view the executive sequence of the system access rules, and the rules listed ahead will be selected first.

---

## Configure Firewall

Firewall configuration includes:

- Enabling and Disabling a Firewall
- Configuring Standard Access Control List
- Configuring Extended Access Control List
- Setting the Default Firewall Filtering Mode
- Configuring Special Timerange
- Configuring Rules for Applying Access Control List on Interface
- Specifying Logging Host

## Enabling and Disabling a Firewall

A firewall should be enabled for filtering messages to set other configurations into effect.

Perform the following configurations in system view.

**Table 621** Enable/Disable Firewall

| Operation        | Command                 |
|------------------|-------------------------|
| Enable firewall  | <b>firewall enable</b>  |
| Disable firewall | <b>firewall disable</b> |

Firewalls are disabled by default.

### Configuring Standard Access Control List

The value of the standard access control list is an integer from 1 to 99. First of all, enter the ACL view through **acl** command, and configure the match sequence of the access control list, and then configure specific access rules through **rule** command. If the matching sequence is not configured, it will be conducted by **auto** mode.

Perform the following configurations in system view and ACL view.

**Table 622** Configure Standard Access Control List

| Operation                                                                  | Command                                                                                       |
|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Enter the ACL view and configure the match sequence of access control list | <b>acl acl-number [ match-order config   auto ]</b>                                           |
| Configure standard access list rule                                        | <b>rule { normal   special }{ permit   deny } [source source-addr source-wildcard   any ]</b> |
| Delete specific access list rule                                           | <b>undo rule { rule-id   normal   special }}</b>                                              |
| Delete access list                                                         | <b>undo acl {acl-number  all }</b>                                                            |

**normal** means that this rule functions during normal time range, while **special** means that this rule will function during the special time range. Users shall set the special time segment when using **special**. Multiple rules with the same serial number will be matched according to “depth-first” command.

By default **normal** is adopted.

### Configuring Extended Access Control List

The value of the extended access control list is an integer from 100 to 199. First of all, enter the ACL view through **acl** command, and configure the match sequence of the access control list, and then configure specific access rules through **rule** command. If the matching sequence is not configured, it will be conducted in **auto** mode.

Perform the following configurations in system view and ACL view.

**Table 623** Configure Extended Access Control List

| Operation                                                                  | Command                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enter the ACL view and configure the match sequence of access control list | <b>acl acl-number [ match-order config   auto ]</b>                                                                                                                                                                                                      |
| Configure extended access control list rule of TCP/UDP protocol            | <b>rule { normal   special }{ permit   deny } { tcp   udp } [source source-addr source-wildcard   any ] [source-port operator port1 [ port2 ] ] [ destination dest-addr dest-wildcard   any ] [destination-port operator port1 [ port2 ] ] [logging]</b> |
| Configure extended access control list rule of ICMP protocol               | <b>rule { normal   special }{ permit   deny } ICMP [source source-addr source-wildcard   any ] [ destination dest-addr dest-wildcard   any ] [icmp-type icmp-type icmp-code] [logging]</b>                                                               |

| Operation                                                      | Command                                                                                                                                                                 |
|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure extended access control list rule of other protocols | <code>rule { normal   special } { permit   deny } pro-number [source source-addr source-wildcard   any ] [ destination dest-addr dest-wildcard   any ] [logging]</code> |
| Delete specific access list rule                               | <code>undo rule { rule-id   normal   special }</code>                                                                                                                   |
| Delete access list                                             | <code>undo acl {acl-number/ all }</code>                                                                                                                                |

**normal** means that this rule functions during normal time range, while **special** means that this rule will function during the special time range. Users shall set the special time range when using **special**. Multiple rules with the same serial number will be matched according to “depth-first” principle.

By default, **normal** is adopted.

### Setting the Default Firewall Filtering Mode

The default firewall-filtering mode means that when there is no suitable access rule to determine whether a user data packet can pass through, the default firewall-filtering mode set by the user will determine whether to permit or inhibit this data packet to pass.

Perform the following configurations in system view.

**Table 624** Set Default Firewall Filtering Mode

| Operation                                                         | Command                              |
|-------------------------------------------------------------------|--------------------------------------|
| Set the default firewall filtering mode as message pass permitted | <code>firewall default permit</code> |
| Set the default firewall filtering mode as message pass inhibited | <code>firewall default deny</code>   |

The default firewall-filtering mode is message pass permitted by default.

### Configuring Special Timerange

#### Enabling and disabling filtering according to timerange

Filtering according to time range means in different time ranges the IP data packets are filtered with different access rules. It is also called the special rules for special time.

The time ranges are classified into two types according to actual applications:

- Special time range: Time within the set time range (specified by key word **special**)
- Normal time range: Time beyond the specified time range (specified by key word **normal**)

Similarly, the access control rules are also classified into two types:

- Normal packet-filtering access rules
- Special time range packet-filtering access rules

These two types of time ranges define different access control lists and access rules, which are not affected by each other. In actual applications, they can be considered as two independent sets of rules, and the system will determine which

one to use after viewing the current time range (special or normal). For example, the current system time is in special time range (which is defined by **rule special acl-number**), and then the special time range rules will be used for filtering. But when the current system time is switched to the normal time range (which is defined by **rule normal acl-number**), the normal time range rules will be used for filtering.

Perform the following configurations in system view.

**Table 625** Enable/Disable Filtering According to Timerange

| Operation                                | Command                  |
|------------------------------------------|--------------------------|
| Enable filtering according to timerange  | <b>timerange enable</b>  |
| Disable filtering according to timerange | <b>timerange disable</b> |

By default, the filtering based on time range is disabled.

Only when the switch of filtering according to time range is enabled will the special time range access rules set by the user be effective. But when this switch is disabled, the normal time range access rules will be applied.

### Set special time range

When you enable message-filtering according to time range, the firewall adopts user defined special time range access rules for filtering during the time range defined by the user. The newly defined special time range becomes valid about 1 minute after it is defined, and that defined last time will become invalid automatically.

Perform the following configurations in system view.

**Table 626** Set Special Time Range

| Operation                 | Command                                                       |
|---------------------------|---------------------------------------------------------------|
| Set special time range    | <b>settr begin-time end-time [ begin-time end-time..... ]</b> |
| Cancel special time range | <b>undo settr</b>                                             |

By default, the system adopts the access rules defined for normal time range for message filtering. The command **settr** can define 6 time ranges at the same time. The format of the time range is hh:mm. The value of hh is 0 - 23 hours and the value of mm is 0 - 59 minutes.

The command **display clock** can be used to view the current clock status of the system.

## Configuring Rules for Applying Access Control List on Interface

To apply access rules to specific interfaces to filter messages, it is necessary to apply the access control list rules to the interfaces. Users can define different access control rules for messages of both inbound and outbound directions at one interface.

Perform the following configurations in interface view.

**Table 627** Configure Rules for Applying Access Control List on Interface

| Operation                                                     | Command                                                                     |
|---------------------------------------------------------------|-----------------------------------------------------------------------------|
| Specify rule for filtering receive/send messages on interface | <b>firewall packet-filter <i>acl-number</i> [ inbound   outbound ]</b>      |
| Cancel rule for filtering receive/send messages on interface  | <b>undo firewall packet-filter <i>acl-number</i> [ inbound   outbound ]</b> |

By default no rule for filtering messages on interface is specified.

In one direction of an interface (**inbound** or **outbound**), up to 20 access rules can be applied. That is to say, 20 rules can be applied in **firewall packet-filter inbound**, and 20 rules can be applied in **firewall packet-filter outbound**.

If two rules with different sequence numbers conflict, then the number with greater *acl-number* should be matched preferentially.

### Specifying Logging Host

Firewall supports a logging function. When an access rule is matched, and if the user has specified to generate logging for this rule, logs can be sent to and recorded and saved by the logging host.

Perform the following configurations in system view.

**Table 628** Specify Logging Host

| Operation            | Command                                        |
|----------------------|------------------------------------------------|
| Specify logging host | <b>ip host <i>unix-hostname ip-address</i></b> |
| Cancel logging host  | <b>undo ip host</b>                            |

For detailed description logging host parameters, see “Logging Function” in “System Management”.

### Displaying and Debugging Firewall

Use **debugging**, **reset** and **display** commands in all views.

**Table 629** Display and Debug Firewall

| Operation                                                      | Command                                                                       |
|----------------------------------------------------------------|-------------------------------------------------------------------------------|
| Display firewall status                                        | <b>display firewall</b>                                                       |
| Display packet filtering rule and its application on interface | <b>display acl [ all   <i>acl-number</i>   interface <i>type number</i> ]</b> |
| Display current timerange                                      | <b>display timerange</b>                                                      |
| Display whether the current time is within special timerange   | <b>display isintr</b>                                                         |
| Clear access rule counters                                     | <b>reset acl counters [ <i>acl-number</i> ]</b>                               |
| Enable the information debugging of firewall packet filtering  | <b>debugging filter { all   icmp   tcp   udp }</b>                            |

### Firewall Configuration Example

The following is a sample firewall configuration in an enterprise.

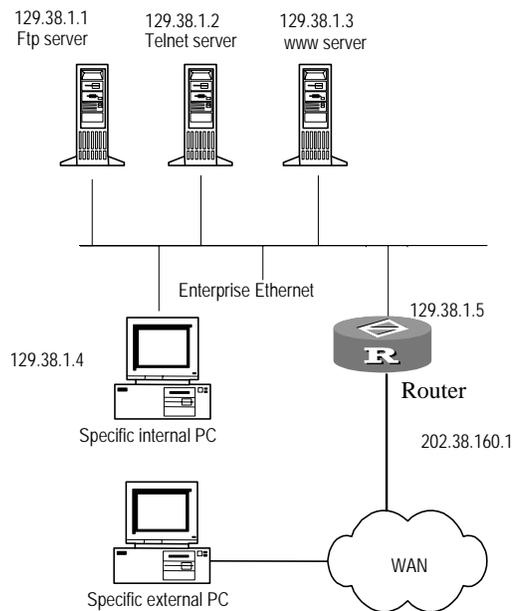
This enterprise accesses the Internet through interface Serial 0 of one 3Com router, and the enterprise provides www, FTP and Telnet services to the outside. The internal sub-network of the enterprise is 129.38.1.0, the internal ftp server address 129.38.1.1, internal Telnet server address 129.38.1.2, and the internal

www server address 129.38.1.3. The enterprise address to the outside is 202.38.160.1. Address conversion has been configured on the router so that the internal PC can access the Internet, and the external PC can access the internal server. By configuring a firewall, the following are expected:

- Only specific users from external network can access the internal server.
- Only a specific internal host can access the external network.

In this example, assume that the IP address of a specific external user is 202.39.2.3.

**Figure 172** Sample networking of firewall configuration



**1** Enable firewall

```
[Router] firewall enable
```

**2** Configure firewall default filtering mode as packet pass permitted

```
[Router] firewall default permit
```

**3** Configure access rules to inhibit passing of all packets

```
[Router] acl 101
[Router-acl-101] rule deny ip source any destination any
```

**4** Configure rules to permit specific host to access external network, to permit internal server to access external network.

```
[Router-acl-101] rule permit ip source 129.38.1.4 0 destination any
[Router-acl-101] rule permit ip source 129.38.1.1 0 destination any
[Router-acl-101] rule permit ip source 129.38.1.2 0 destination any
[Router-acl-101] rule permit ip source 129.38.1.3 0 destination any
```

**5** Configure rules to permit specific external user to access internal server

```
[Router] acl 102
[Router-acl-102] rule permit tcp source 202.39.2.3 0 destination
202.38.160.1 0
```

- 6 Configure rules to permit specific user to obtain data (only packets of port greater than 1024) from an external network

```
[Router-acl-102] rule permit tcp source any destination 202.38.160.1
0.0.0.0 destination-port greater-than 1024
```

- 7 Apply rule 101 on packets coming in from interface Ethernet0

```
[Router-Ethernet0] firewall packet-filter 101 inbound
```

- 8 Apply rule 102 on packets coming in from interface Serial0

```
[Router-Serial0] firewall packet-filter 102 inbound
```

This chapter covers the following topics:

- IPsec Protocol Overview
- Configuring IPsec
- Creating a Security Policy
- Displaying and Debugging IPsec
- IPsec Configuration Example
- Troubleshooting IPsec

---

### IPsec Protocol Overview

IPsec is the general name of a series of network security protocols that provide services such as access control, connectionless integrity, data authentication, anti-replay, encryption and classified encryption of data flow for both communication parties.

With IPsec, it is unnecessary to worry about the data to be monitored, modified or forged when they are transmitted in public network, which enables secure access to VPN (Virtual Private Network), including internal, external networks and that between remote users.

#### NDEC Card

In actual implementation, the packets processing performed by IPsec includes processing ESP protocol, adding an authentication header to packets after encryption, and deleting the authentication header after packets are authenticated. To ensure security, the algorithms of encryption, decryption, and authentication are very complicated. The encryption and decryption algorithm process of the router occupies large quantities of resources; as a result the performance of the integrated machine is affected. Using crypto cards (modular plug-in cards), the 3Com modular series routers process encryption and decryption operation in a way of hardware. It improves performance of the router when software is processing the IPsec, and improves the operating efficiency of the router.

A crypto card uses the following procedure to implement encryption/decryption. The host of the router transmits the data to be encrypted or decrypted to the crypto card. Then the crypto card performs the encryption or decryption algorithms, and adds or deletes encryption frame header. After that, the crypto card will send the encrypted or decrypted data back to the host to forward.

Dividing the works of processing user data among multiple crypto cards. 3Com modular series routers can support multiple crypto cards. The host software divides the work of processing the user data among the crypto cards in normal

state by polling. Thus, crypto cards can synchronously process user data, which improves the speed of data encryption and decryption.

For the IPsec applied at the crypto card side, the crypto cards will be unable to implement the IPsec processing if all the crypto cards on the router are in abnormal state. In this case, given that the host has been enabled to backup the crypto cards, the IPsec module of the operating system will replace the crypto cards to implement the IPsec processing, if the IPsec module supports the encryption/authentication algorithm used by the crypto cards. Thus, the software IPsec module fulfills the backup of crypto cards.



*The processing mechanism of the crypto cards and that of the software IPsec module is almost the same. The only difference is that the former implements the encryption/decryption processing through the software and the latter through the the main operating system.*

### IPsec Message Processing

IPsec can process messages as follows (with AH protocol as an example):

- Add authentication header to messages: IP messages sent by the module block from IPsec queue are read, and an AH header is added according to the configured protocol mode (transport or tunnel mode), then forward it by IP layer.
- Cancel the authentication header after messages are authenticated: The IP message received at the IP layer is analyzed as a local host address with protocol number 51, then the corresponding protocol switch table item is searched and the corresponding input processing function is called. This processing function authenticates the message to make a comparison with the original authentication value. If the values are the same, the added AH is canceled, and the original IP message is restored. Then IP input flow is recalled for processing. Otherwise, this message is discarded.

### IPsec Related Terms

The following terms are important to an understanding of IPsec:

- **Data stream:** A combination of a group of traffic, which is prescribed by source address/mask, destination address/mask, encapsulation upper-level protocol number of IP message, source port number, destination port number, etc. Generally, a data stream is defined by an access list, and all messages permitted by access list are called a data stream logically. A data stream can be a TCP connection between the endpoints, or all the data stream transferred between two subnets. IPsec can implement different security protections for different data streams. For example, it can use different security protocols for different data flow, algorithm and ciphering.
- **Security policy:** The policy, which is configured manually by the user to define what security measure to take for what data stream. The data stream is defined by configuring multiple rules in an access list, and in security policy this access list is quoted to determine to protect the data flow. *Name* and *Sequence number* define a security policy uniquely.
- **Security policy group:** The set of the security policies with the same name. A security policy group can be applied or cancelled on an interface, applying multiple security polices in the same security policy group to this interface, to implement different security protection for different data streams. The security

policy with smaller sequence number in the same security policy group is of higher priority.

- **SA (Security Association):** IPSec provides security service for data streams through security association, which includes protocol, algorithm, key and other contents and specifies how to process IP messages. An SA is a unidirectional logical connection between two IPSec systems. Inbound data stream and outbound data stream are processed separately by inbound SA and outbound SA. SA is identified uniquely by a triple (SPI, IP destination address and security protocol number (AH or ESP)). SA can be established through manual configuration or automatic negotiation. A SA can be manually established after some parameters set by the users at two ends are matched and the agreement is reached through negotiation. Automatic negotiation mode is created and maintained by IKE, i.e., both communication parties are matched and negotiated based on their own security policies without user's interface.
- **SA Update Time:** There are two SA update time modes: *time-based* during which SA is updated at regular intervals and *traffic-based*, during which SA is updated whenever certain bytes are transmitted.
- **SPI (Security Parameter Index):** a 32-bit value, which is carried by each IPSec message. The trio of SPI, IP destination address, security protocol number, identify a specific SA uniquely. When SA is configured manually, SPI should also be set manually. To ensure the uniqueness of an SA, you must specify different SPI values for different SAs. When SA is generated with IKE negotiation, SPI will be generated at random.
- **IPSec Proposal:** It includes security protocol, algorithm used by security protocol, and the mode how security protocol encapsulates messages, and prescribes how ordinary IP messages are transformed into IPSec messages. In security policy, a IPSec proposal is quoted to prescribe the protocol and algorithm adopted by this security policy.

---

## Configuring IPSec

IPSec configuration includes:

- Creating an Encryption Access Control List
- Configure NDEC Cards
- Enable the main software backup
- Defining IPSec Proposal
- Selecting the Encryption and Authentication Algorithm
- Creating a Security Policy
- Apply Security Policy Group on Interface

### Creating an Encryption Access Control List

Matching the encrypted access control list determines which IP packets are encrypted and sent, and which IP packets are directly forwarded. Encryption access control lists are different from the ordinary ones, because the ordinary ones only determine which data can pass an interface. An encryption access list is defined by an extended IP access list.

For one kind of communication to accept one security protection mode (only authentication, for instance), and another kind to accept a different one (both

authentication and encryption, for instance), it is necessary to create two different encryption access control lists and apply them to different security policies.

Encryption access control list can be used to judge both inbound communication and outbound communication.

To create an encryption access control list, perform the following configurations in system view.

**Table 630** Create Encryption Access Control List

| Operation                                                                               | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Establish encryption access control list (applicable to IPsec software and crypto card) | <code>acl <i>acl-number</i> [ <i>match-order config</i>   <i>auto</i> ]<br/>rule { <i>normal</i>   <i>special</i> } { <i>permit</i>   <i>deny</i> } <i>pro-number</i> [<i>source source-addr source-wildcard</i>   <i>any</i> ] [<i>source-port operator port1</i> [ <i>port2</i> ] ] [ <i>destination dest-addr dest-wildcard</i>   <i>any</i> ] [<i>destination-port operator port1</i> [ <i>port2</i> ] ] [<i>icmp-type icmp-type icmp-code</i>] [<i>logging</i>]</code> |
| Delete encryption access control list (applicable to IPsec software and crypto card)    | <code>undo rule { <i>rule-id</i>   <i>normal</i>   <i>special</i> }<br/>undo acl { <i>acl-number</i> / <i>all</i> }</code>                                                                                                                                                                                                                                                                                                                                                  |

The information transmitted between the source and destination addresses specified by the **permit** key word is encrypted/decrypted by the peer router.

The **deny** key word does not allow the defined policy to be applied in the security policy. This can prevent the router from encrypting or decrypting communication information. (that is to say not allowing the policy defined in this security policy to be applied). If all the security policies on an interface are denied, this communication is not protected by encryption.

Do not use the wildcard **any** in the source address and destination address of the command **rule** when creating an encryption ACL. This is because when the data packet enters the router, and is sent to a router not configured with encryption, the key word **any** will cause the router to try to establish encryption session with a router without encryption.

The encryption access list defined at local router must have a mirror encryption access list defined by the remote router so that the communication contents encrypted locally can be decrypted remotely.

When the user uses the **display acl** command to browse the access lists of the router, all extended IP access lists, including those for both communication filtering and for encryption, will be displayed in the command outputs. That is to say, these two kinds of extended access lists for different purposes are not distinguished in the screen output information.

## Configure NDEC Cards **Enable the crypto cards**

When several crypto cards on the router work simultaneously, The commands **enable** and **disable** can be used to manage the crypto cards. To facilitate the management and debugging, you can set a crypto card to be in disabled state (disable the crypto card to process data) or enabled state as needed. Executing the **enable** command on a crypto card in **disable** state will reset and initiate it.

Perform the following configurations in system view.

**Table 631** Enable/Disable the NDECCard

| Operation               | Command                                 |
|-------------------------|-----------------------------------------|
| Enable the crypto card  | <b>encrypt-card enable [ slot-id ]</b>  |
| Disable the crypto card | <b>encrypt-card disable [ slot-id ]</b> |

By default, all the crypto cards are enabled.

### **Synchronize the crypto card clock with the router host clock**

NDEC cards have their own clock. To synchronize the crypto card clock and the host clock, the host will send the command of synchronizing clocks to the crypto card periodically. The users can synchronize the crypto card clock and the host clock immediately using this command.

Perform the following configuration in system view.

**Table 632** Synchronize the NDEC Card Clock and the Router Host Clock

| Operation                                                      | Command                                  |
|----------------------------------------------------------------|------------------------------------------|
| Synchronize the crypto card clock (applicable to crypto cards) | <b>encrypt-card set time [ slot-id ]</b> |

### **Set the output of the crypto card log**

Perform the following configuration in system view.

**Table 633** Set the Output of the NDEC Card Log

| Operation                                                     | Command                                                         |
|---------------------------------------------------------------|-----------------------------------------------------------------|
| Enable/Disable the output of log (applicable to crypto cards) | <b>encrypt-card set syslog { enable   disable } [ slot-id ]</b> |

By default, the outputting of log is disabled.

## **Enable the main software backup**

For the SAs applied at the encrypt-card side, the works of IPSec processing on the traffic will be shared among the normal encrypt-cards as long as there are encrypt-cards in normal status on the router. If all the encrypt-cards are abnormal, there will be no encrypt-cards can conduct the IPSec processing. In this case, given that the host has already been enabled to backup the encrypt-cards, the IPSec module will replace the encrypt-cards to conduct IPSec processing on the packets, if the IPSec module (the main software) supports the encryption/authentication algorithm used by this SA. If it does not, the packets will be discarded.

Perform the following configurations in system view.

**Table 634** Enable/Disable the Host to Backup the NDEC Cards

| Operation                                   | Command                                 |
|---------------------------------------------|-----------------------------------------|
| Enable the host to backup the crypto cards  | <code>encrypt-card backuped</code>      |
| Disable the host to backup the crypto cards | <code>undo encrypt-card backuped</code> |

By default, the host is disabled to backup the crypto cards.

## Defining IPsec Proposal

The IPsec saved in conversion mode needs a special security protocol and encryption/authentication algorithm to provide various security parameters for the IPsec negotiation security confederation. Both ends must use the same conversion mode for successfully negotiating IPsec security confederation.

### Define IPsec proposal

Multiple IPsec proposals can be defined, and then one or many of them can be quoted in one security policy. The same security protocol and algorithm conversion must be configured at both ends when security confederation is manually created.

If you modify the conversion mode after successful security confederation negotiation, this security confederation will still use the former conversion mode, while the newly negotiated security confederation will use the new conversion mode. To make the new setting effective at once, it is necessary to use the `reset ipsec sa` command to clear part or all of the SA database.

Perform the following configurations in system view.

**Table 635** Define IPsec Proposal

| Operation                                                                                     | Command                                                    |
|-----------------------------------------------------------------------------------------------|------------------------------------------------------------|
| Define IPsec proposal to enter the view of IPsec proposal view (applicable to IPsec software) | <code>ipsec proposal proposal-name</code>                  |
| Delete IPsec proposal view (applicable to IPsec software)                                     | <code>undo ipsec proposal proposal-name</code>             |
| Define the IPsec proposal and enter view of IPsec proposal view (applicable to crypto card)   | <code>crypto ipsec card-proposal proposal-name</code>      |
| Delete IPsec proposal view of the crypto card (applicable to crypto card)                     | <code>undo crypto ipsec card-proposal proposal-name</code> |

By default, no proposal view is configured.

### Set the Mode for Security Protocol to Encapsulate IP Message

The IP message encapsulating mode selected by both ends of security tunnel must be consistent.

Configure the following in IPsec proposal view (or proposal view of crypto card).

**Table 636** Set the Mode for Security Protocol to Encapsulate Messages

| Operation                                                                                                 | Command                                                |
|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Set the mode for security protocol to encapsulate messages (applicable to IPsec software and crypto card) | <code>encapsulation-mode { transport   tunnel }</code> |

|                                                                                               |                                      |
|-----------------------------------------------------------------------------------------------|--------------------------------------|
| Restore the default message encapsulating mode (applicable to IPsec software and crypto card) | <code>undo encapsulation-mode</code> |
|-----------------------------------------------------------------------------------------------|--------------------------------------|

The default mode is tunnel-encapsulation mode.

### Select Security Protocol

After the transport mode is defined, it is necessary to select the security protocol for the transport mode. The security protocols available at present include AH and ESP, both of which can also be used at the same time. Both ends of security tunnel must select the same security protocols.

The data encapsulation forms of various security protocols in transport and tunnel mode are shown in the following figure:

**Figure 173** Data encapsulation form of the security protocol

| Encryption protocol | Transmission mode            |                                   |
|---------------------|------------------------------|-----------------------------------|
|                     | transport                    | tunnel                            |
| ah-new              | IP   AH   data               | IP   AH   IP   data               |
| esp-new             | IP   ESP   data   ESP-T      | IP   ESP   IP   data   ESP-T      |
| ah-esp-new          | IP   AH   ESP   data   ESP-T | IP   AH   ESP   IP   data   ESP-T |

Please configure the following in IPsec Proposal view (or proposal view of crypto card).

**Table 637** Select Security Protocol

| Operation                                                                                    | Command                                                  |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Set security protocol used for IPsec proposal (applicable to IPsec software and crypto card) | <code>transform { ah-new   esp-new   ah-esp-new }</code> |
| Restore the default security protocol (applicable to IPsec software and crypto card)         | <code>undo transform</code>                              |

The security protocol `esp-new` prescribed in RFC2406 is used by default.

### Selecting the Encryption and Authentication Algorithm

AH protocol cannot encrypt but authenticate packets. ESP in IPsec software supports five security encryption algorithms that are **3des**, **des**, **blowfish**, **cast** and **skipjack**. There are seven kinds of security encryption algorithms supported by ESP crypto card, which are **3des**, **des**, **blowfish**, **cast**, **skipjack**, **aes**, and **qc5**.

The current security authentication algorithm includes MD5 (message digest Version 5) and SHA (security hashing algorithm), both of which are HMAC variables. HMAC is a hashing algorithm with key, which can authenticate data. The algorithm md5 uses 128-bit key and the algorithm sha1 uses 160-bit key, and the former calculates faster than the latter while the latter is more secure than the former.

Both ends of security tunnel must select the same encryption algorithm and authentication algorithm.

Perform the following configurations in IPsec proposal view (or proposal view of crypto card)

**Table 638** Select Encryption Algorithm and Authentication Algorithm

| Operation                                                                                                  | Command                                                                                           |
|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Set the encryption algorithm adopted by ESP protocol (applicable to IPsec software)                        | <code>esp-new encryption-algorithm { 3des   des   blowfish   cast   skipjack }</code>             |
| Set the encryption algorithm adopted by ESP protocol (applicable to crypto card)                           | <code>esp-new encryption-algorithm { 3des   des   blowfish   cast   skipjack   aes   qc5 }</code> |
| Cancel the encryption algorithm adopted by ESP protocol (applicable to IPsec software and crypto card)     | <code>undo esp-new encryption-algorithm</code>                                                    |
| Set the authentication algorithm adopted by ESP protocol (applicable to IPsec software and crypto card)    | <code>esp-new authentication-algorithm { md5-hmac-96   sha1-hmac-96 }</code>                      |
| Cancel the authentication algorithm adopted by ESP protocol (applicable to IPsec software and crypto card) | <code>undo esp-new authentication-algorithm</code>                                                |
| Set the authentication algorithm adopted by AH protocol (applicable to IPsec software and crypto card)     | <code>ah-new authentication-algorithm { md5-hmac-96   sha1-hmac-96 }</code>                       |
| Restore the authentication algorithm adopted by AH protocol (applicable to IPsec software and crypto card) | <code>undo ah-new authentication-algorithm</code>                                                 |

By default, ESP protocol adopts **des** encryption algorithm and **md5-hmac-96** authentication algorithm, and AH protocol adopts **md5-hmac-96** authentication algorithm.



*The commands `undo esp-new encryption-algorithm` and `undo esp-new authentication-algorithm` cannot be used at the same time. That is, ESP must use at least one type of encryption algorithm or authentication algorithm.*

## Creating a Security Policy

The following questions should be answered before a security policy is created:

- Which data needs IPsec protection?
- How long should the data stream be protected by SA?
- What security policy will be used?
- Is the security policy created manually or through IKE negotiation?

The following aspects require attention when a security policy is created:

- To create a security policy, you must specify its negotiation mode. Once a security policy is created, its negotiation mode cannot be modified. To create a new security policy, the current one must be deleted. For example, a security policy created with **manual** mode cannot be modified to a policy with **isakmp** mode. To have the same policy with a different mode, you must delete the policy then recreate it with a different mode.
- Security policies with the same name together comprise a security policy group. The name and the sequence number define a security policy uniquely, and a security policy group can include at most 100 security policies. The security policy with smaller sequence number in the same security policy group is of

higher priority. When a security policy group is applied on an interface, actually multiple different security policies in this security policy group are applied on it at the same time, so that different data streams are protected by different SAs.

## Creating a Security Policy Manually

Perform the following configurations in system view.

**Table 639** Establish Security Policy Manually

| Operation                                                                                                 | Command                                                                  |
|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Create security policy manually to enter IPsec policy view (applicable to IPsec software and crypto card) | <b>ipsec policy <i>policy-name</i><br/><i>sequence-number</i> manual</b> |
| Modify the created security policy manually (applicable to IPsec software and crypto card)                | <b>ipsec policy <i>policy-name</i><br/><i>sequence-number</i></b>        |
| Delete the created security policy (applicable to IPsec software and crypto card)                         | <b>undo ipsec policy <i>policy-name</i><br/><i>sequence-number</i></b>   |

By default, no security policy is created.

### Configure access control list quoted in security policy

After a security policy is created, it is also necessary to specify the quoted encryption access control list item for it to judge which inbound/outbound communications should be encrypted and which should not.

Perform the following configurations in IPsec policy view.

**Table 640** Configure Encryption Access Control List Quoted in Security Policy

| Operation                                                                                                         | Command                                       |
|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Configure encryption access control list quoted in security policy (applicable to IPsec software and crypto card) | <b>security acl <i>access-list-number</i></b> |
| Cancel encryption access control list quoted in security policy (applicable to IPsec software and crypto card)    | <b>undo security acl</b>                      |

By default, no encryption access control list is quoted in the security policy.

### Set start point and end point of security tunnel

The channel with security policy applied is usually called a *security tunnel*. A security tunnel is established between local and peer gateways, so the local address and the remote address must be set correctly to successfully establish a security tunnel.

For the security policy created manually, only one remote address can be specified. To set a new remote address, the previously specified one must be deleted first. Only when both local address and remote address are set correctly can a security tunnel be created.

Perform the following configurations in IPsec policy view.

**Table 641** Specify Start Point and End Point of Security Tunnel

| Operation                                                                           | Command                               |
|-------------------------------------------------------------------------------------|---------------------------------------|
| Set local address of security tunnel (applicable to IPsec software and crypto card) | <b>tunnel local <i>ip-address</i></b> |

| Operation                                                                               | Command                              |
|-----------------------------------------------------------------------------------------|--------------------------------------|
| Delete local address of security tunnel (applicable to IPsec software and crypto card)  | <b>undo tunnel local ip-address</b>  |
| Set remote address of security tunnel (applicable to IPsec software and crypto card)    | <b>tunnel remote ip-address</b>      |
| Delete remote address of security tunnel (applicable to IPsec software and crypto card) | <b>undo tunnel remote ip-address</b> |

By default, the start point and the end point of the security tunnel are not specified.

### Set IPsec proposal quoted in security policy

When SA is created manually, a security policy can quote only one IPsec proposal, and to set new IPsec proposal, the previously configured one must be deleted first. If the local IPsec proposal cannot match the peer one completely, then it will not establish SA successfully, then the messages that require protection will be discarded.

The security policy determines its protocol, algorithm and encapsulation mode by quoting the IPsec proposal. A IPsec proposal must be established before it is quoted.

Perform the following configurations in IPsec policy view.

**Table 642** Configure IPsec Proposal Quoted in Security Policy

| Operation                                                                                      | Command                       |
|------------------------------------------------------------------------------------------------|-------------------------------|
| Set IPsec proposal quoted in security policy (applicable to IPsec software and crypto card)    | <b>proposal proposal-name</b> |
| Cancel IPsec proposal quoted in security policy (applicable to IPsec software and crypto card) | <b>undo proposal</b>          |

By default, the security policy quotes no IPsec proposal.

### Set SPI of security policy association and its adopted key

In security policy association established manually, if AH protocol is included in the quoted IPsec proposal, it is necessary to set manually the SPI of AH SA and the quoted authentication key for the inbound/outbound communications. If the ESP protocol is included in the quoted IPsec proposal, it is necessary to manually set the SPI of ESP SA and the quoted authentication key and ciphering key for the inbound/outbound communications.

At both ends of a security tunnel, the SPI and the key of the local inbound SA must be the same as those of the peer outbound SA, and the SPI and the key of the local outbound SA must be the same as those of the peer inbound SA.

Perform the following configurations in IPsec policy view.

1 Set SPI parameters for the security policy association

**Table 643** Configure SPI Parameters of Security Policy Association

| Operation                                                                                              | Command                                      |
|--------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Set SPI parameters of inbound SA of AH/ESP protocol (applicable to IPsec software and crypto card)     | <b>sa inbound {ah   esp} spi spi-number</b>  |
| Delete SPI parameters of inbound SA of AH/ESP protocol (applicable to IPsec software and crypto card)  | <b>undo sa inbound {ah   esp} spi</b>        |
| Set SPI parameters of outbound SA of AH/ESP protocol (applicable to IPsec software and crypto card)    | <b>sa outbound {ah   esp} spi spi-number</b> |
| Delete SPI parameters of outbound SA of AH/ESP protocol (applicable to IPsec software and crypto card) | <b>undo sa outbound {ah   esp} spi</b>       |

By default, no SPI value of inbound/outbound SA is set.

2 Set the key used by the security policy association

**Table 644** Configure Key Used by Security Policy Association

| Operation                                                                                                                         | Command                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Set authentication key of AH protocol (input in hexadecimal mode) (applicable to IPsec software and crypto card)                  | <b>sa { inbound   outbound } ah hex-key-string hex-key</b>      |
| Delete authentication key of AH protocol (in hexadecimal mode) (applicable to IPsec software and crypto card)                     | <b>undo sa { inbound   outbound } ah hex-key-string</b>         |
| Set authentication key of AH protocol (input in string mode) (applicable to IPsec software and crypto card)                       | <b>sa { inbound   outbound } { ah string-key string-key</b>     |
| Delete authentication key of AH protocol (character string) (applicable to IPsec software and crypto card)                        | <b>undo sa { inbound   outbound } ah string-key</b>             |
| Configure authentication key of ESP protocol (input in hexadecimal system) (applicable to IPsec software and crypto card)         | <b>sa { inbound   outbound } esp authentication-hex hex-key</b> |
| Delete authentication key of ESP protocol (applicable to IPsec software and crypto card)                                          | <b>undo sa { inbound   outbound } esp authentication-hex</b>    |
| Set ciphering key of ESP protocol (input in hexadecimal system) (applicable to IPsec software and crypto card)                    | <b>sa { inbound   outbound } esp encryption-hex hex-key</b>     |
| Delete ciphering key of ESP protocol (applicable to IPsec software and crypto card)                                               | <b>undo sa { inbound   outbound } esp encryption-hex</b>        |
| Configure both ciphering and authentication keys of ESP protocol (input in string) (applicable to IPsec software and crypto card) | <b>sa { inbound   outbound } esp string-key string-key</b>      |
| Delete the ciphering and authentication keys of ESP protocol (applicable to IPsec software and crypto card)                       | <b>undo sa { inbound   outbound } esp string-key</b>            |

By default, no key is used by any security policy.

The keys are input in two modes and those input in string mode are preferred. At both ends of the security tunnel, the keys should be input in the same mode. If the key is input at one end in string mode, but at the other end in hexadecimal mode, the security tunnel cannot be created correctly. To set a new key, the previous key must be deleted first.

### Creating a Security Policy Association with IKE

Perform the following configurations in system view.

**Table 645** Establish Security Policy Association with IKE Negotiation View

| Operation                                                                                                                | Command                                                                    |
|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Create a security policy association with IKE to enter IPsec policy view (applicable to IPsec software and crypto card). | <b>ipsec policy <i>policy-name</i><br/><i>sequence-number</i> isakmp</b>   |
| Modify the security policy established by IKE (applicable to the main software IPsec and crypto cards)                   | <b>ipsec policy <i>policy-name</i><br/><i>sequence-number</i></b>          |
| Delete the created security policy (applicable to IPsec software and crypto card)                                        | <b>undo ipsec policy <i>policy-name</i> [<br/><i>sequence-number</i> ]</b> |

By default, no security policy is created.

### Set access control list quoted by security policy

After a security policy is created, it is also necessary to specify the quoted encryption access control list item for it so as to judge which inbound/outbound communications should be encrypted and which should not.

Perform the following configurations in IPsec policy view.

**Table 646** Configure Encryption Access Control List Quoted in Security Policy

| Operation                                                                                                         | Command                                            |
|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| Configure encryption access control list quoted in security policy (applicable to IPsec software and crypto card) | <b>security acl <i>access-list-number</i></b>      |
| Cancel encryption access control list quoted in security policy (applicable to IPsec software and crypto card)    | <b>undo security acl <i>access-list-number</i></b> |

By default, no encryption access control list is quoted in the security policy.

### Set end point of security tunnel

For the security policy created with IKE negotiation view, it is unnecessary to set a local address, because IKE can obtain the local address from the interface on which this security policy is applied.

Only specify one remote address for security policy can be established by IKE. If a remote address is specified, the previous address must be deleted before specifying the new remote address.

Perform the following configurations in IPsec policy view.

**Table 647** Specify End Point of Security Tunnel

| Operation                                                                            | Command                                |
|--------------------------------------------------------------------------------------|----------------------------------------|
| Set remote address of security tunnel (applicable to IPsec software and crypto card) | <b>tunnel remote <i>ip-address</i></b> |

|                                                                                         |                                            |
|-----------------------------------------------------------------------------------------|--------------------------------------------|
| Delete remote address of security tunnel (applicable to IPSec software and crypto card) | <code>undo tunnel remote ip-address</code> |
|-----------------------------------------------------------------------------------------|--------------------------------------------|

By default, the end point of the security tunnel is not specified.

### Set the IPSec proposal quoted in security policy

Perform the following configurations in IPSec policy view.

**Table 648** Configure IPSec Proposal Quoted in Security Policy

| Operation                                                                                      | Command                                                                                |
|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Set IPSec proposal quoted in security policy (applicable to IPSec software and crypto card)    | <code>proposal proposal-name1</code><br><code>[proposal-name2...proposal-name6]</code> |
| Cancel IPSec proposal quoted in security policy (applicable to IPSec software and crypto card) | <code>undo proposal</code>                                                             |

By default, the security policy quotes no IPSec proposal.

When SA is created through IKE negotiation, a security policy can quote at most 6 IPSec proposals and IKE negotiation will search the completely matched IPSec proposal at both ends of the security tunnel. If IKE cannot find completely matched IPSec proposal, then it will not establish SA successfully, then the messages that require protection will be discarded.

The security policy determines its protocol, algorithm and encapsulation mode by quoting the IPSec proposal. A IPSec proposal must be established before it is quoted

### Set SA lifetime

There are two types of SA lifetime (or lifecycle): *time-based* and *traffic-based*. The SA becomes invalid on the first expiration of either type of lifetime. Before the SA becomes invalid, IKE establishes a new SA for IPSec negotiation, so a new SA is ready when the previous one becomes invalid. If the global lifetime is modified during the valid period of the current SA, the new one will be applied, not to the present SA but to the later SA negotiation.

The SA lifetime is only effective for an SA established with IKE, and the SA established manually does not involve the concept of lifetime.

If a security policy is not configured with lifetime value, when the router applies for a new SA, it sends a request to the remote end to set up a security tunnel negotiation and gets the SA lifetime of the remote end, and applies it as the new SA lifetime. If the local end has configured the SA lifetime when creating security policy, when it receives the application for security tunnel negotiation from the remote end, it will compare the lifetime proposed by the remote end with its own lifetime, and choose the smaller one as the SA lifetime.

SA is timeout based on the first expiration of the lifetime by seconds (specified by the key word **time-based**) or kilobytes of communication traffic (specified by the key word **traffic-based**).

The new SA should have completed the negotiation before the original SA times out, so that the new SA can be put into use as soon as the original SA expires. Soft timeout of SA occurs when a new SA is negotiated at the time when the existing SA lives for a certain percentage of lifetime defined by *seconds* (such as 90%), or when the traffic reaches a certain percentage (such as 90%) of the lifetime

defined by *kilobytes*. Hard timeout of SA means that the SA lives for the whole lifetime.

Perform the following configurations in system view.

**Table 649** Configure Global SA Lifetime

| Operation                                                                                                          | Command                                                 |
|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| Set global SA "Time-based" lifetime (applicable to IPsec software and crypto card)                                 | <b>ipsec sa global-duration time-based seconds</b>      |
| Restore the default value of the global SA (applicable to IPsec software and crypto card) "Time-based" lifetime    | <b>undo ipsec sa global-duration time-based</b>         |
| Set global SA "Traffic-based" lifetime (applicable to IPsec software and crypto card)                              | <b>ipsec sa global-duration traffic-based kilobytes</b> |
| Restore the default value of the global SA "Traffic-based" lifetime (applicable to IPsec software and crypto card) | <b>undo ipsec sa global-duration traffic-based</b>      |

By default, *time-based* lifetime is 3600 seconds (an hour),- and *traffic-based* lifetime is 1843200 kilobytes.

### Configure a separate SA lifetime

To be different from the global lifetime, SA should be configured with separate SA lifetime.

Perform the following configurations in ipsec policy view.

**Table 650** Configure Separate SA Lifetime

| Operation                                                                                        | Command                                                                  |
|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Set separate SA lifetime (applicable to IPsec software and crypto card)                          | <b>sa duration { time-based seconds   traffic-based kilobytes }</b>      |
| Restore the default value of separate SA lifetime (applicable to IPsec software and crypto card) | <b>undo sa duration { time-based seconds   traffic-based kilobytes }</b> |

By default, apply the global SA lifetime.

### Enable the detection on the reach ability of router at the remote end of the tunnel

When there are primary and backup links between two routers, and both ends adopt IKE mode to create the SA dynamically, once the primary link goes into DOWN state, the communication switches to the backup link automatically. In this case, a new SA pair (including phase 1 SA and phase 2 SA) that correspond to the backup link are created, but the original SA pair on the primary link is not deleted in time. Once the phase 2 SA on the primary link times out and is released (phase 1 SA still exists), if the primary link is restored and the communication switches back to the primary link, the phase 1 SAs saved on the local router and the remote router may be inconsistent, so that the IPsec tunnel cannot be established.

Enabling the monitoring function can ensure that the phase 1 SA can be released when the phase 2 SA is released, so that a new SA pair can be reestablished between the two routers when the primary link goes into UP state, then the IPsec tunneling can be created correctly.

Please perform the following configurations in system view.

**Table 651** Enable Detection of the Router at the Remote End of the Tunnel

| Operation                                                                                                                                             | Command                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Enable the detect on the reachability of router at the remote end of the tunnel (It is applicable to the operating system host software IPSec, NDEC)  | <code>ipsec sa dynamic-detect</code>      |
| Disable the detect on the reachability of router at the remote end of the tunnel (It is applicable to the operating system host software IPSec, NDEC) | <code>undo ipsec sa dynamic-detect</code> |

By default, detection of the router at the remote end of the tunnel is disabled.

**Apply Security Policy Group on Interface**

To put the defined SA into effect, it is necessary to apply a security policy to each interface (logical or physical) that will encrypt site-out data and decrypt site-in data. According to the encryption set configured on the interface, the interface cooperates with the remote encryption router to perform the packet encryption. When the security policy group is deleted from the interface, this interface will not have IPSec security protection function.

When messages are transmitted on an interface, the security policies in the security policy group are searched one by one, from the smaller sequence number to the greater one. If a message is matched with an access list quoted by a security policy, then this security policy is used for processing this message. If a message has no matched access list quoted by a security policy, then it will go on looking for next security policy. If a message is matched with no access list quoted by the security policy, then the message will be directly transmitted (IPSec will not protect the message).

One interface can be applied with only one security policy group, and one security policy group can be applied to only one interface.

Perform the following configurations in the interface view.

**Table 652** Apply Security Policy Group on Interface

| Operation                                                                                            | Command                               |
|------------------------------------------------------------------------------------------------------|---------------------------------------|
| Apply security policy group on interface (applicable to IPSec software and crypto card)              | <code>ipsec policy policy-name</code> |
| Delete the security policy group applied on interface (applicable to IPSec software and crypto card) | <code>undo ipsec policy</code>        |

By default, no security policy group is applied to the interface.

**Table 653** Display and Debug IPsec

| Operation                                                                                | Command                                                                    |
|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Display all created SA (applicable to IPsec software)                                    | <code>display ipsec sa all</code>                                          |
| Display all SA information briefly (applicable to IPsec software)                        | <code>display ipsec sa brief</code>                                        |
| Display the specific SA information (applicable to IPsec software)                       | <code>display ipsec sa parameters<br/>dest-address protocol spi</code>     |
| Display global SA lifetime (applicable to IPsec software)                                | <code>display ipsec sa duration</code>                                     |
| Display SA established with specific peer ends (applicable to IPsec software)            | <code>display ipsec sa remote ip-address</code>                            |
| Display all security policy base information (applicable to IPsec software)              | <code>display ipsec sa policy policy-name [<br/>sequence-number ]</code>   |
| Display statistic information related to security message (applicable to IPsec software) | <code>display ipsec statistics</code>                                      |
| Display configured IPsec proposal (applicable to IPsec software)                         | <code>display ipsec proposal [<br/>proposal-name ]</code>                  |
| Display all security policy base information (applicable to IPsec software)              | <code>display ipsec policy all</code>                                      |
| Display brief security policy base information (applicable to IPsec software)            | <code>display ipsec policy brief</code>                                    |
| Display all security policy base information by name (applicable to IPsec software)      | <code>display ipsec policy name policy-name<br/>[ sequence-number ]</code> |
| Clear all SA (applicable to IPsec software)                                              | <code>reset ipsec sa all</code>                                            |
| Clear specific SA information (applicable to IPsec software)                             | <code>reset ipsec sa parameters<br/>dest-address protocol spi</code>       |
| Clear SA of the specified security policy base (applicable to IPsec software)            | <code>reset ipsec sa policy policy-name [<br/>sequence-number ]</code>     |
| Clear SA established with specified peer ends (applicable to IPsec software)             | <code>reset ipsec sa remote ip-address</code>                              |
| Clear statistic information related to security messages (applicable to IPsec software)  | <code>reset ipsec statistics</code>                                        |
| information debugging related to IPsec (applicable to IPsec software)                    | <code>debugging ipsec { sa   packet   misc }</code>                        |

### Displaying and Debugging the NDEC Card

#### Resetting the crypto card

When the crypto card operates abnormally, resetting the crypto card can be used to restore the crypto card to normality. When resetting the crypto card, the crypto card restores its initialization. At the same time, the host retransmits the card's configured information and SA information being used to the crypto card. In addition, the host automatically resets the crypto card when it finds that the crypto card operates abnormally.

Configure the following in the system view:

**Table 654** Reset crypto card

| Operation                                     | Command                                     |
|-----------------------------------------------|---------------------------------------------|
| Reset crypto card (applicable to crypto card) | <code>encrypt-card reset [ slot-id ]</code> |

## Displaying and Debugging the crypto card

Use the **debugging**, **reset** and **display** command in all views.

**Table 655** Display and Debug NDEC Card

| Operation                                                                                                           | Command                                                                                        |
|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Display the detailed information of crypto cards (applicable to crypto cards)                                       | <code>display encrypt-card details [ slot-id ]</code>                                          |
| Display all established Security Association on crypto card (applicable to crypto card)                             | <code>display encrypt-card ipsec sa all [ slot-id ]</code>                                     |
| Display a specified Security Association on crypto card (applicable to crypto card)                                 | <code>display encrypt-card ipsec sa parameters remote-address protocol spi-number</code>       |
| Display statistical information of the security packets processing on crypto card (applicable to crypto card)       | <code>display encrypt-card statistic [ slot-id ]</code>                                        |
| Display current operating status of crypto card (applicable to crypto card)                                         | <code>display encrypt-card status [ slot-id ]</code>                                           |
| Display current operating logging of crypto card (applicable to crypto card)                                        | <code>display encrypt-card syslog [ slot-id ]</code>                                           |
| Display version number of crypto card (applicable to crypto card)                                                   | <code>display encrypt-card version [ slot-id ]</code>                                          |
| Delete all established Security Association (applicable to crypto card)                                             | <code>reset encrypt-card sa all [ slot-id ]</code>                                             |
| Delete the specified Security Association on crypto card (applicable to crypto card)                                | <code>reset encrypt-card sa parameters remote-address protocol spi-number</code>               |
| Clear the statistical information of security packets on crypto card (applicable to crypto card)                    | <code>reset encrypt-card statistic [ slot-id ]</code>                                          |
| Clear all the logging information on the crypto card (applicable to crypto cards)                                   | <code>reset encrypt-card syslog [ slot-id ]</code>                                             |
| Enable the debugging of information, packets, SA, command, error and other information (applicable to crypto cards) | <code>debugging encrypt-card { all   packet   sa   command   error   misc } [ slot-id ]</code> |
| Enable the debugging of the main software on the crypto card (applicable to crypto cards)                           | <code>debugging encrypt-card host { all   packet   sa   command   error   misc }</code>        |

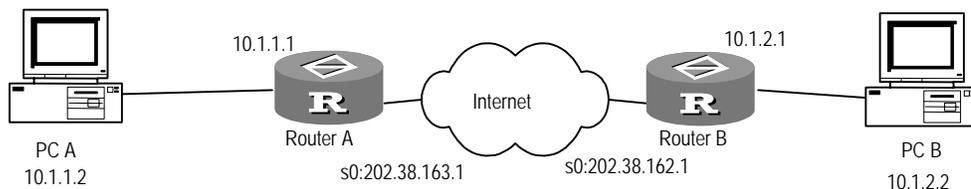
### IPSec Configuration Example

The following sections demonstrate the following IPSec configurations:

- Creating an SA Manually
- Creating an SA in IKE Negotiation Mode
- Encrypting, Decrypting, and Authenticating NDEC Cards

### Creating an SA Manually

Establish a security tunnel between Router-A and Router-B to perform security protection for the data streams between PC-A represented subnet (10.1.1.x) and PC-B represented subnet (10.1.2.x). The security protocol adopts ESP protocol, algorithm adopts DES, and authentication algorithm adopts sha1-hmac-96.

**Figure 174** Networking diagram of manually creating SA

Prior to the configuration, you should ensure that Router A and Router B can interwork at the network layer through a serial interface.

### 1 Configure Router A:

- a Configure an access list and define the data stream from Subnet 10.1.1x to Subnet 10.1.2x.

```
[RouterA] acl 101 permit
[RouterA-acl-101] rule permit ip source 10.1.1.0 0.0.0.255
destination 10.1.2.0 0.0.0.255
[RouterA-acl-101] rule deny ip source any destination any
```

- b Create the IPsec proposal view named tran1

```
[RouterA] ipsec proposal tran1
```

- c Adopt tunnel mode as the message-encapsulating form

```
[RouterA-ipsec-proposal-tran1] encapsulation-mode tunnel
```

- d Adopt ESP protocol as security protocol

```
[RouterA-ipsec-proposal-tran1] transform esp-new
```

- e Select authentication algorithm and encryption algorithm

```
[RouterA-ipsec-proposal-tran1] esp-new encryption-algorithm des
[RouterA-ipsec-proposal-tran1] esp-new authentication-algorithm
sha1-hmac-96
```

- f Create a security policy with negotiation view as manual

```
[RouterA] ipsec policy policy1 10 manual
```

- g Quote access list

```
[RouterA-ipsec-policy-policy1-10] security acl 101
```

- h Quote IPsec proposal

```
[RouterA-ipsec-policy-policy1-10] proposal tran1
```

- i Set local and remote addresses

```
[RouterA-ipsec-policy-policy1-10] tunnel local 202.38.163.1
[RouterA-ipsec-policy-policy1-10] tunnel remote 202.38.162.1
```

- j Set SPI

```
[RouterA-ipsec-policy-policy1-10] sa outbound esp spi 12345
[RouterA-ipsec-policy-policy1-10] sa inbound esp spi 54321
```

- k Set session key

```
[RouterA-ipsec-policy-policy1-10] sa outbound esp string-key abcdefg
[RouterA-ipsec-policy-policy1-10] sa inbound esp string-key gfedcba
```

**l** Apply security policy group on serial interface

```
[RouterA] interface serial 0
[RouterA-Serial0] ipsec policy policy1
[RouterA-Serial0] ip address 202.38.163.1 255.255.255.0
```

**m** Configure the route.

```
[RouterA] ip route-static 10.1.2.0 255.255.255.0 202.38.162.1
```

**2** Configure Router B:**a** Configure an access list and define the data stream from Subnet 10.1.2x to Subnet 10.1.1x.

```
[RouterB] acl 101
[RouterB-acl-101] rule permit ip source 10.1.2.0 0.0.0.255
destination 10.1.1.0 0.0.0.255
[RouterB-acl-101] rule deny ip source any destination any
```

**b** Create the IPSec proposal view named tran1

```
[RouterB] ipsec proposal tran1
```

**c** Adopt tunnel mode as the message-encapsulating form

```
[RouterB-ipsec-proposal-tran1] encapsulation-mode tunnel
```

**d** Adopt ESP protocol as security protocol

```
[RouterB-ipsec-proposal-tran1] transform esp-new
```

**e** Select authentication algorithm and encryption algorithm

```
[RouterB-ipsec-proposal-tran1] esp-new encryption-algorithm des
[RouterB-ipsec-proposal-tran1] esp-new authentication-algorithm
sha1-hmac-96
```

**f** Create a security policy with negotiation mode as manual

```
[RouterB] ipsec policy use1 10 manual
```

**g** Quote access list

```
[RouterB-ipsec-policy-use1-10] security acl 101
```

**h** Quote IPSec proposal

```
[RouterB-ipsec-policy-use1-10] proposal tran1
```

**i** Set local and remote addresses

```
[RouterB-ipsec-policy-use1-10] tunnel local 202.38.162.1
[RouterB-ipsec-policy-use1-10] tunnel remote 202.38.163.1
```

**j** Set SPI

```
[RouterB-ipsec-policy-use1-10] sa outbound esp spi 54321
[RouterB-ipsec-policy-use1-10] sa inbound esp spi 12345
```

**k** Set session key

```
[RouterB-ipsec-policy-use1-10] sa outbound esp string-key gfedcba
[RouterB-ipsec-policy-use1-10] sa inbound esp string-key abcdefg
```

**l** Exit to system view

```
[RouterB-ipsec-policy-use1-10] quit
```

**m** Enter serial interface view

```
[RouterB] interface serial 0
```

**n** Apply security policy group on serial interface

```
[RouterB-Serial0] ipsec policy usel
[RouterB-Serial0] ip address 202.38.162.1 255.255.255.0
```

- o Configure the route.

```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
```

After the configuration is complete and the security tunnel between Router A and Router B is established, the data stream between Subnet 10.1.1.x and Subnet 10.1.2.x will be transmitted with encryption.

### Creating an SA in IKE Negotiation Mode

Establish a security tunnel between Router A and Router B to perform security protection for the data streams between PC-A represented subnet (10.1.1.x) and PC-B represented subnet (10.1.2.x). The security protocol adopts ESP protocol, algorithm adopts DES, and authentication algorithm adopts sha1-hmac-96. See Figure 174 for an illustration of the configuration.

Prior to configuring, you should ensure that Router A and Router B can interwork at the network layer through a serial interface.

#### 1 Configure Router A:

- a Configure an access list and define the data stream from Subnet 10.1.1x to Subnet 10.1.2x.

```
[RouterA] acl 101
[RouterA-acl-101] rule permit ip source 10.1.1.0 0.0.0.255
destination 10.1.2.0 0.0.0.255
[RouterA-acl-101] rule deny ip source any destination any
```

- b Create the IPSec proposal view named tran1

```
[RouterA] ipsec proposal tran1
```

- c Adopt tunnel mode as the message-encapsulating form

```
[RouterA-ipsec-proposal-tran1] encapsulation-mode tunnel
```

- d Adopt ESP protocol as security protocol

```
[RouterA-ipsec-proposal-tran1] transform esp-new
```

- e Select authentication algorithm and encryption algorithm

```
[RouterA-ipsec-proposal-tran1] esp-new encryption-algorithm des
[RouterA-ipsec-proposal-tran1] esp-new authentication-algorithm
sha1-hmac-96
```

- f Create a security policy with negotiation mode as isakmp

```
[RouterA] ipsec policy policy1 10 isakmp
```

- g Set remote addresses

```
[RouterA-ipsec-policy-policy1-10] tunnel remote 202.38.162.1
```

- h Quote IPSec proposal

```
[RouterA-ipsec-policy-policy1-10] proposal tran1
```

- i Quote access list

```
[RouterA-ipsec-policy-policy1-10] security acl 101
```

- j Exit to system view

```
[RouterA-ipsec-policy-policy1-10] quit
```

- k Enter serial interface view

```
[RouterA] interface serial 0
l Configure ip address of the serial interface
[RouterA-Serial0] ip address 202.38.163.1 255.255.255.0
m Apply security policy group on serial interface
[RouterA-Serial0] ipsec policy policy1
n Configure the route.
[RouterA] ip route-static 10.1.2.0 255.255.255.0 202.38.162.1
o Configure corresponding IKE
[RouterA] ike pre-shared-key abcde remote 202.38.162.1
```

## 2 Configure Router B:

- a Configure an access list and define the data stream from Subnet 10.1.2x to Subnet 10.1.1x.

```
[RouterB] acl 101
[RouterB-acl-101] rule permit ip source 10.1.2.0 0.0.0.255
destination 10.1.1.0 0.0.0.255
[RouterB-acl-101] rule deny ip source any destination any
```

- b Create the IPSec proposal view named tran1

```
[RouterB] ipsec proposal tran1
```

- c Adopt tunnel mode as the message-encapsulating form

```
[RouterB-ipsec-proposal-tran1] encapsulation-mode tunnel
```

- d Adopt ESP protocol as security protocol

```
[RouterB-ipsec-proposal-tran1] transform esp-new
```

- e Select authentication algorithm and encryption algorithm

```
[RouterB-ipsec-proposal-tran1] esp-new encryption-algorithm des
[RouterB-ipsec-proposal-tran1] esp-new authentication-algorithm
sha1-hmac-96
```

- f Create a security policy with negotiation view as isakmp

```
[RouterB] ipsec policy use1 10 isakmp
```

- g Quote access list

```
[RouterB-crypto-map-use1-10] match address 101
```

- h Set remote address

```
[RouterB-ipsec-policy-policy1-10] security acl 101
```

- i Quote IPSec proposal

```
[RouterB-ipsec-policy-policy1-10] proposal tran1
```

- j Configure serial interface Serial0

```
[RouterB] interface serial 0
[RouterB-Serial0] ip address 202.38.162.1 255.255.255.0
```

- k Apply security policy group on serial interface

```
[RouterB-Serial0] ipsec policy use1
```

- l Configure the route.

```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
```

**m** Configure corresponding IKE

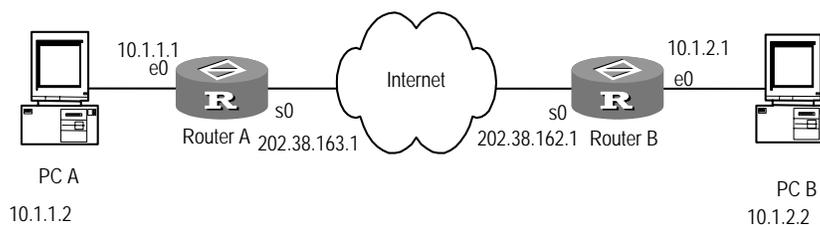
```
[RouterB] ike pre-shared-key abcde remote 202.38.163.1
```

After the above configurations are completed, if the messages between Subnet 10.1.1.x and Subnet 10.1.2.x transmits between Router-A and Router-B, IKE will be triggered to negotiate to establish SA. After IKE negotiates successfully and SA is established, the data stream between Subnet 10.1.1.x and Subnet 10.1.2.x will be transmitted with encryption.

### Encrypting, Decrypting, and Authenticating NDEC Cards

Establish a security tunnel between Router A and Router B to conduct security protection to data stream between subnet (10.1.1.x) represented by PC A and subnet (10.1.2.x) represented by PC B. It is to establish security association with manual method. The security protocol adopts ESP protocol, and the encryption algorithm adopts DES, and the authentication algorithm adopts sha1-hmac-96.

**Figure 175** Establish networking diagram of security tunnel using crypto cards

**1** Configure Router A

- a** Configure an access list and define a data stream from subnet 10.1.1.x to subnet 10.1.1.2.x.

```
[RouterA] acl 101 permit
[RouterA-acl-101] rule permit ip source 10.1.1.0 0.0.0.255
destination 10.1.2.0 0.0.0.255
[RouterA-acl-101] rule deny ip source any destination any
```

- b** Establish proposal view of crypto card in the name of tran1.

```
[RouterA] crypto ipsec card-proposal tran1
```

- c** Adopt tunnel module for packets encapsulation form.

```
[RouterA-ipsec-card-proposal-tran1] encapsulation-mode tunnel
```

- d** Adopt ESP protocol for security protocol

```
[RouterA-ipsec-card-proposal-tran1] transform esp-new
```

- e** Select algorithm

```
[RouterA-ipsec-card-proposal-tran1] esp-new encryption-algorithm des
[RouterA-ipsec-card-proposal-tran1] esp-new authentication-algorithm
sha1-hmac-96
```

- f** Return to system view.

```
[RouterA-ipsec-card-proposal-tran1] quit
```

- g** Establish a security policy with manual negotiation mode.

```
[RouterA] ipsec policy policy1 10 manual
```

- h** Quote access list.

```
[RouterA-ipsec-policy-policy1-10] security acl 101
i Set remote address.
[RouterA-ipsec-policy-policy1-10] tunnel remote 202.38.162.1
j Set local address.
[RouterA-ipsec-policy-policy1-10] tunnel local 202.38.163.1
k Quote IPSec proposal.
[RouterA-ipsec-policy-policy1-10] proposal tran1
l Set SPI.
[RouterA-ipsec-policy-policy1-10] sa outbound esp spi 12345
[RouterA-ipsec-policy-policy1-10] sa inbound esp spi 54321
m Set encryption key.
[RouterA-ipsec-policy-policy1-10] sa outbound esp string-key abcdefg
[RouterA-ipsec-policy-policy1-10] sa inbound esp string-key gfedcba
n Return to system view.
[RouterA-ipsec-policy-policy1-10] quit
o Enter Ethernet interface view and configure IP address.
[RouterA-Ethernet0] ip address 10.1.1.1 255.255.255.0
[RouterA-Ethernet0] quit
p Enter serial port configuration mode and configure IP address.
[RouterA] interface serial 0
[RouterA-Serial0] ip address 202.38.163.1 255.255.255.0
q Return to system view and configure the static routing to network segment
10.1.2.x.
[RouterA-Serial0] quit
[RouterA] ip route-static 10.1.2.0 255.255.255.0 202.38.162.1
r Apply security policy base on serial port.
[RouterA-Serial0] ipsec policy policy1
```

## 2 Configure Router B

- a Configure an access list and define a data stream from subnet 10.1.2.x to subnet 10.1.1.x.

```
[RouterB] acl 100
[RouterB-acl-100] rule permit ip source 10.1.2.0 0.0.0.255
destination 10.1.1.0 0.0.0.255
[RouterB-acl-100] rule deny ip source any destination any
```

- b Establish IPSec proposal in the name of tran1.

```
[RouterB] ipsec card-proposal tran1
```

- c Adopt tunnel module for packets encapsulation.

```
[RouterB-ipsec-card-proposal-tran1] encapsulation-mode tunnel
```

- d Adopt ESP protocol for security protocol.

```
[RouterB-ipsec-card-proposal-tran1] transform esp-new
```

- e Select algorithm.

```
[RouterB-ipsec-card-proposal-tran1] esp-new encryption-algorithm des
```

```
[RouterB-ipsec-card-proposal-tran1] esp-new authentication-algorithm
sha1-hmac-96
```

**f** Return to system view.

```
[RouterB-ipsec-card-proposal-tran1] quit
```

**g** Establish a security policy with manual configuration mode.

```
[RouterB] ipsec policy map1 10 manual
```

**h** Quote access list.

```
[RouterB-ipsec-policy-map1-10] security acl 100
```

**i** Set remote address.

```
[RouterB-ipsec-policy-map1-10] tunnel remote 202.38.163.1
```

**j** Set local address.

```
[RouterB-ipsec-policy-map1-10] tunnel local 202.38.162.1
```

**k** Quote IPSec proposal.

```
[RouterB-ipsec-policy-map1-10] proposal tran1
```

**l** Set SPI.

```
[RouterB-ipsec-policy-map1-10] sa outbound esp spi 54321
```

```
[RouterB-ipsec-policy-map1-10] sa inbound esp spi 12345
```

**m** Set encryption key.

```
[RouterB-ipsec-policy-map1-10] sa outbound esp string-key gfedcba
```

```
[RouterB-ipsec-policy-map1-10] sa inbound esp string-key abcdefg
```

**n** Return to the system view.

```
[RouterB-ipsec-policy-map1-10] quit
```

**o** Enter Ethernet port configuration mode and configure IP address.

```
[RouterB-Ethernet0] ip address 10.1.2.1 255.255.255.0
```

```
[RouterB-Ethernet0] quit
```

**p** Enter serial port configuration mode and configure IP address.

```
[RouterB] interface serial 0
```

```
[RouterB-Serial0] ip address 202.38.162.1 255.255.255.0
```

**q** Return to system view and configure static routing to network segment 10.1.1.x.

```
[RouterB-Serial0] quit
```

```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
```

**r** Apply security policy base on serial port.

```
[RouterB-Serial0] ipsec policy map1
```

---

## Troubleshooting IPsec NDEC card cannot be configured.

When configuring relevant commands of crypto card, the following message displays: *No valid encrypt-card.*

Do the following:

- Display the plugging conditions of the crypto card to check whether the crypto card was plugged in correctly. Under normal condition, the “run” indicator of the crypto card will blink normally (one second on, one second off).
- Use the **display encrypt-card version** command to check the crypto card status. It shall display the card and version condition of the crypto card under normal conditions. If nothing displayed, it means that the host does not detect the crypto card. The crypto card may be enabled (“run” indicator blinks quickly). If 5 seconds later the crypto card is still enabled, the router may be restarted (it must be noted that the configuration of the router must be saved first).

### **Routers cannot ping through each other after IPSec configuration**

Do the following:

- Check whether security policy was applied on the interface. Use the **display current-configuration interface** command to check whether it is configured policy on the interface. It shall display configuration policy under normal condition. If no policy is configured, map shall be configured under interface view.
- Check the matching of the security policy. If the security policy map was established manually, the local and remote address of the security association must be correct and the parameters of security association must be identified. After changing the parameters of security association, it is necessary to delete the security policy map and then to re-apply security policy map.
- Check the identity of the security protocol. For security policy established manually, the security protocol selected by the IPSec proposal of the both ends of the router shall be the same.
- Check Access Control List. If no problem was found through above check procedure, or the problem is not eliminated after correcting the above checkup, the access control list may be checked. Check whether the access control list allows both interconnection parties to pass.
- Check the hardware link. If the problem cannot be eliminated through above methods, please check whether the hardware link is normal or not.



This chapter covers the following topics:

- IKE Protocol Overview
- Configuring IKE
- Displaying and Debugging IKE
- IKE Configuration Example
- Troubleshooting IKE

---

### **IKE Protocol Overview**

The Internet Key Exchange (IKE) protocol, implements hybrid protocols of both Oakley and SKEME key exchanges in an ISAKMP network. This protocol defines standards for automatically authenticating IPSec peer end, negotiating security service and generating shared key, and provide services such as automatic key exchange negotiation and security association creation, thus simplifying the use and management of IPSec.

IKE has a set of self-protection mechanism, which enables to securely deliver keys, authenticate ID and establish IPSec secure association in insecure network.

After establishing security association by both parties of the security association, if the peer party is invalid and cannot operate normally (such as shut-off), the local party has no way to know about it. When the peer party restarts the machine, because there is a security association locally, the negotiation cannot be initiated, or only initiated by the peer party, or negotiated after timeout. Thus, the keepalive function of IKE will detect and delete the idle security association when the peer party was invalid and cannot operate normally.

IKE uses ISAKMP at two stages:

- The first stage is to negotiate to create a communication channel and authenticate it, as well as to provide confidentiality, message integrity and message source authentication services for further IKE communication between both parties.
- The second stage is to use the created IKE SA to create IPSec SA.

The following figure shows the relationship between IKE and IPSec.



- Hashing algorithm: SHA-1(HMAC anamorphosis) or MD5 (HMAC anamorphosis) algorithm
- Authentication method: RSA signature or RSA real-time encryption
- Diffie-Hellman group ID
- SA lifetime

To negotiate the IKE policies used by two ends, the initiator sends all the IKE policies to the peer to negotiate the public IKE policy used by both sides. The remote terminal will match the received policy with all of its IKE policies as per the precedence order. The one of highest precedence will be first judged. If one IKE policy is found to have the same encryption, hash, authentication and Diffie-Hellman parameters with the received IKE policy, and its life cycle is equal to or longer than that specified by the received IKE policy, then the common IKE policy at both ends can be determined. (Note that if no life cycle is specified for the IKE policy, the relatively short policy life cycle of the remote terminal will be selected.) Then, IPsec security path will be created by using the IKE policy to protect the following data. Otherwise, IKE refuses negotiation, and will not create IPsec security path.

The following issues should be decided before configuring IKE:

- Determine the intensity of the authentication algorithm, encryption algorithm and Diffie-Hellman algorithm (the calculation resources consumed and the security capability provided). Different algorithms are of different intensities, and the higher the algorithm intensity is, the more difficult it is to decode the protected data, but the more resources are consumed. The longer key usually has higher algorithm intensity.
- Determine the security protection intensity needed in IKE exchange (including hashing algorithm, encryption algorithm, ID authentication algorithm and DH algorithm).
- Determine the authentication algorithm, encryption algorithm, hashing algorithm and Diffie-Hellman group.
- Determine the pre-shared key of both parties.
- Create IKE policy

The user can create multiple IKE policies, but must allocate a unique priority value for each created policy. Both parties in negotiation must have at least one matched policy for successfully negotiation, that is to say, a policy and the one in the remote terminal must have the same encryption, hashing, authentication and Diffie-Hellman parameters (the lifetime parameters may be a little different). If it is found that there are multiple matching policies after negotiation, the matching policy with higher priority will be matched first.

Perform the following configurations in system view.

**Table 656** Create IKE Policy

| Operation                                     | Command                                       |
|-----------------------------------------------|-----------------------------------------------|
| Create IKE policy and enter IKE proposal view | <b>ike proposal <i>policy-number</i></b>      |
| Delete IKE policy                             | <b>undo ike proposal <i>policy-number</i></b> |

The system creates only the default IKE security policy that cannot be deleted or modified by users.

### Selecting an Encryption Algorithm

The two types of encryption algorithms that are supported are the 56-bit DES-Cipher Block Chaining (DES-CBC) algorithm and the 168-bit 3DES-CBC algorithm. Before being encrypted, each plain text block performs exclusive-OR operation with an encryption block, thus the same plain text block never maps the same encryption and the security is enhanced.

Perform the following configurations in IKE proposal view.

**Table 657** Select Encryption Algorithm

| Operation                                         | Command                                            |
|---------------------------------------------------|----------------------------------------------------|
| Select encryption algorithm                       | <b>encryption-algorithm { des-cbc   3des-cbc }</b> |
| Set the encryption algorithm to the default value | <b>undo encryption-algorithm</b>                   |

By default, DES-CBC encryption algorithm (i.e. parameter **des-cbc**) is adopted.

### Selecting an Authentication Algorithm

Pre-share key is the only supported authentication algorithm.

Perform the following configurations in IKE proposal view.

**Table 658** Select Authentication Method

| Operation                                              | Command                                     |
|--------------------------------------------------------|---------------------------------------------|
| Select authentication method                           | <b>authentication-method pre-share</b>      |
| Restore the authentication method to the default value | <b>undo authentication-method pre-share</b> |

By default, pre share key (i.e., **pre-share**) algorithm is adopted.

### Configuring Pre-shared Key

If pre-shared key authentication method is selected, it is necessary to configure pre-shared key.

Perform the following configurations in system view.

**Table 659** Configure Pre-shared Key

| Operation                                          | Command                                                  |
|----------------------------------------------------|----------------------------------------------------------|
| Configure pre-shared key                           | <b>ike pre-shared-key key remote remote-address</b>      |
| Delete pre-shared key to restore its default value | <b>undo ike pre-shared-key key remote remote-address</b> |

By default, both ends of the security channel have no pre-shared keys.

### Selecting the Hashing Algorithm

Hashing algorithms use HMAC framework to achieve its function. HMAC algorithm adopts an encryption hashing function to authenticate messages, providing frameworks to insert various hashing algorithms, such as SHA-1 and MD5.

There are two hashing algorithm options: SHA-1 and MD5. Both algorithms provide data source authentication and integrity protection mechanism. Compared with MD5, SHA-1 contained more summary information, and is more secure, but the authentication speed is relatively slow. A kind of attack subject to MD5 can be successful, though difficult, but HMAC anamorphous used by IKE can stop such attacks.

Perform the following configurations in IKE proposal view.

**Table 660** Select Hashing Algorithm

| Operation                                  | Command                                       |
|--------------------------------------------|-----------------------------------------------|
| Select hashing algorithm                   | <b>authentication-algorithm { md5   sha }</b> |
| Set hashing algorithm to the default value | <b>undo authentication-algorithm</b>          |

By default SHA-1 hashing algorithm (i.e., parameter **sha**) is adopted.

### Selecting DH Group ID

There are two DH (Diffie-Hellman) group ID options: 768-bit Diffie-Hellman group (Group 1) or 1024-bit Diffie-Hellman group (Group 2). The 1024-bit Diffie-Hellman group (Group 2) takes longer CPU time

Perform the following configurations in IKE proposal view.

**Table 661** Select DH Group ID

| Operation                                | Command                       |
|------------------------------------------|-------------------------------|
| Select DH group ID                       | <b>dh { group1   group2 }</b> |
| Restore the default value of DH group ID | <b>undo dh</b>                |

By default, 768-bit Diffie-Hellman group is selected.

### Setting the Lifetime of IKE Association SA

Lifetime means how long IKE exists before it becomes invalid. When IKE begins negotiation, it must first make its security parameters of the two parties be consistent. SA quotes the consistent parameters at each terminal, and each terminal keeps SA until its lifetime expires. Before SA becomes invalid, the sequent IKE negotiation can use it again. The new SA is negotiated before the current SA becomes invalid.

IKE negotiation can be set with a relatively short life cycle for the purpose of improving IKE negotiation security. There is a critical IKE life cycle value. If the policy lifetimes of the two terminals are different, that of the originating party will be taken as the lifetime of the IKE SA.

If the policy lifetimes of two terminals are different, only when the lifetime of originating terminals is reater than or equal to that of the peer end can the IKE policy be selected, and the shorter lifetime selected as IKE SA lifetime.

Perform the following configurations in IKE proposal view.

**Table 662** Set Lifetime of IKE Negotiation SA

| Operation                         | Command                    |
|-----------------------------------|----------------------------|
| Set lifetime of IKE SA            | <b>sa duration seconds</b> |
| Set lifetime as the default value | <b>undo sa duration</b>    |

By default, SA lifetime is 86400 seconds (a day). It is recommended that the configured *seconds* should be greater than 10 minutes.

### Configuring IKE Keepalive Timer

The Keepalive function detects and deletes idle security association when the peer party is invalid and cannot operate. Usually, the initiator transmits a packet proving itself still alive to the peer party, while the responder confirms that the peer party is still alive after receiving it. The keepalive function includes two timers, interval and timeout.

- The interval timer mainly assists in transmitting keepalive packets to the peer party, following a set time interval, to prove that it is still alive.
- The timeout timer mainly assists timing events to query the status of security tunnel periodically, and deletes the timed out security tunnel.

Configure the following in system view.

**Table 663** Configure IKE Keepalive Timer

| Operation                                                                | Command                                        |
|--------------------------------------------------------------------------|------------------------------------------------|
| Configure transmitting time interval of IKE keepalive packets (interval) | <b>ike sa keepalive-timer interval seconds</b> |
| Delete interval timing event of IKE keepalive function                   | <b>undo ike sa keepalive-timer interval</b>    |
| Configure IKE keepalive link timeout time (timeout)                      | <b>ike sa keepalive-timer timeout seconds</b>  |
| Delete timeout timing event of IKE keepalive function                    | <b>undo ike sa keepalive-timer timeout</b>     |

By default, the system does not enable IKE keepalive timing (interval and timeout) event.

Usually, the interval and timeout timers are applied in pairs at the initiator side or the receiver side. If an interval timer is configured at one side, the other side should be configured with a timeout timer. In the actual application, if one side is configured with the timeout timer, the other side must be configured with the interval timer or the SA will be deleted. If one side is configured with the interval timer, it is not necessary to configure the timeout timer at the other side. To avoid the negative influence of network congestion on the keepalive function, you should set the value of the timeout timer three times higher than that of the interval timer.

### Displaying and Debugging IKE

Use **debugging**, **reset** and **display** commands in all views.

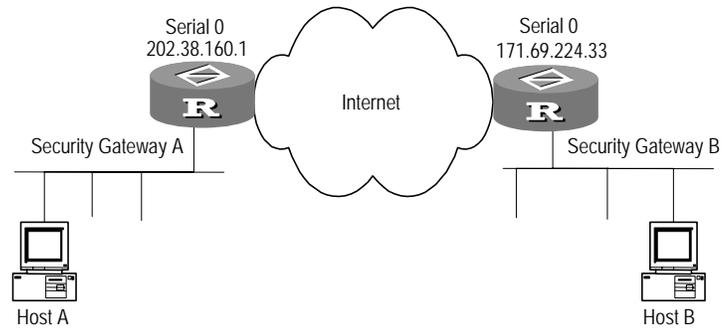
**Table 664** Display and Debug IKE

| Operation                                      | Command                                                                                     |
|------------------------------------------------|---------------------------------------------------------------------------------------------|
| Display IKE security association parameter     | <b>display ike sa</b>                                                                       |
| Display IKE security policy                    | <b>display ike proposal</b>                                                                 |
| Delete the security channel established by IKE | <b>reset ike sa { connection-ike-sa-id   all }</b>                                          |
| Clear an SA                                    | <b>debugging ike { all   crypto   error   message   misc   sysdep   timer   transport }</b> |

## IKE Configuration Example

- Hosts A and B communicates securely, and a security channel is established with IKE automatic negotiation between security gateways A and B.
- Configure an IKE policy on Gateway A, with Policy 10 is of highest priority and the default IKE policy is of the lowest priority.
- Pre-shared key authentication algorithm is adopted.

**Figure 177** Networking diagram of IKE configuration example



### 1 Configure Security Gateway A.

#### a Configure a IKE Policy 10

```
[RouterA] ike proposal 10
```

#### b Specify the hashing algorithm used by IKE policy as MD5

```
[RouterA-ike-proposal-10] authentication-algorithm md5
```

#### c Use pre-shared key authentication method

```
[RouterA-ike-proposal-10] authentication-method pre-share
```

#### d Configure "abcde" for peer 171.69.224.33

```
[RouterA] ike pre-share-key abcde remote 171.69.224.33
```

#### e Configure IKE SA lifetime to 5000 seconds

```
[RouterA-ike-proposal-10] sa duration 5000
```

### 2 Configure Security Gateway B.

#### a Use default IKE policy on Gateway B and configure the peer authentication word.

```
[RouterB] ike pre-share-key abcde remote 202.38.160.1
```

These steps configure IKE negotiation. To establish an IPSec security channel for secure communication, it is necessary to configure IPSec correspondingly. For detailed contents, see the configuration examples in *IPSec Configuration*.

## Troubleshooting IKE

When configuring parameters to establish IPSec security channel, you can use the `debugging ike error` command to enable error debugging of IKE.

### Invalid user ID information

User ID information is the data for the user originating IPSec communication to identify itself. In practical applications user ID establishes a different security path

for protecting different data streams. At present, we use the user IP address to identify the user.

```
got NOTIFY of type INVALID_ID_INFORMATION
```

or

```
drop message from X.X.X.X due to notification type
INVALID_ID_INFORMATION
```

Check whether ACL contents in **ipsec policy** configured at interfaces of both ends are compatible. It is recommended for the user to configure ACL of both ends to mirror each other.

### Unmatched policy

Enable the **debugging ike error** command to see the debugging information.

```
got NOTIFY of type NO_PROPOSAL_CHOSEN
```

or

```
drop message from X.X.X.X due to notification type
NO_PROPOSAL_CHOSEN
```

Both parties of negotiation have no matched policy. Check the protocol used by **ipsec policy** configured on interfaces of both parties to see whether the encryption algorithm and authentication algorithm are the same.

### Unable to establish security channel

Follow these steps:

- Check whether the state of network is stable and whether the security channel has been properly established. You may encounter the situation as follows: the two parties cannot communicate via the existing security channel, while the access control list of two parties have been properly configured and there is a matching policy. This case is generally due to a party restarting the router after establishing the security channel.
- 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 show 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.

# IX

## VPN

Chapter 42    Configuring VPN

Chapter 43    Configuring L2TP

Chapter 44    Configuring GRE



This chapter covers the following topics:

- VPN Overview
- Basic Networking Applications of VPN
- Classification of IP VPN

---

### VPN Overview

VPN establishes private networks on public networks by creating a “virtual”, or logical network from resources of the existing network. Carriers can make use of their spare network resources to provide VPN service and profit from the network resources to the maximum extent. In addition:

- VPNs are used by enterprises or user groups to securely access remote networks. From the perspective of VPN users, it makes no difference whether they use VPN service or traditional private networks. Being a private network, VPN keeps its resources independent from those of the carrying network and the resources of a VPN cannot be used by other VPNs on the same carrying network or by network users who do not belong to the VPN. The VPN is safe enough to make sure that the internal information within a VPN is free from being invaded by external users.
- VPN technology is more complicated than the mechanisms of various ordinary point-to-point applications. Network interconnection between the users of private networks is required for VPN service, including the creation of VPN internal network topology, route calculation, adding and deleting of members.

The advantages of VPN include:

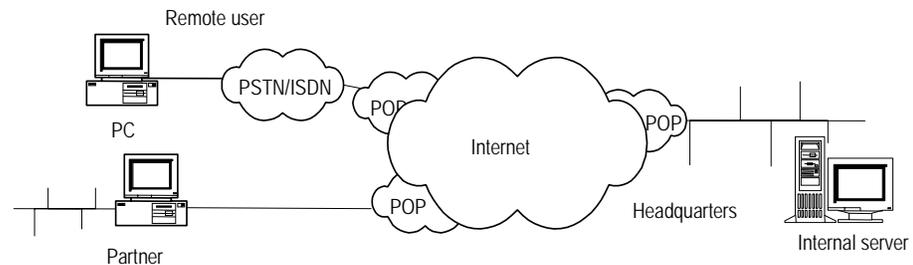
- The security of data transportation can be ensured. With VPN, reliable and safe connections can be established between remote users, branches of companies and commercial partners, and between suppliers and headquarters of companies. The advantage is especially significant in the integration of E-commerce or financial networks with the communication networks.
- Communicating information over the public networks decreases the cost for enterprises in connecting their remote branches, staff on business trips, and the business partners. It also improves the utility ratio of network resources and thereby increases the profits of Internet Service Providers (ISPs).
- VPN users can be added and deleted by configuring parameters without changing hardware, which makes VPN applications highly flexible.
- With VPN, VPN users can make mobile access at any time and any place, meeting the increasing mobile service requirements.

The VPN with service quality guarantee can provide different levels of service quality guarantees for users by charging for different services.

## Basic Networking Applications of VPN

An enterprise that has an intranet established with VPN is shown in the following figure.

**Figure 178** Schematic diagram of VPN networking



In this configuration, the users who need the internal resources of enterprises, can access the POP (Point of Presence) server of local ISP via PSTN or ISDN, and further access the internal resources of the enterprises. Traditional WAN construction techniques only supply the service with the aid of leased line between them. After a VPN is established, the remote users and the clients in other places can access internal resources of enterprises even if they do not have the Internet access authority given by local ISP.

VPN services of enterprises only require a server supporting VPN (a Windows NT server or a router). After connecting the local POP server via PSTN or ISDN, the users who want a resource directly call the remote servers of enterprises (VPN servers). The access server of ISP along with the VPN server accomplishes the call process.

## Classification of IP VPN

IP VPN is the emulation of leased line services (remote dial-up and DDN) of WAN equipment using IP facilities (including public Internet or private IP backbone network). IP VPN classification is based on:

- Operation Mode
- Tunnel Protocols
- Service Purpose
- Networking Model

### Operation Mode

VPNs can be CPE- or network-based. CPE-based VPN's require installation of networking and authentication equipment to support establishment of the VPN. It requires configuration and administration of WAN resources and bandwidth management.

In a network-based VPN, the maintenance of VPN is allocated to the ISP, although users are allowed to manage and control services to some extent. VPN functions are mainly fulfilled on the equipment at the network side. This type of service reduces the investments of the users, increases the flexibility and scalability of services, bringing profits to the service providers.

**Tunnel Protocols** The tunnel protocols can be divided into layer 2 tunneling protocols and layer 3 tunneling protocols depending on the layer at which the tunneling is implemented based on OSI model.

### Layer 2 tunneling protocol

The Layer 2 tunneling protocol encapsulates the whole PPP frame in the internal tunnel. The current layer 2 tunneling protocols mainly include:

- Point-to-Point Tunneling Protocol (PPTP): supported by Microsoft Corporation, Lucent Technologies and 3Com Corporation, and supported in Windows NT 4.0 version and above. This protocol supports the tunneling encapsulation of PPP protocols on IP networks. Being a calling control and management protocol, PPTP adopts the enhanced Generic Routing Encapsulation (GRE) technique to provide the encapsulation service of flow and congestion control for the transmitted PPP packets.
- Layer 2 Forwarding Protocol (L2F): As for the physical location, it supports the tunneling encapsulation of higher level protocols at the link layer and achieves the separation of dial-up server and dial-up protocol connection.
- Layer 2 Tunneling Protocol (L2TP): drafted by IETF and aided by companies such as Microsoft Corporation. It integrates the advantages of the above two protocols, and thus is accepted by the most enterprises as standard RFC. L2TP can be used not only for dial-up VPN (VPDN accessing) services but also leased line VPN services.

### Layer 3 tunneling protocol

Layer 3 tunneling protocol starts from and ends in ISP. PPP session ends in NAS and only layer 3 messages are carried over the tunnel. The current layer 3 tunneling protocols include:

- General Routing Encapsulation (GRE) protocol: used to implement the encapsulation of any network layer protocol on another network layer protocol.
- IP Security (IPSec) protocols: The IPSec protocol is composed of multiple protocols, such as Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE). They build a complete data security architecture on IP networks.

GRE and IPSec are mainly used for VPN leased line services.

### Comparison of layer 2 and layer 3 tunnel protocols

Layer 3 tunnel is more secure, scalable, and reliable. In terms of security, because layer 2 tunnel usually ends on the equipment at the user side, there is a high demand for security and firewall technology over a user network. Layer 3 tunnel usually ends at an ISP gateway and does not impose any threat to the security of the user's network

In terms of scalability, transmission efficiency may be degraded on a Layer 2 IP tunnel because all the PPP frames are encapsulated. And PPP session will run through the entire tunnel and end on the equipment at user side. So the gateway at the user side must store status and information about the PPP session, which affects the load and scalability of the system. In addition, because LCP and NCP negotiations of PPP are very time sensitive, the efficiency of IP tunnel results in a series of problems, such as PPP session timeout. Fortunately, layer 3 tunnel ends at

ISP gateway and PPP session ends at NAS, it is unnecessary for the gateway at the user end to manage and maintain the status of every PPP session, thus improving system performance.

Generally, Layer 2 and Layer 3 tunnel protocols are used independently so combining L2TP together with the IPSec protocol provides better performance and security for the users.

**Service Purpose** VPNs are also classified according to the types of service they provide:

- Intranet VPN: In an intranet VPN, the branches of an enterprise located everywhere are interconnected through the public network, which is the extension or substitute of traditional leased line networks or other enterprise networks.
- Access VPN: Access VPN provides a means to establish private connections with the intranet or extranet of enterprises through the public networks for those staff members on business errands, remote personnel and SOHO. Access VPN has two types: client-initiated VPN connections and NAS-initiated VPN connections.
- Extranet VPN: Extranet VPN extends an intranet to partners and clients through VPN so that different enterprises can build their VPNs using public networks.

**Networking Model** VPNs are classified by the type of networking model that they use:

- Virtual Leased Line (VLL): VLL emulates the traditional leased line service with the help of the IP network and hence providing asymmetrical and inexpensive leased line service. For the users at both ends of the VLL, the VLL is similar to the traditional leased line.
- Virtual Private Dial-up Network (VPDN): VPDN is implemented utilizing dial-up and access services of the public network (ISDN and PSTN), which provides access services for enterprises, small-sized ISPs, and mobile offices.
- Virtual Private LAN Segment (VPLS) service: In VPLS, LANs can be interconnected through virtual private segment with the help of IP public networks. It is the extension of LAN across IP public network.
- Virtual Private Routing Network (VPRN) service: VPRN implements the interconnection of headquarters, branches and remote offices by means of managing virtual routers, with the aid of the IP public networks. There are two ways to implement the services: one is to utilize the traditional VPN protocols as IPSec and GRE, and the other is to utilize the MPLS (Multiple Protocol Label Switching) technology.

---

**VPDN and L2TP  
Overview**

Virtual Private Dial Network (VPDN) is fulfilled with the help of dial-up and access services of public network (ISDN and PSTN), which provides access services for enterprises, small ISPs, and mobile offices.

VPDN adopts private communication protocols with network encryption feature, so enterprises can establish safe VPNs on public networks. Branch employees can connect to their enterprise's remote internal network through virtual encryption tunnels, while other users on public networks cannot access the Intranet resources through such virtual tunnels.

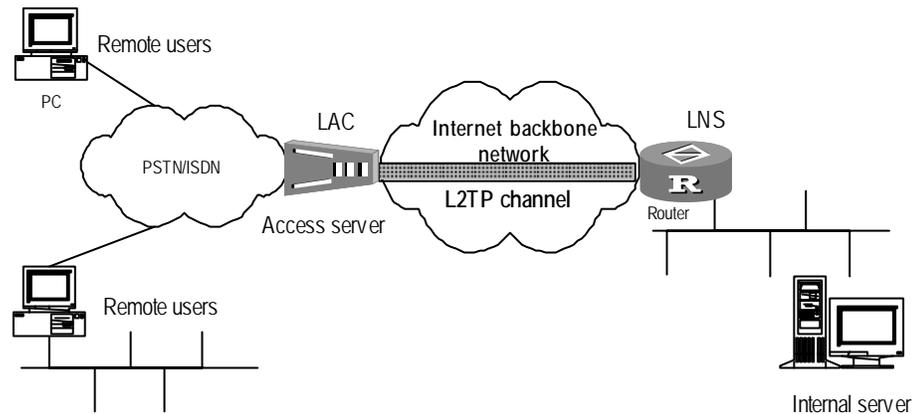
VPDN system is composed of NAS (Network Access Server), equipment, and management tools at the user end.

- NAS is provided by telecom departments or large-sized ISPs. As the access server of VPDN, NAS provides WAN interfaces, in charge of connecting PSTN or ISDN, and supports various LAN protocols, security management and authentication, and supports tunnels and other related techniques.
- The user-side equipment is located in the headquarters of an enterprise. According to different network functions, the equipment can function as a NAS, router or firewall.
- The management tool is responsible for managing VPDN equipment and users, including NMS and AAA.

Remote dial-up users access local ISP NAS by dialing via the local PSTN or ISDN. With the aid of a connection to the local ISP and proper tunneling protocol encapsulating a higher-level protocol, a VPN is established between the NAS and the peer gateway.

**VPDN Operation**

The VPDN tunneling protocol can be PPTP, L2F, or L2TP, the dominant protocol. When adopting the L2TP to build a VPDN, the typical networking is illustrated in Figure 179.

**Figure 179** Networking diagram of typical VPDN application

In this figure, LAC stands for L2TP Access Concentrator, which is a switch network device with a PPP end system and L2TP client-side processing ability. Usually, LAC is a NAS, which provides access service for users through PSTN/ISDN. LNS stands for L2TP Network Server, which is the device with a PPP end system and L2TP server-side processing ability.

LAC resides between the LNS and the remote system (remote users and remote branches) and is responsible for transmitting packets between them. It encapsulates the packets received from the remote system according to L2TP and sends them to the LNS, then de-encapsulates the packets from the LNS and sends them to the remote system. A local connection or PPP link can be used between the LAC and the remote system, but in a VPDN application, the PPP link is often adopted. Being an end of the L2TP tunnel, LNS is the peer device of LAC and is the logical terminating end of the PPP sessions transmitted by the LAC through the tunnel.

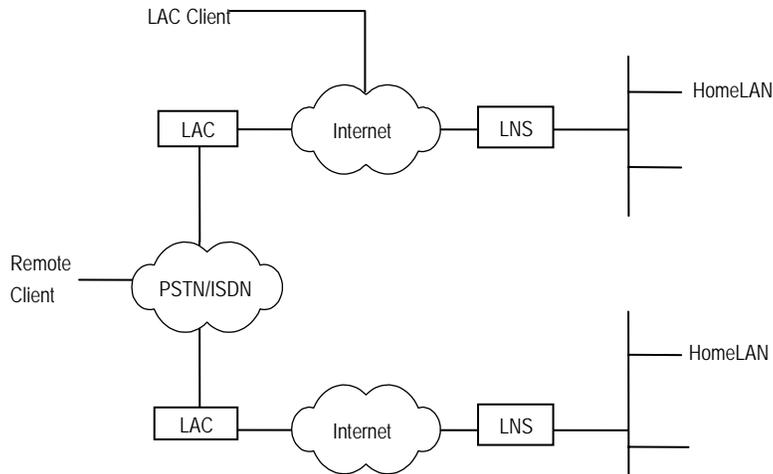
### Methods of Implementing VPDN

There are two methods to implement VPDN:

- **NAS-originated VPN:** NAS first establishes a tunnel with VPDN gateway using tunneling protocol, conveying the PPP connection to the gateways of enterprises. The current available protocols are L2F and L2TP. The advantage of the method is its transparency to users. After logging in once, the users can access the Intranet, which authenticates the users and distributes the internal addresses for users, avoiding consuming public addresses. The accounting of dial-up users can be implemented by the AAA at the LNS or LAC side. Users can access the network through various platforms. With the method, NAS should support VPDN protocol and the authentication system should support VPDN attributes. The gateway is usually a router or a VPN private gateway.
- **Client-originated VPN:** The client at the user end establishes a tunnel with the VPDN gateway. The client first calls and connects to the Internet, then establishes a tunnel connection with the enterprise gateway through special software for client (such as L2TP supported by Windows2000 platform). The advantage of the method is that there is no mode or geographical limit on accessing the Internet for users, independent of the ISP. The accounting of dial-up users can only be implemented through the AAA at the LNS side. The disadvantage of this method is that the users may be required to install special software.

The networking diagram of these two typical methods is illustrated in the following figure:

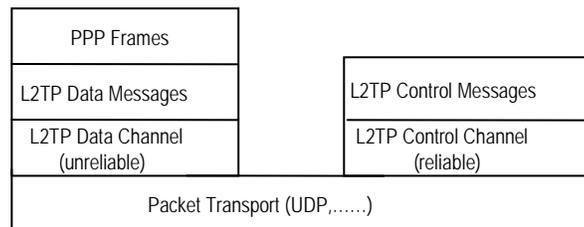
**Figure 180** Networking diagram of two typical methods of VPDN



**Overview of L2TP**

The L2TP (Layer 2 Tunneling Protocol) supports transmitting PPP frames by tunneling, and the end of layer 2 data link and the PPP session can reside on different devices, communicating based on packet switching which extends the PPP model. Integrating the respective advantages of L2F protocol and PPTP, L2TP has become the industrial standard of layer 2 tunneling protocol. The architecture of the protocol stack to which the L2TP belongs is illustrated in Figure 181.

**Figure 181** L2TP architecture



The L2TP architecture illustrated in Figure 181 describes the relation among PPP frames, control channels and data channels. A PPP frame is first transmitted in the unreliable data channel after being encapsulated with the L2TP header, and then undergoes the packet transmission process of UDP, Frame Relay and ATM. A control message is transmitted in the reliable L2TP control channel.

**Tunnel and session**

A L2TP tunnel is established between LAC and LNS, which is composed of one control connection and n (n0) sessions. Only one L2TP tunnel can be established between a pair of LAC and LNS. Both control message and PPP data message are transmitted in the tunnel. A session is also established between LAC and LNS, but session establishment must follow the successful establishment of the tunnel (including the exchange of such information as identity protection, L2TP version, frame type and hardware transmission type). One session connection corresponds to one PPP data stream between LAC and LNS.

The L2TP header includes the information of tunnel and session IDs, which are used to identify different tunnels and sessions. The messages with the same tunnel ID and different session IDs is multiplexed in one tunnel. Tunnel ID and session ID are distributed to the opposite end of the tunnel.

L2TP detects the connectivity of a tunnel using a Hello message. When the tunnel is idle for some time, LAC and LNS begin to transmit the Hello message to the opposite end. If no response to the Hello message is received for some time, the session is cleared up.

### **Control message and data message**

L2TP has two types of messages: control message and data message. The control message is used to establish, maintain and transmit the tunnel and session connection. The data message is used to encapsulate the PPP frame and transmit it in the tunnel. The transmission of a control message is reliable, but data message transmission is not reliable. If a data message is lost, it is not transmitted again. L2TP supports flow control and congestion control only for control messages, not for data messages.

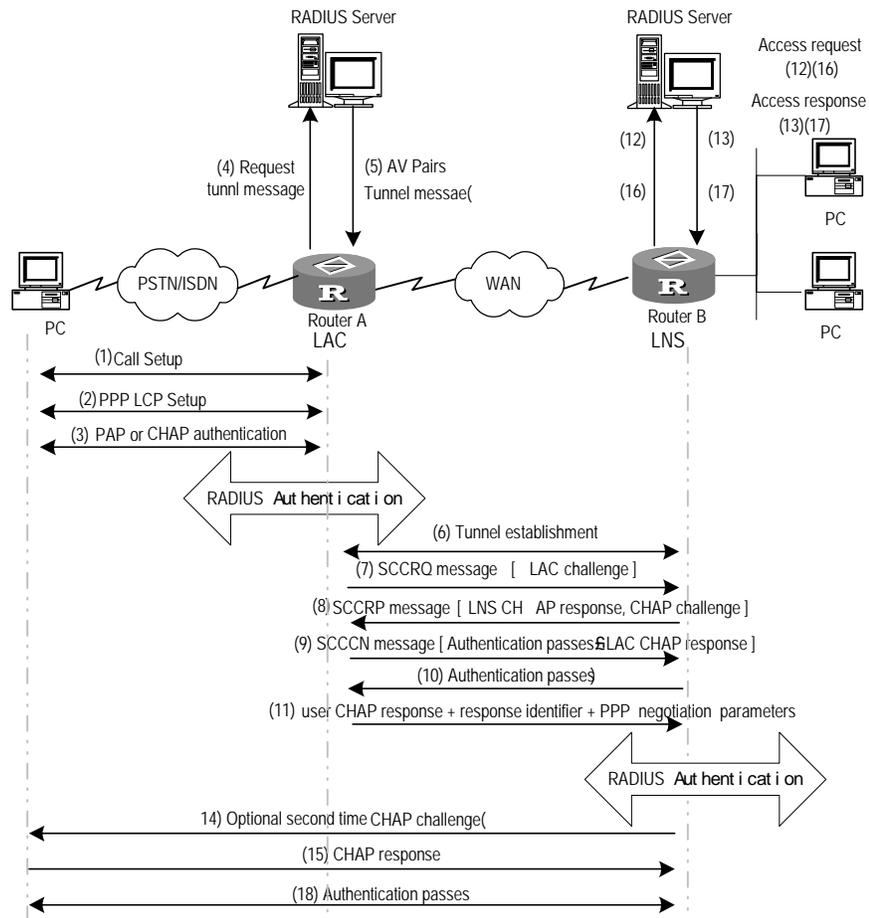
L2TP is transmitted in the form of a UDP message. L2TP registers UDP Port 1701, which is used only for initial tunnel establishment. Originating side of L2TP tunnel randomly selects an idle port (it need not to be 1701) and transmits a message to 1701 port of receiving side. After receiving the message, the receiving side randomly selects an idle port (it need not to be 1701) and transmits a message back to the specified port of the originating side. By now, the selected ports of both sides are selected and remain unchanged during the time segment when the tunnel is connected.

After being transmitted to L2TP and encapsulated with L2TP header, the PPP frame will be eventually encapsulated into UDP messages and transmitted on a TCP/IP network.

### **IV. Call setup flow of L2TP tunnel**

Call setup flow of L2TP tunnel is shown in the following figure:

Figure 182 Call setup flow of L2TP channel



### V. Features of L2TP

- Flexible identity authentication mechanism and high security
 

L2TP protocol by itself does not provide connection security, but it can depend on the authentication (e.g. CHAP and PAP) provided by PPP, so it has all security features of PPP. L2TP can be integrated with IPsec to fulfill data security, so it is difficult to attack the data transmitted with L2TP. As required by specific network security, L2TP adopts channel encryption technique, end-to-end data encryption or application layer data encryption on it to improve data security.
- Multi-protocol transmission
 

L2TP transmits PPP packets, so multiple protocols can be encapsulated in PPP packets.
- Supports the authentication of RADIUS server
 

LAC requires the authentication of RADIUS with user name and password. RADIUS server receives authentication request of the user, fulfils the authentication and returns the configuration information to establish the connection to LAC.
- Supports internal address allocation
 

LNS can be put behind the Intranet firewall. It can dynamically distribute and manage the addresses of remote users and support the application of private

addresses (RFC1918). The addresses allocated to remote users are private addresses belonging to an enterprise, thus the addresses can be easily managed and the security can also be improved.

- Flexible network charging

Charging can be fulfilled at both LAC and LNS sides at the same time, that is, at ISP (to generate bills) and Intranet gateway (to pay for charge and audit). L2TP can provide such charging data as transmitted packet number, byte number, start time and end time of the connection. And it can easily perform network charging according to these data.

- Reliability

L2TP supports the backup of LNS. When an active LNS is inaccessible, LAC can reconnect the backup LNS, which improves the reliability and error tolerance of VPN services.

### Basic Configuration at LAC

Basic configuration at LAC side includes:

- Enable L2TP
- Create a L2TP group
- Originate L2TP connection request and configure LNS address

Configure AAA and local users

### Enable L2TP

The L2TP on a router can work normally only after it is enabled. If it is disabled, the router will not provide the related function even if the L2TP parameters are configured.

Perform the following tasks in the system view.

**Table 665** Enable/Disable L2TP

| Operation    | Command                 |
|--------------|-------------------------|
| Enable L2TP  | <b>l2tp enable</b>      |
| Disable L2TP | <b>undo l2tp enable</b> |

By default, L2TP is disabled.

### Create a L2TP Group

To configure related parameters of L2TP, an L2TP group should be added. The L2TP group is used to configure the L2TP functions on the router and facilitate the networking applications of one-to-one, one-to-multiple, multiple-to-one and multiple-to-multiple connections between the LAC and LNS. L2TP group is numbered separately on the LAC and the LNS. Hence, it is only necessary to keep the corresponding relations between the related configurations of L2TP group at LAC and LNS side (e.g., the peer end name of the tunnel originating L2TP connection request and the LNS address).

After a L2TP group is created, other configurations related to this L2TP group, such as local name, originating L2TP connection request and LNS address, can be performed in L2TP group view. L2TP group1 works as the default L2TP group.

Perform the following tasks in the system view.

**Table 666** Create/Delete a L2TP Group

| Operation            | Command                                   |
|----------------------|-------------------------------------------|
| Create a L2TP group  | <code>l2tp-group group-number</code>      |
| Delete a L2TP group. | <code>undo l2tp-group group-number</code> |

### Originate L2TP Connection Request and Configure LNS Address

After a dial-up user passes VPN authentication successfully, LAC conveys the request of creating tunnel to a designated LNS. Besides the IP address of the LNS, LAC can fulfill authentication for 3 types (namely, 3 triggering conditions) of dial-up users based on this configuration: full user name (**fullusername**), user with a particular domain (**domain**) and called number (**dnis**). A maximum of 5 LNSs can be configured and LNSs will be searched for according to the address order configured.

Perform the following configurations in L2TP group view.

**Table 667** Originate L2TP Connection Request and LNS Address

| Operation                                                                                                | Command                                                                                                                              |
|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Configure to authenticate whether the user is a VPN user and set the IP address of the corresponding LNS | <code>start l2tp { ip ip-address [ ip ip-address ... ] } { domain domain-name   dnis dialed-number   fullusername user-name }</code> |
| Remove the connection request configuration                                                              | <code>undo start l2tp [ ip ip-address ]</code>                                                                                       |

There is no default value. One triggering condition must be configured.

### Configure AAA and Local Users

When configuring the AAA at LAC side, the local user name and password should be configured at LAC side if the **local** (authenticating locally) mode is selected.

LAC will authenticate remote dial-in user name and password to see whether they are compliant with the local registered user name and password, and hence to check whether these users are legal VPN users. Only after passing authentication successfully, can the request of establishing tunnel connection be processed, otherwise the user will be turned to services of other types except VPN.

When user ID authentication is implemented at LAC side, user name can be given in by the following means:

- Adopting the authentication based on particular domain (**domain**), the local user name and password configured are respectively the full user name and password registered.
- Adopting the authentication based on full user name (**fullusername**), the local user name configured is the domain name of the VPN user and the user's password.

Perform the `ppp authentication-mode` configuration in interface view and make the other configurations in system view.

**Table 668** Configure AAA and Local Users

| Operation                                             | Command                                                                                 |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Enable AAA.                                           | <b>aaa-enable</b>                                                                       |
| Configure the authentication method table of PPP user | <b>aaa authentication-scheme ppp { default   list-name } { method1} [ method2 ... ]</b> |
| Specify accounting scheme configure information       | <b>aaa accounting-scheme optional</b>                                                   |
| Configure to authenticate users.                      | <b>ppp authentication-mode { pap   chap }</b>                                           |
| Set user name and password.                           | <b>local-user username password { simple   cipher } password</b>                        |
| Remove the user name and password                     | <b>undo local-user username</b>                                                         |

By default, the local user name and password are not configured.

As the AAA attributes of L2TP are not standard attributes of RADIUS protocol, it is necessary to add the definition of L2TP attributes to the attribute set of RADIUS server.

**Table 669** L2TP Attribute Table

| Attribute value | Name                 | Description                      |
|-----------------|----------------------|----------------------------------|
| 100             | Tunnel-Type          | Tunnel type (L2TP=1)             |
| 101             | L2TP-Tunnel-Password | L2TP tunnel password             |
| 102             | Local-Name           | Local name of tunnel             |
| 103             | LNS-IP-Address       | IP address of LNS                |
| 104             | Tunnel-Medium-Type   | Medium type of the tunnel (IP=1) |
| 105             | L2TP group Number    | L2TP group number                |

## Basic Configuration at LNS

Basic configuration at LNS side includes:

- Enable L2TP
- Create a L2TP group
- Create a virtual template
- Configure the name of the receiving end of the tunnel
- Configure the local VPN user

**Enable L2TP** The L2TP on a router can work normally only after it is enabled. If it is disabled, the router will not provide the related function even if the L2TP parameters are configured.

Perform the following configurations in system view.

**Table 670** Enable/Disable L2TP

| Operation    | Command                 |
|--------------|-------------------------|
| Enable L2TP  | <b>l2tp enable</b>      |
| Disable L2TP | <b>undo l2tp enable</b> |

By default, L2TP is disabled.

**Create an L2TP Group**

To configure related parameters of L2TP, L2TP group should be added. The L2TP group is used to configure the L2TP functions on the router and facilitate the networking applications of one-to-one, one-to-multiple, multiple-to-one and multiple-to-multiple connections between the LAC and LNS. L2TP group is numbered separately on the LAC and the LNS. Hence, it is only necessary to keep the corresponding relations between the related configurations of L2TP group at LAC and LNS side (e.g., the peer end name of the tunnel originating L2TP connection request and the LNS address).

After a L2TP group is created, other configurations related to this L2TP group, such as local name, originating L2TP connection request and LNS address, can be performed in L2TP group view. L2TP group1 works as the default L2TP group.

Perform the following configurations in system view.

**Table 671** Create/Delete L2TP Group

| Operation           | Command                                    |
|---------------------|--------------------------------------------|
| Create a L2TP group | <b>l2tp-group</b> <i>group-number</i>      |
| Delete a L2TP group | <b>undo l2tp-group</b> <i>group-number</i> |

**Create a Virtual Template**

Virtual template is mainly used to configure working parameters of the virtual interfaces dynamically created by the router in the process of operation, such as configuring MP-bounding logic interface and L2TP logic interface.

Perform the following configurations in system view.

**Table 672** Create/Delete a Virtual Template

| Operation                 | Command                                                                  |
|---------------------------|--------------------------------------------------------------------------|
| Create a virtual template | <b>interface virtual-template</b><br><i>virtual-template-number</i>      |
| Delete a virtual template | <b>undo interface virtual-template</b><br><i>virtual-template-number</i> |



*By far, the virtual template in L2TP application only supports one peer but does not support IP unnumbered, that is, the virtual template has to be configured with its own IP address.*



*Dial-up users should only be allocated with negotiation IP addresses by LNS dynamically, not be configured with fix addresses.*



*When using the **ip pool** command to configure the address allocated to the peer, the user should ensure that the virtual template address and the address pool are on the same segment.*

**Configure the Name of the Receiving End of the Tunnel**

The LNS can receive the requests of establishing tunnels from different LACs using different virtual templates. After a request of this is received, the LNS will check whether the name of LAC is compliant with that of the legal remote end of the tunnel first, then decide whether the tunnel will be created.

Perform the following configurations in L2TP group view.

**Table 673** Configure the Name of the Receiving End of the Tunnel

| Operation                                           | Command                                                                           |
|-----------------------------------------------------|-----------------------------------------------------------------------------------|
| Set the name of the receiving end of the tunnel.    | <b>allow l2tp virtual-template virtual-template-number [ remote remote-name ]</b> |
| Remove the name of the receiving end of the tunnel. | <b>undo allow</b>                                                                 |

When the group number of L2TP is 1 (the default L2TP group number), it is unnecessary to specify the *remote-name*. If the name of remote end is still specified in the view of L2TP group 1, L2TP group 1 will not work as the default L2TP group.



*Only L2TP group 1 can be set as the default group.*



*The **start l2tp** command and the **allow l2tp** command are mutually exclusive. That means after one is configured, the other will automatically become invalid. A L2TP group cannot serve LAC and LNS at the same time.*

By default, receiving dial-in from LAC is disabled.

### Configure the Local VPN User

In the mode of "fullusername@domain" and password, LAC conveys these information input by VPN users to LNS for authentication, LNS will perform the local authentication first and then the RADIUS authentication to ensure these users are legal VPN users. The process of RADIUS authentication will be removed once users have passed local authentication. These VPN users can access internal resource after the authentication at LNS.

Perform the **ppp authentication-mode** configuration in interface view and make the other configurations in system view.

**Table 674** Configure Local VPN Users

| Operation                                             | Command                                                                                 |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Enable AAA.                                           | <b>aaa-enable</b>                                                                       |
| Configure the authentication method table of PPP user | <b>aaa authentication-scheme ppp { default   list-name } { method1} [ method2 ... ]</b> |
| Specify accounting scheme configure information       | <b>aaa accounting-scheme optional</b>                                                   |
| Configure to authenticate users.                      | <b>ppp authentication-mode { pap   chap }</b>                                           |
| Set user name and password.                           | <b>local-user username password { simple   cipher } password</b>                        |



*At LNS, local user name configured adopts the mode of "fullusername@domain"*

### Advanced Configuration at LAC or LNS

Advanced configurations at LAC side includes:

- Configure the local name
- Enable tunnel authentication and set password
- Configure the interval for sending Hello messages

- Configure to disconnect tunnel by force
- Configure the receiving window size for controlling flow over tunnel
- Enable/Disable hiding AV pairs
- Configure the maximum number of L2TP sessions
- Configure domain delimiter and searching order

Advanced configurations at LNS side includes:

- Configure the local name
- Enable tunnel authentication and set password
- Configure the interval for sending Hello messages
- Configure to disconnect tunnel by force
- Configure the receiving window size for controlling flow over tunnel
- Enable/Disable hiding AV pairs
- Configure the maximum number of L2TP sessions
- Configure to force the local end to implement CHAP authentication
- Configure to force the LCP to renegotiate
- Configure the local address and address pool

## Configure the Local Name

This configuration is applicable to LAC and LNS.

Users can configure the local tunnel name at both LAC and LNS. The tunnel name at LAC should keep consistent with the name of the receiving end of the tunnel configured at LNS.

Perform the following configurations in L2TP group view.

**Table 675** Set Local Name

| Operation                                    | Command                 |
|----------------------------------------------|-------------------------|
| Set the local name.                          | <b>tunnel name name</b> |
| Restore the default value of the local name. | <b>undo tunnel name</b> |

By default, the local name is the host name of router.



*The tunnel name configured through the **tunnel name** command at LAC side must be consistent with the name of the remote receiving tunnel configured through the **allow l2tp** command at LNS side.*

## Enable Tunnel Authentication and Setting Password

This configuration is applicable to LAC and LNS.

Before creating a tunnel connection, the users can decide, as needed, whether to enable tunnel authentication. There are three tunnel authentication modes as follows:

- LAC authenticates LNS.
- LNS authenticates LAC.

- LAC and LNS authenticate each other.

It can be found that either LAC or LNS can originate tunnel authentication request. However, if one side enables the tunnel authentication, the tunnel can be established only when the passwords on both ends of the tunnel are exactly the same. If tunnel authentication is disabled on both ends, whether or not the tunnel authentication passwords are the same will make no sense.

Perform the following configurations in L2TP group view.

**Table 676** Set Tunnel Authentication and Password

| Operation                                     | Command                                             |
|-----------------------------------------------|-----------------------------------------------------|
| Enable tunnel authentication                  | <b>tunnel authentication</b>                        |
| Disable tunnel authentication.                | <b>undo tunnel authentication</b>                   |
| Set the password of tunnel authentication.    | <b>tunnel password { simple   cipher } password</b> |
| Remove the password of tunnel authentication. | <b>undo tunnel password</b>                         |

Tunnel authentication is enabled by default. If no tunnel authentication password is configured, the host name of the router will act as the tunnel authentication password. In order to ensure tunnel security, users are recommended not to disable tunnel authentication.



*To ensure the tunnel security, it is recommended that the user should not disable tunnel authentication.*



*The tunnel authentication password is the router host name, so you must manually configure the tunnel authentication password after the authentication is enabled, and ensure that the password at the LAC side is the same as that at the LNS side.*

### Configure the Interval for Sending Hello Messages

This configuration is available to LAC and LNS.

To detect the connectivity of the tunnel between LAC and LNS, both the LAC and the LNS will regularly send Hello messages to the peer and the receiving end will make responses upon receiving. If the LAC or LNS does not receive the Hello response within the specified interval, the Hello messages will be repeatedly sent. If no response message from the peer is received after three Hello messages are sent, the local end will assume the L2TP tunnel has already been disconnected. In order to restore connectivity between the LAC and LNS, a new tunnel will have to be established.

Perform the following configurations in L2TP group view.

**Table 677** Set the Interval for Sending Hello Message

| Operation                                            | Command                                  |
|------------------------------------------------------|------------------------------------------|
| Set the interval for sending tunnel hello packet     | <b>tunnel timer hello hello-interval</b> |
| Restore the interval for sending tunnel hello packet | <b>undo tunnel timer hello</b>           |

By default, the interval for sending the tunnel Hello message is 60 seconds. If this configuration is not implemented, LAC or LNS will adopt the default value as the interval to send the Hello message to the peer.

### Configure Domain Delimiter and Searching Order

This configuration is applicable to LAC only.

If there are a lot of users dialing in domain name mode, it is time-consuming to search users in sequence. Therefore, it is recommended to set the necessary searching policies (e.g., prefix and suffix delimiters) at LAC side to speed up the searching.

The delimiters fall into prefix delimiter and suffix delimiter, including @, #, & and /. The user with prefix delimiter can be "3Com.com#vpdnuser" and correspondingly the suffix delimiter will be "vpdnuser@3Com.com". During the searching, separating user name from prefix/suffix delimiter, based on the defined rules will greatly speed up the searching.

In domain name mode, there are four optional searching rules on condition that the prefix/suffix delimiter is set:

- **dnis-domain** (Search according to dialed number first, then according to domain name)
- **dnis** (Search according to dialed number only)
- **domain-dnis** (Search according to domain name first, then according to dialed number)
- **domain** (Search according to domain name only)

Perform the following configurations in system view.

**Table 678** Set Domain Name Delimiter and Searching Order

| Operation                           | Command                                                                          |
|-------------------------------------|----------------------------------------------------------------------------------|
| Set prefix/suffix delimiter         | <code>l2tp domain { prefix-separator   suffix-separator } delimiters</code>      |
| Delete the prefix/suffix delimiter  | <code>undo l2tp domain { prefix-separator   suffix-separator } delimiters</code> |
| Set searching order                 | <code>l2tp match-order { dnis-domain   dnis   domain-dnis   domain }</code>      |
| Restore the default searching order | <code>undo l2tp match-order</code>                                               |

The `l2tp match-order` command merely configures the order of dialed number and domain name for searching. In an actual searching process, the searching is by all means conducted according to the full user name first, and then the configured order of this command.

By default, search according to dialed number prior to domain name.

### Disconnect Tunnel by Force

This configuration is applicable to LAC and LNS.

When the number of users decreases to 0, or faults occur on the network, or administrator takes the initiative to disconnect the tunnel, the tunnel will be cleared. Either LAC or LNS can originate the request of clearing the tunnel. The end receiving the request of clearing should transmit acknowledgement

information (ACK) and wait for some time before clearing the tunnel, so that the request transmitted again from the peer can be properly received when ACK message is lost. After disconnecting the tunnel by force, all control connections and session connections on the tunnel will also be cleared. After tunnel disconnection, a new tunnel will be established again when new users dial in.

Perform the following configuration in system view.

**Table 679** Force to Disconnect Channel

| Operation                  | Command                              |
|----------------------------|--------------------------------------|
| Force to disconnect tunnel | <b>reset l2tp tunnel remote-name</b> |

### Configure to Force the Local End to Implement CHAP Authentication

This configuration is applicable to LNS only.

After LAC performs the proxy authentication for dial-up users, LNS can authenticate these users again. In this case, the users will be authenticated twice, the first authentication being at LAC and the second one at LNS side. Only after passing both of the authentications can the L2TP tunnel be established.

In actual L2TP application, there are three methods of authentication: proxy authentication, forcing CHAP authentication and LCP renegotiation.

- The priority of LCP renegotiation has the highest priority among the three types, which means if LCP renegotiation and forcing CHAP authentication are configured at LNS at the same time, L2TP will adopt LCP renegotiation first and then use authentication methods configured on corresponding virtual template.
- If only forcing CHAP authentication is configured, LNS will authenticate users by means of CHAP. Only after user name, password and authentication are configured at LNS, and AAA function is enabled, can the process of forcing CHAP authentication locally take effect.
- If neither LCP renegotiation nor forcing CHAP authentication is configured, LNS will perform the proxy authentication for the users. In this case, LAC conveys all the authentication information received from users and the information configured at LAC itself to LNS, and LNS will authenticate users according to the information and authentication mode of LAC. When proxy authentication is used at LNS, if LAC is configured with PAP, while the virtual interface template at LNS is configured with CHAP, which is higher than PAP, the process of authentication fails all the time and no sessions can be created.



*If the **aaa authentication-scheme ppp default none** is configured at LAC side, the AAA authentication will not be enabled, no matter whether PAP or CHAP authentication is adopted at LAC side. However, after the authentication mode is transmitted to LNS, LNS will still authenticate the user, no matter whether LNS is configured with **aaa-enable** command.*

Perform the following configurations in L2TP group view.

**Table 680** Force Local End to Perform CHAP Authentication

| Operation                                       | Command                    |
|-------------------------------------------------|----------------------------|
| Force local end to perform CHAP authentication. | <b>mandatory-chap</b>      |
| Remove the local CHAP authentication.           | <b>undo mandatory-chap</b> |

Local CHAP authentication will not be carried out by default.

### Configure to Force the LCP to Renegotiate

This configuration is applicable to LNS only.

For an NAS-originated VPN service request, at the beginning of PPP session, the user will first perform the PPP negotiation with the NAS. If the negotiation succeeds, the NAS will initiate the L2TP tunnel connection and transmit the user information to the LNS where the user will be checked based on the received proxy authentication information.

But in some specific cases (e.g., when it is necessary to authenticate and charge at LNS side), the LCP renegotiation between the LNS and the user will be implemented by force, at that time, the proxy authentication information at NAS side will be ignored.

Perform the following configurations in L2TP group view.

**Table 681** Force LCP to Renegotiate

| Operation                   | Command                   |
|-----------------------------|---------------------------|
| Force LCP to renegotiate.   | <b>mandatory-lcp</b>      |
| Disable LCP to renegotiate. | <b>undo mandatory-lcp</b> |

LCP does not renegotiate by default.



*After LCP renegotiation is enabled, LNS will not reauthenticate users if there is no authentication information configured on the virtual template, then users are authenticated only once at LAC.*

### Configure the Local Address and Address Pool

This configuration is applicable to LNS only.

After the L2TP tunnel connection between LAC and LNS is established, the LNS should allocate the IP addresses in an address pool to the VPN users. Before selecting an address pool, the user should use the **ip pool** command in system view.

Perform the following configurations in Virtual template interface view.

**Table 682** Set the Local Address and the Address Pool

| Operation                   | Command                                                     |
|-----------------------------|-------------------------------------------------------------|
| Set the local IP address    | <b>ip address ip-address netmask [ sub ]</b>                |
| Remove the local IP address | <b>undo ip address [ ip-address netmask [ sub ] ]</b>       |
| Specify the address pool    | <b>remote address { ip-address / pool [ pool-number ] }</b> |
| Delete the address pool     | <b>undo remote address</b>                                  |

By default, address pool 0 (the default one) will be used by the peer for allocating addresses.



*When specifying the address pool from which addresses are allocated for users, the default address pool will be used for allocating addresses if no specific pool-number value is configured after the key word **pool**.*

### Configure the Receiving Window Size for Controlling Flow over Tunnel

This configuration is applicable to LAC and LNS.

L2TP has simple flow control function. The users can specify the size of receiving window for controlling flow over tunnel.

Perform the following configurations in L2TP group view.

**Table 683** Set the Size of Receiving Window for Controlling Flow Over Tunnel

| Operation                                                                            | Command                                        |
|--------------------------------------------------------------------------------------|------------------------------------------------|
| Set the receiving window size for controlling flow over tunnel.                      | <b>tunnel flow-control receive-window size</b> |
| Restore the receiving window size for controlling flow over tunnel to default value. | <b>undo tunnel flow-control receive-window</b> |

By default, the receiving window size for controlling flow on tunnel is 0 (no flow control).

### Enable/Disable Hiding Attribute Value Pairs (AV pairs)

This configuration is used at the LAC and LNS sides.

L2TP enables hiding AV pairs, and it is very useful when PAP or proxy authentication is employed between LAC and LNS. Only after the tunnel authentication and tunnel password are configured first, can the AV pairs hiding be meaningful. After the AV pairs are hidden, the L2TP hiding algorithm will be implemented, so that the username and password transmitted in plaintext during proxy authentication can be encrypted in AV pairs.

Please perform the following configurations in L2TP group view.

**Table 684** Enable/Disable Hiding AV Pairs

| Operation               | Command                       |
|-------------------------|-------------------------------|
| Enable hiding AV pairs  | <b>tunnel avp-hidden</b>      |
| Disable hiding AV pairs | <b>undo tunnel avp-hidden</b> |

By default, AV pairs are hidden.



*In actual configuration, it is recommended to enable hiding AV pairs at LAC and LNS sides at the same time, or disable hiding AV pairs at LAC and LNS sides at the same time*

### Configure the Maximum Number of L2TP Sessions

This configuration is applicable to LAC and LNS.

Users can configure the maximum number of sessions at local end as needed, so as to effectively control the quantity of VPN users who are accessing the network simultaneously and keep it within a reasonable range. Thereby, the service quality

of each VPN connection can be guaranteed. The maximum number of sessions can be configured at either LNS or LAC, and the smaller one is valid.

Perform the following configurations in system view.

**Table 685** Configure the Maximum Number of L2TP Sessions

| Operation                                                             | Command                                  |
|-----------------------------------------------------------------------|------------------------------------------|
| Configure the maximum number of L2TP sessions at local                | <b>l2tp session-limit session-number</b> |
| Restore the maximum number of L2TP sessions at local to default value | <b>undo l2tp session-limit</b>           |

By default, the maximum number of L2TP sessions is 1000.



*Given that a certain number of sessions have existed on the router, the system will display the information indicating misconfiguration if the **l2tp session-limit** command is used to configure a session-number smaller than the current one.*

## Display and Debug L2TP

Use **debugging**, **display** command in all views.

**Table 686** Display and Debug L2TP

| Operation                                    | Command                                                                                 |
|----------------------------------------------|-----------------------------------------------------------------------------------------|
| Display the current L2TP tunnel information. | <b>display l2tp tunnel</b>                                                              |
| Display the current L2TP session information | <b>display l2tp session</b>                                                             |
| Enable the debugging of L2TP.                | <b>debugging l2tp { all   control   error   event   hidden   payload   time-stamp }</b> |

## L2TP Configuration Examples

### NAS-originated VPN Networking

#### I. Networking requirements

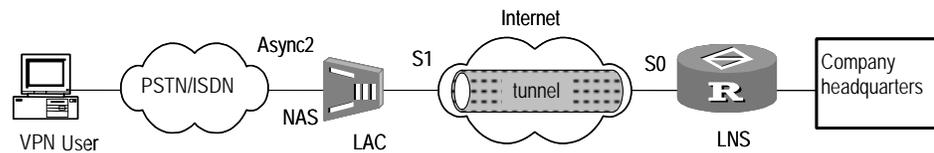
A user can access the Intranet of an enterprise through local dial-up access. The NAS authenticates the users to determine whether they are VPN users. The tunnel is used to transmit data between NAS and LNS.

A user can have access to the LAN of a company through dialup. Both the LAC (NAS) and LNS connect to the Internet through serial interfaces, and transmit data through Tunnel. The PC is installed with Windows2000 operation system.

The Async2 interface of LAC and PC are connected to a Modem, and the numbers are 5660046 and 5660040 separately.

## II. Networking diagram

**Figure 183** Networking diagram of NAS-originated VPN



## III. Configuration procedure

### 1 Configuration at the LAC (NAS) side:

- a Configure username and password (when dialing in Windows2000).

```
[Router-LAC] local-user lac service-type ppp password simple lac
```

- b Implement local AAA authentication on VPN user.

```
[Router-LAC] aaa-enable
[Router-LAC] aaa authentication-scheme ppp default local
[Router-LAC] aaa accounting-scheme optional
```

- c Configure the IP address of Serial1 interface of LAC.

```
[Router-LAC] interface serial 1
[Router-LAC-Serial1] ip address 192.167.0.2 255.255.255.0
```

- d Enable L2TP service and configure a L2TP group.

```
[Router-LAC] l2tp enable
[Router-LAC] l2tp-group 1
[Router-LAC-l2tp1] tunnel name lac-end
[Router-LAC-l2tp1] start l2tp ip 192.167.0.1 fullusername lac
```

- e Enable tunnel authentication and configure a tunnel authentication password.

```
[Router-LAC-l2tp1] tunnel authentication
[Router-LAC-l2tp1] tunnel password simple 3Com router
```

- f Configure BDR dialup parameters.

```
[Router-LAC] dialer-rule 1 ip permit
[Router-LAC] interface async 2
[Router-LAC-Async2] async mode protocol
[Router-LAC-Async2] link-protocol ppp
[Router-LAC-Async2] ppp authentication-mode chap
[Router-LAC-Async2] dialer enable-legacy
[Router-LAC-Async2] dialer-group 1
```

### 2 Configuration at LNS side

- a Configure username and password (they should be the same as those configured at LAC side)

```
[Router-LNS] local-user lac service-type ppp password simple lac
```

- b Define an address pool and assign an address for the dialup user.

```
[Router-LNS] ip pool 1 192.168.0.3 192.168.0.100
```

- c Implement local AAA authentication for the VPN user.

```
[Router-LNS] aaa-enable
[Router-LNS] aaa authentication-scheme ppp default local
[Router-LNS] aaa accounting-scheme optional
```

d Configure the IP address of Serial0 interface of LNS.

```
[Router-LNS] interface serial 0
[Router-LNS-Serial0] ip address 192.167.0.1 255.255.255.0
```

e Configure the Virtual-Template-related information.

```
[Router-LNS] interface virtual-template 1
[Router-LNS-Virtual-Template1] ip address 192.168.0.1 255.255.255.0
[Router-LNS-Virtual-Template1] ppp authentication-mode chap
[Router-LNS-Virtual-Template1] remote address pool 1
```

f Enable L2TP service and configure a L2TP group.

```
[Router-LNS] l2tp enable
[Router-LNS] l2tp-group 1
[Router-LNS-l2tp1] tunnel name lns-end
[Router-LNS-l2tp1] allow l2tp virtual-template 1 remote lac-end
```

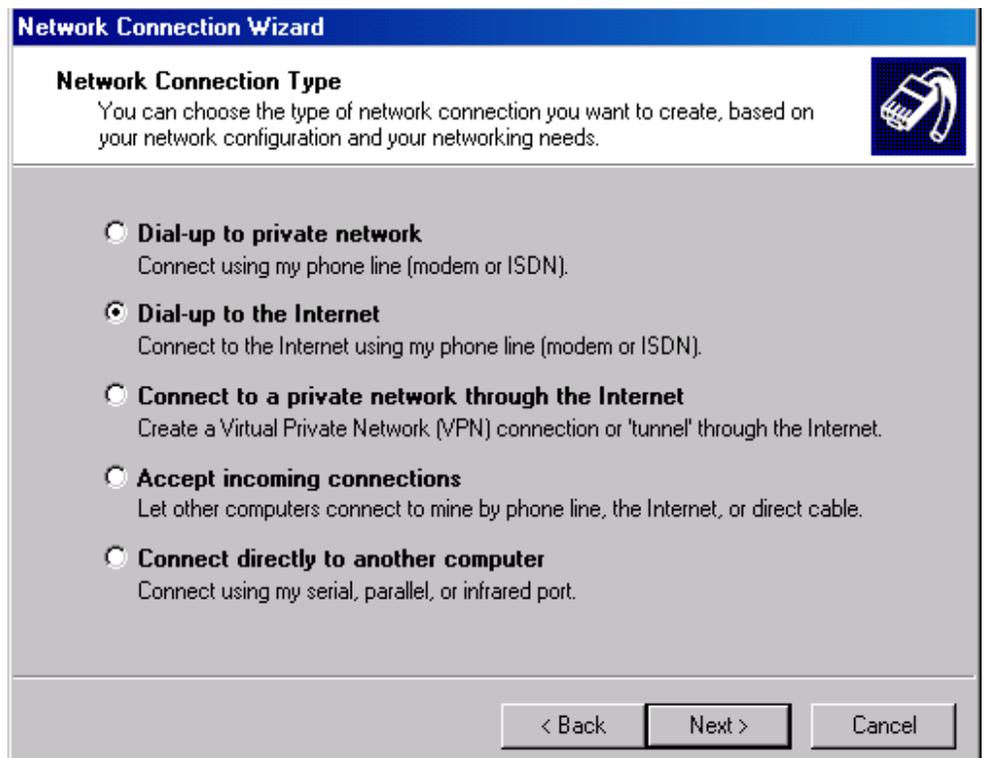
g Enable tunnel authentication and configure a tunnel authentication password.

```
[Router-LNS-l2tp1] tunnel authentication
[Router-LNS-l2tp1] tunnel password simple 3Com router
```

### 3 Configuration at the user side

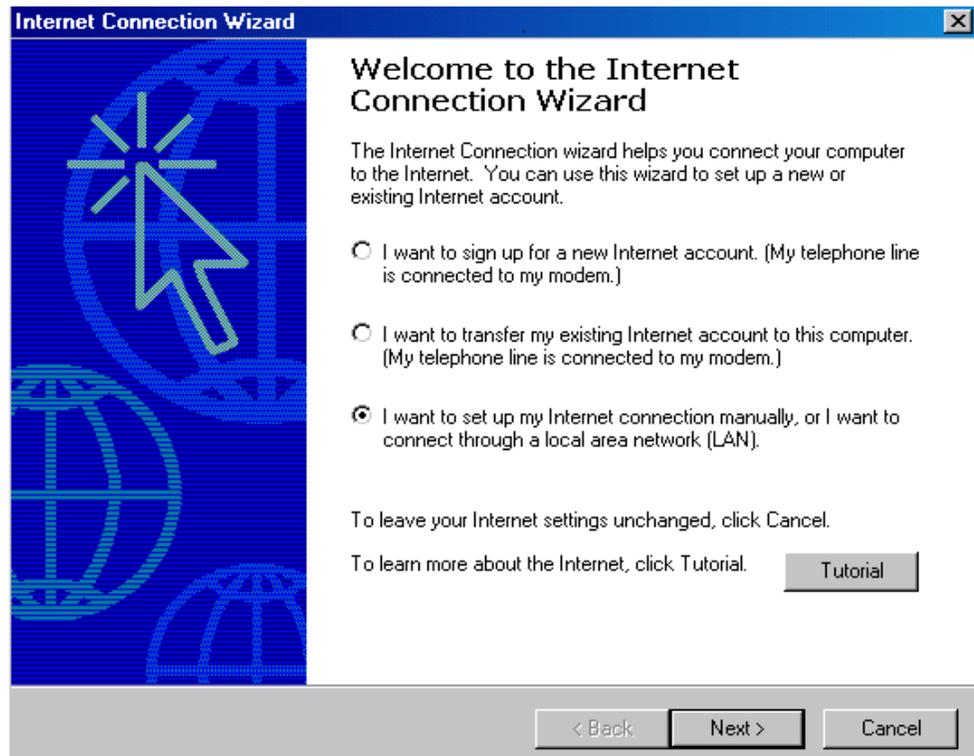
- Open [Start/Program/Accessories/Communication/Network Connection Wizard] on the PC installed with Windows2000 operation system. Double click [New Connection] and choose "Dial-up to the Internet".

Figure 184 Network Connection Wizard



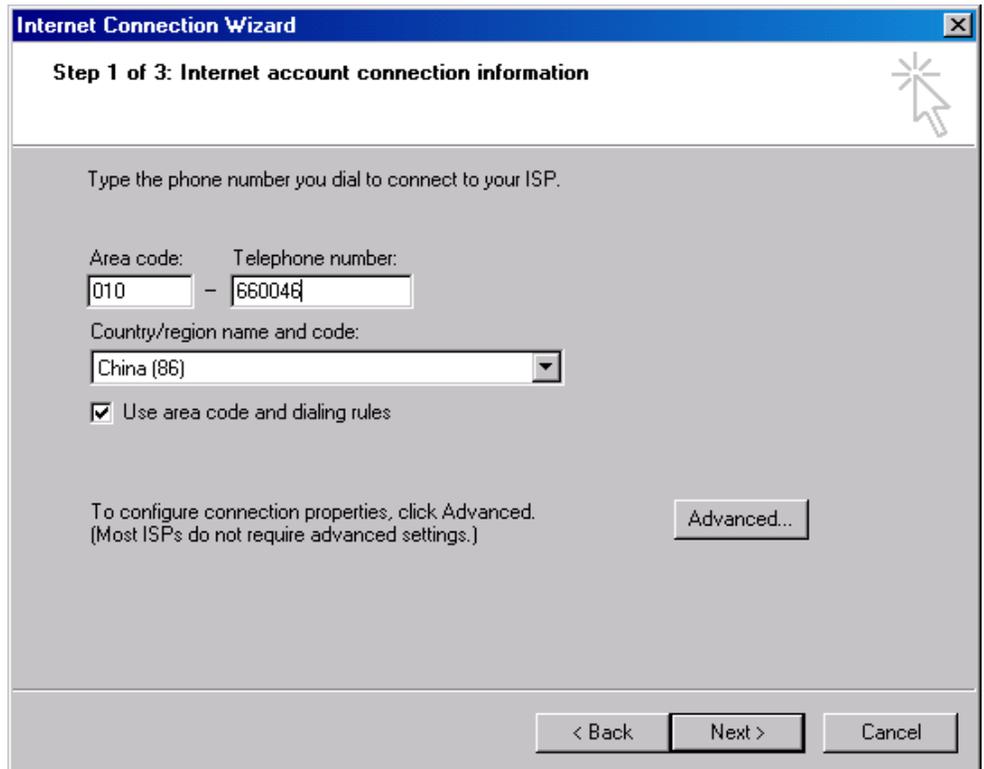
- Click <Next> and choose "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" in the popup dialog box, as shown in the following figure.

Figure 185 Internet Connection Wizard (1)



- Click <Next> and input the telephone number at the NAS side in the popup dialog box (if it is a local telephone number, you should deselect "Use area code and dialing rules"), as shown in the following figure.

Figure 186 Internet Connection Wizard (2)

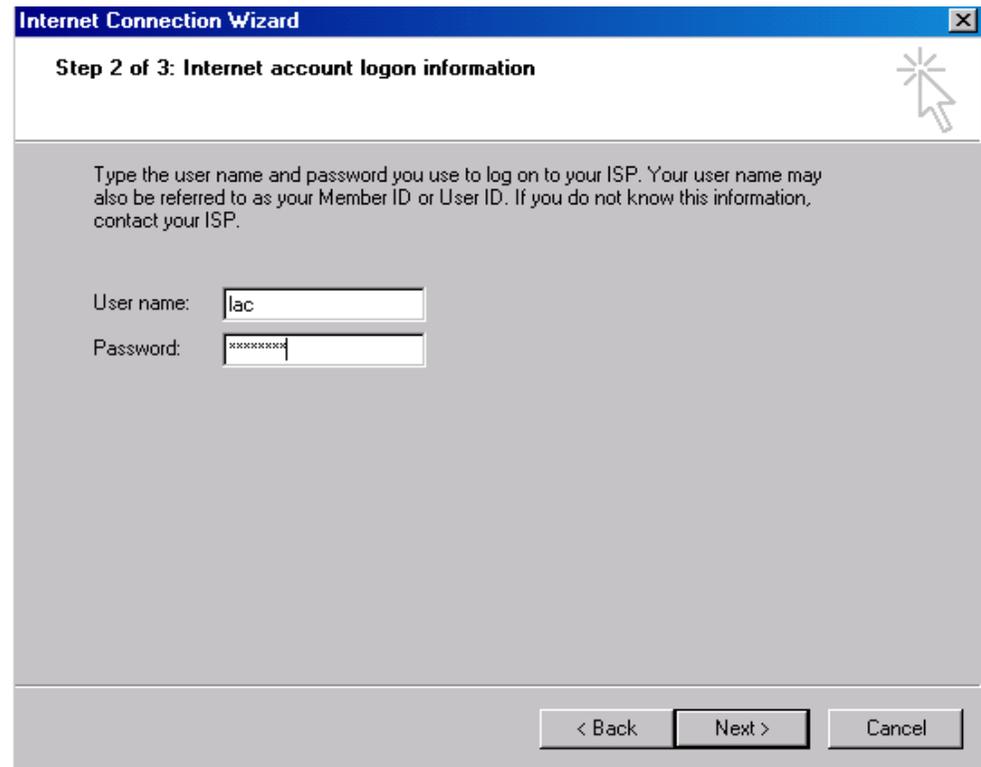


The screenshot shows a window titled "Internet Connection Wizard" with a close button in the top right corner. The main heading is "Step 1 of 3: Internet account connection information". Below this, there is a text prompt: "Type the phone number you dial to connect to your ISP." The form contains the following fields and controls:

- "Area code:" with an input field containing "010".
- "Telephone number:" with an input field containing "660046".
- "Country/region name and code:" with a dropdown menu showing "China (86)".
- A checked checkbox labeled "Use area code and dialing rules".
- An "Advanced..." button.
- At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

- Click <Next> and input username and password (such as the username lac and password lac) in the popup dialog box so as to access ISP. The input contents must be the same as the configuration at the NAS side, as shown in the following figure.

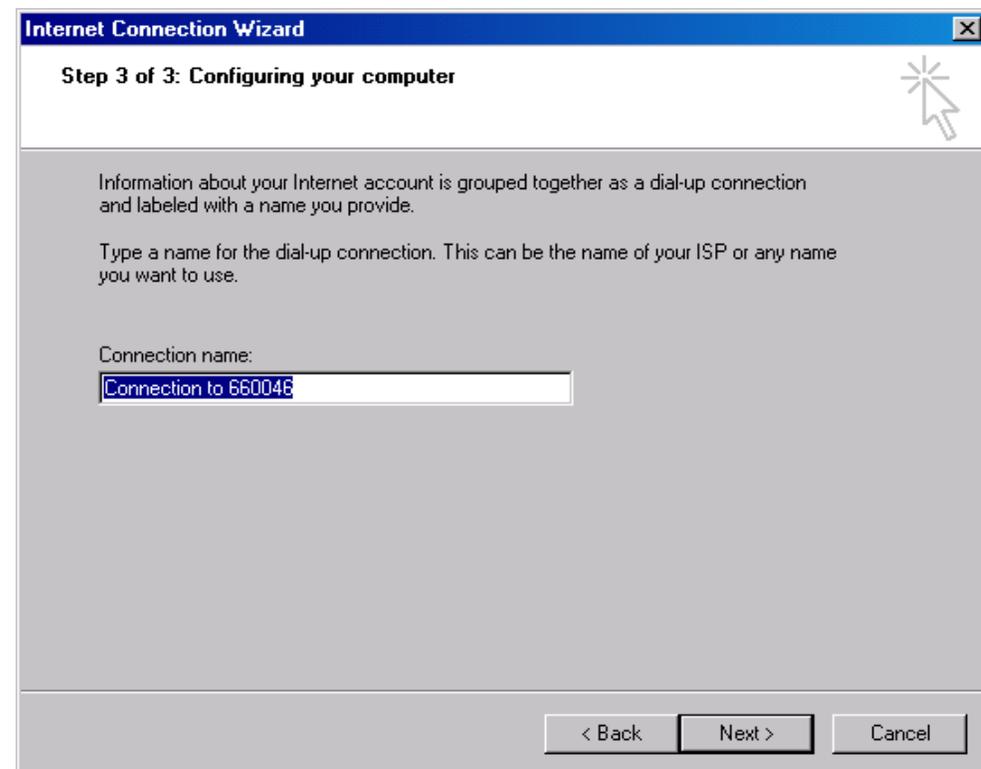
Figure 187 Internet Connection Wizard (3)



The screenshot shows the 'Internet Connection Wizard' window at 'Step 2 of 3: Internet account logon information'. The window title bar is blue with the text 'Internet Connection Wizard' and a close button. The main area has a white header with the step title and a mouse cursor icon. Below the header, there is instructional text: 'Type the user name and password you use to log on to your ISP. Your user name may also be referred to as your Member ID or User ID. If you do not know this information, contact your ISP.' There are two input fields: 'User name:' with the text 'lac' and 'Password:' with masked characters 'XXXXXXXX'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- Click <Next> and input the name of dialup connection (such as "Connection to 660046") in the popup dialog box, as shown in the following figure.

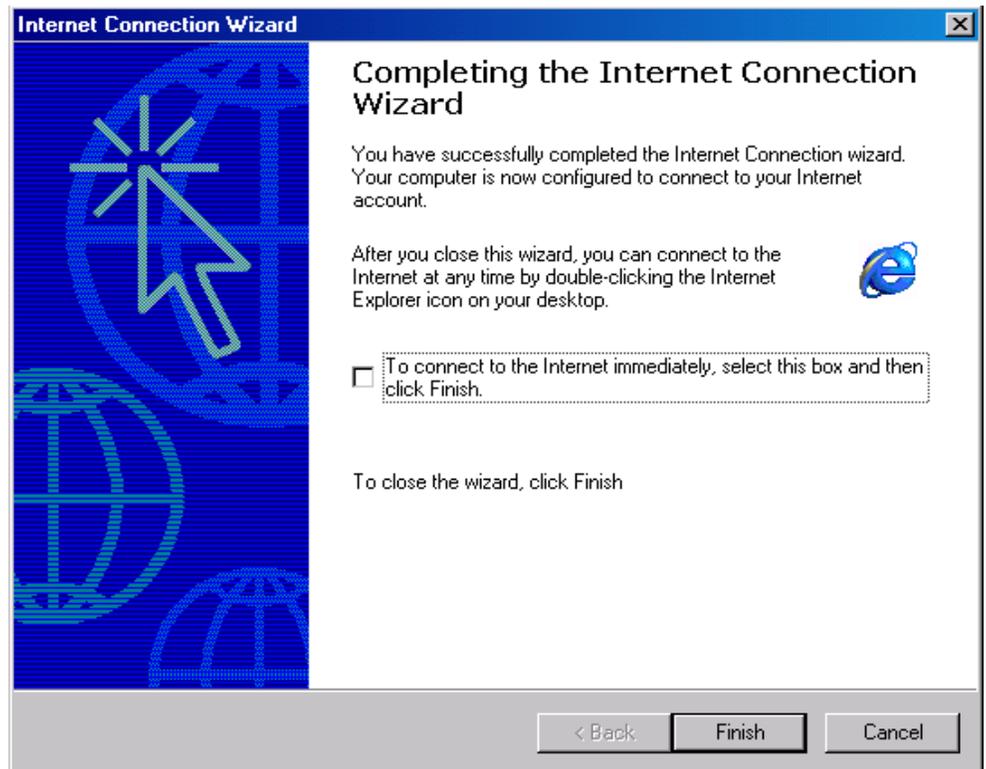
Figure 188 Internet Connection Wizard (4)



The screenshot shows the 'Internet Connection Wizard' window at 'Step 3 of 3: Configuring your computer'. The window title bar is blue with the text 'Internet Connection Wizard' and a close button. The main area has a white header with the step title and a mouse cursor icon. Below the header, there is instructional text: 'Information about your Internet account is grouped together as a dial-up connection and labeled with a name you provide.' and 'Type a name for the dial-up connection. This can be the name of your ISP or any name you want to use.' There is one input field labeled 'Connection name:' with the text 'Connection to 660046'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

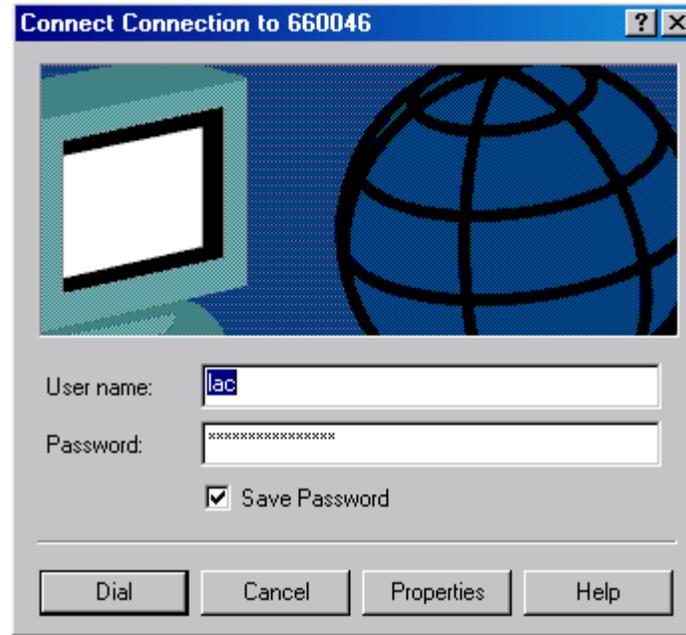
- Click <Next> and deselect "To connect to the Internet immediately, select this box and then click Finish" in the popup dialog box, as shown in the following figure.

**Figure 189** Internet Connection Wizard (5)



- Click <Finish> and double click "Connection to 66046" icon, then after inputting the username and password, you can dial up to access NAS. As receiving the call, NAS will establish a tunnel and session to LNS, as shown in the following figure. The input username and password must be the same as those configured at LAC and LNS side.

Figure 190 Connect to "Connection to 66046"



To determine the IP address assigned to your computer by the LNS, use the DOS-based command `ipconfig`.

## Client-originated VPN Networking

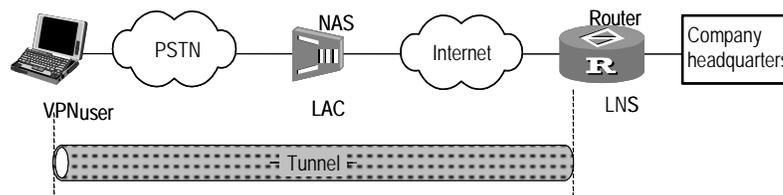
### I. Networking requirements

After connecting to the Internet, the VPN user originates request for connecting Tunnel. At receiving the request, LNS establishes a Tunnel with the VPN, so as to transmit data between the user and the company headquarters.

LAC (NAS) and LNS are connected to a 3Com router. They connect to the Internet through serial interfaces and transmit data through Tunnel. The PC named win2000 is installed with Windows2000. The Async2 interface and the PC are connected to a Modem, and the number are 660046 and 600040 separately.

### II. Networking diagram

Figure 191 Networking diagram of client-originated VPN



### III. Configuration procedure

- 1 Configuration at the LAC (NAS) side
  - a Configure the username and password (when dialing up in Windows2000)
 

```
[Router-LAC] local-user lac service-type ppp password simple lac
```
  - b Configure address pool, and assign Internet address for the user.
 

```
[Router-LAC] ip pool 1 192.170.0.3 192.170.0.100
```

- c Configure the IP address of Serial1 interface at LAC side.

```
[Router-LAC] interface serial 1
[Router-LAC-Serial1] ip address 192.167.0.2 255.255.255.0
```

- d Configure BDR parameters.

```
[Router-LAC] dialer-rule 1 ip permit
[Router-LAC] interface async 2
[Router-LAC-Async2] async mode protocol
[Router-LAC-Async2] link-protocol ppp
[Router-LAC-Async2] ip address 192.170.0.1 255.255.255.0
[Router-LAC-Async2] ppp authentication-mode chap
[Router-LAC-Async2] remote address pool 1
[Router-LAC-Async2] dialer enable-legacy
[Router-LAC-Async2] dialer-group 1
```

## 2 Configuration at the LNS side

- a Configure the username and password (when establishing VPN connection in Windows2000).

```
[Router-LNS] local-user lns_user service-type ppp password simple
lns
```

- b Define an address pool and assign a VPN address for the dialup user.

```
[Router-LNS] ip pool 1 192.168.0.3 192.168.0.100
```

- c Implement local AAA authentication on VPN user.

```
[Router-LNS] aaa-enable
[Router-LNS] aaa authentication-scheme ppp default local
[Router-LNS] aaa accounting-scheme optional
```

- d Configure the IP address of Serial0 interface at LNS side.

```
[Router-LNS] interface serial 0
[Router-LNS-Serial0] ip address 192.167.0.1 255.255.255.0
```

- e Enable L2TP service and configure a L2TP group.

```
[Router-LNS] l2tp enable
[Router-LNS] l2tp-group 1
[Router-LNS-l2tp1] tunnel name lns-end
[Router-LNS-l2tp1] allow l2tp virtual-template 1 remote win2000
```

- f Configure the Virtual-Template-related information.

```
[Router-LNS] interface virtual-template 1
[Router-LNS-Virtual-Template1] ip address 192.168.0.1 255.255.255.0
[Router-LNS-Virtual-Template1] ppp authentication-mode chap
[Router-LNS-Virtual-Template1] remote address pool 1
```

- g Disable tunnel authentication.

```
[Router-LNS-l2tp1] undo tunnel authentication
```

- h Configure the route to Windows2000.

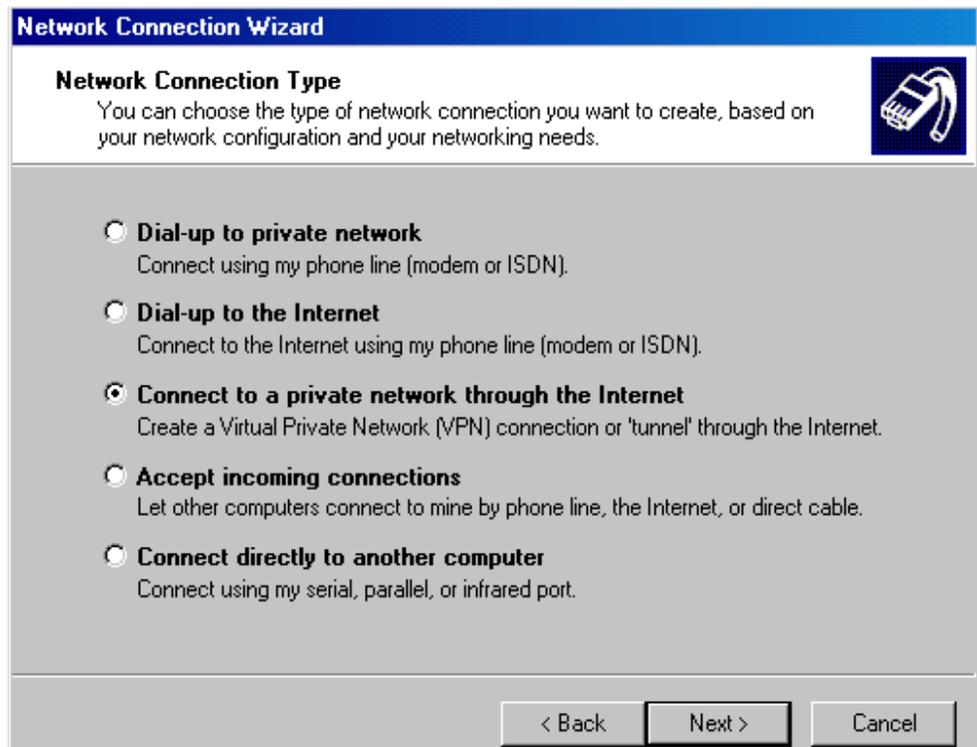
```
[Router-LNS] ip route-static 192.170.0.0 255.255.255.0 192.167.0.2
```

## 3 Configuration at the user side

- By default, IPSec is enabled in Windows2000 operation system, so the IPSec should be disabled after VPN request is originated. Execute `regedit` command in CLI mode, the [Register Editor] dialog box will pop up.

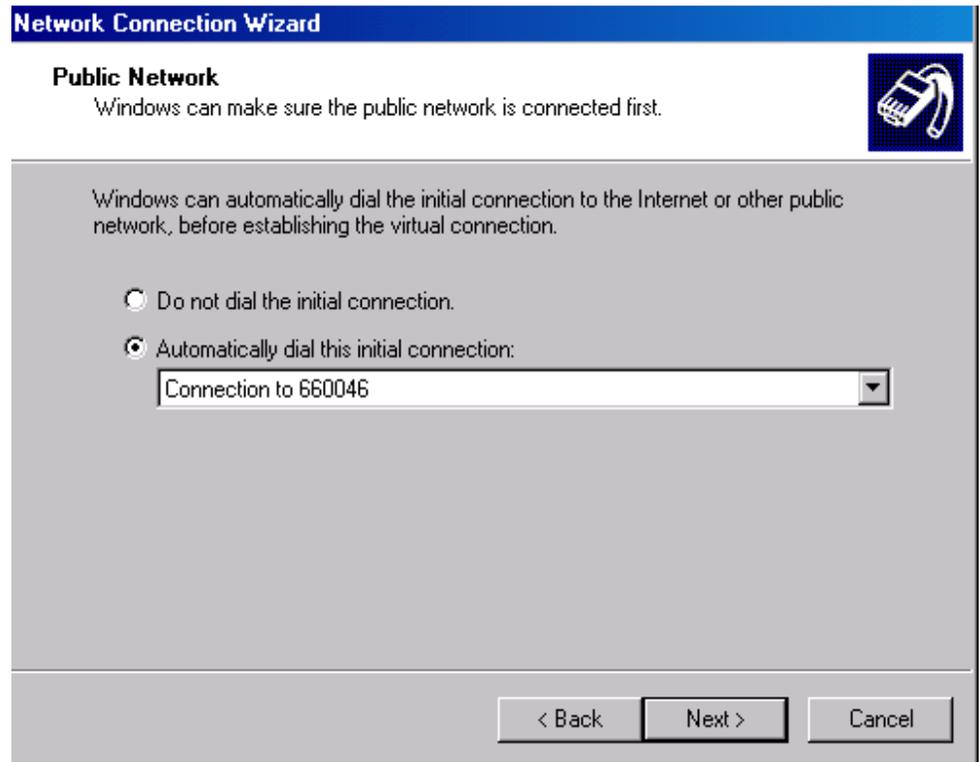
- Search for HKEY\_LOCAL\_MACHINE, System, CurrentControlSet, Services, Rasman and Parameters level by level in the register in the left. Click <Parameters>, and click in the blank space in the right window. Choose {Create/Double byte value} and create a register value (name: ProhibitIPSec, value:1), then restart Windows2000.
- Create a dialup connection and a VPN connection in Windows2000 operation system. The way to create a dialup connection is the same as that introduced in the example of “NAS-originated VPN Networking”.
- To create a VPN connection, open [Start/Program/Accessories/Network and Dialup Connection], click [New Connection], and then choose “Connect to a private network through the Internet” as the “Connection Type”, as shown in the following figure.

Figure 192 Network Connection Wizard (1)



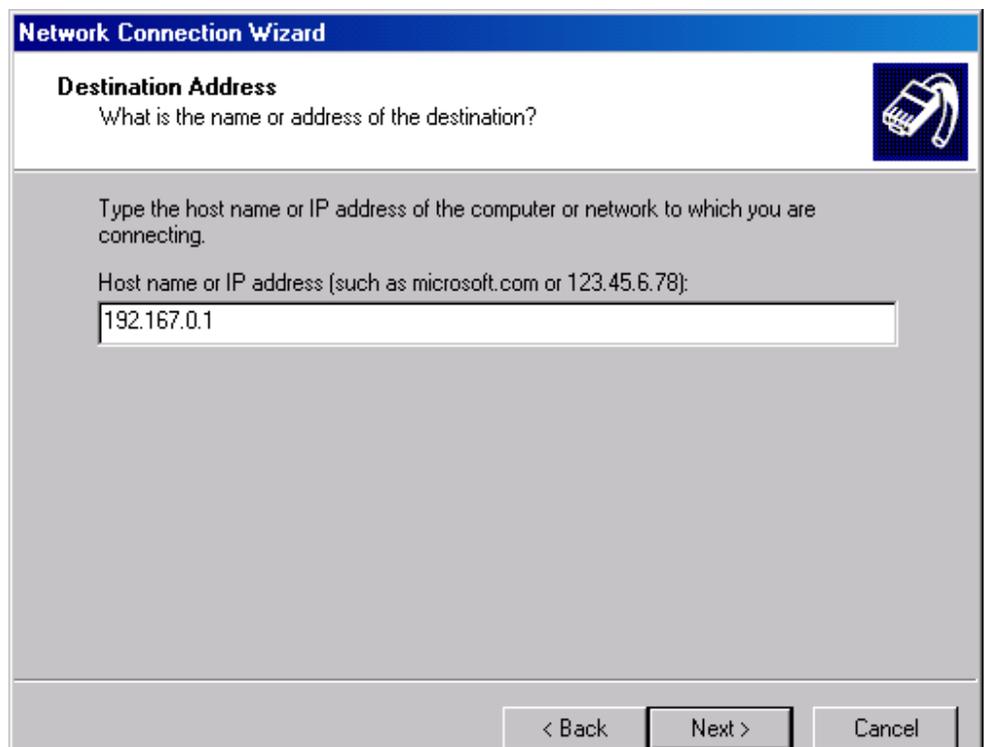
- Click <Next>, choose “Automatic dial this initial connection”, and select “Connection to 660046”, as shown in the following figure:

Figure 193 Network Connection Wizard (2)



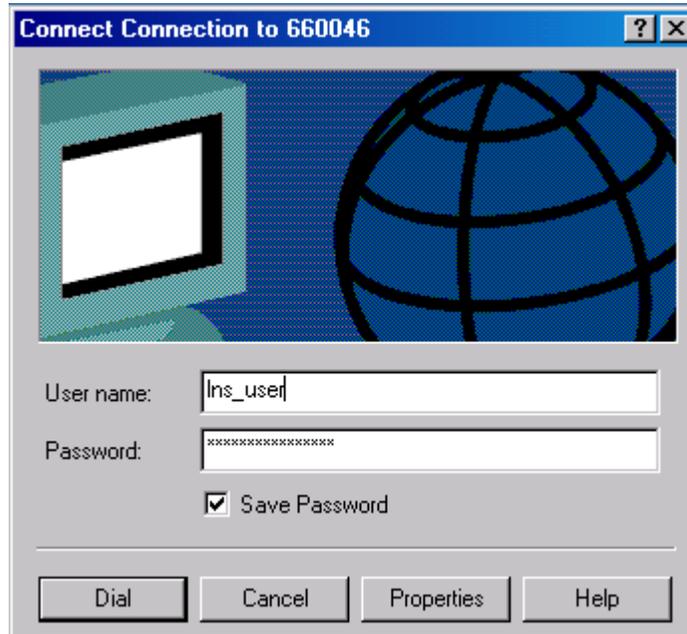
- Click <Next>, and configure the IP address of LNS in the popup dialog box (The address is the address of LNS interface connected to the Internet), as shown in the following figure.

Figure 194 Network Connection Wizard (3)



- Click <Next> to complete the configuration.
- Double click [Connect Connection to 660046] to start VPN connection. Before that, if the dialup connection is not set up, the system will automatically prompt you to set up dialup connection. After connection, input the username and password that are the same as those configured at LNS side, as shown in the following figure.

Figure 195 Connect Connection to 660046



- After the VPN is established, execute `ipconfig` command in the CLI mode of Windows2000, and then you can view the IP addresses assigned by LAC (NAS) and LNS, as shown in the following figure.

```
Windows 2000 IP Configuration
Ethernet adapter
Media State:Cable Disconnected
PPP adapter
Connection-specific DNS Suffix . . .:
IP Address.:192.168.0.3
Subnet Mask:255.255.255.255
Default Gateway:192.168.0.3
PPP adapter:
Connection-specific DNS Suffix. . .:
IP Address.:192.170.0.3
Subnet Mask:255.255.255.255
Default Gateway:192.170.0.3
```

### An Individual User Interconnects Headquarters via the Router

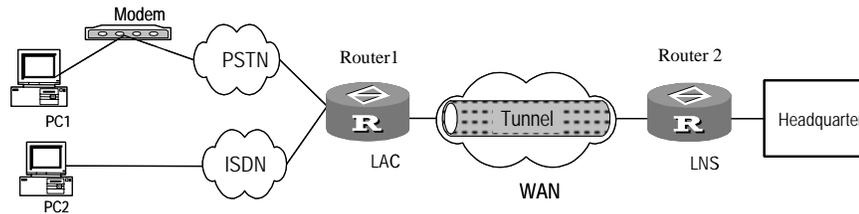
#### I. Networking requirements

A user wants to communicate with the headquarters, but the headquarters adopts a private address (e.g., 192.168.0.0), so the user cannot visit the internal server

through the Internet. Through setting up a VPN, the user can have access to the information in the internal network.

## II. Networking diagram

**Figure 196** Networking diagram of an individual user interconnecting headquarters



## III. Configuration procedure

### 1 Configuration at the user side

Set up a dialup network, with the same access number as that of Router1, and it receives the address assigned by LNS server. Input `vpduser@3Com.com` as the username and `Hello` as the password in the popup terminal window.

### 2 Configuration of Router1 (at LAC side)

Make sure to enable CHAP authentication on the access interface (e.g., dialup interface) at the LAC dialup user side.

**a** Configure the username and password.

```
[Router1] local-user vpduser@3Com.com password simple Hello
```

**b** Adopt AAA authentication.

```
[Router1] aaa-enable
[Router1] aaa authentication-scheme ppp default local
[Router1] aaa accounting-scheme optional
```

**c** Configure an IP address on Serial0 interface.

```
[Router1] interface serial 0
[Router1-Serial0] ip address 202.38.160.1 255.255.255.0
[Router1-Serial0] ppp authentication-mode chap
```

**d** Configure a L2TP group and the related attributes.

```
[Router1] l2tp enable
[Router1] l2tp-group 1
[Router1-l2tp1] tunnel name lac-end
[Router1-l2tp1] start l2tp ip 202.38.160.2 domain 3Com.com
```

**e** Enable tunnel authentication and configure a tunnel authentication password.

```
[Router1-l2tp1] tunnel authentication
[Router1-l2tp1] tunnel password simple 3Com router
```

**f** Configure the domain suffix separator to @.

```
[Router1] l2tp domain suffix-separator @
```

**g** Configure the match order to matching domain firstly and then called number.

### 3 Configuration of Router2 (at LNS side)

**a** Configure the address pool 1 which is in the range from 192.168.0.2 to 192.168.0.100.

```
[Router2] ip pool 1 192.168.0.2 192.168.0.100
```

**b** Enable AAA authentication.

```
[Router2] aaa-enable
[Router2] aaa authentication-scheme ppp default local
```

**c** Configure Virtual-Template 1.

```
[Router2] interface virtual-template 1
[Router2-Virtual-Template1] ip address 192.168.0.1 255.255.255.0
[Router2-Virtual-Template1] ppp authentication-mode chap
[Router2-Virtual-Template1] remote address pool 1
```

**d** Configure a L2TP group and the related attributes.

```
[Router2] l2tp enable
[Router2] l2tp-group 1
[Router2-l2tp1] tunnel name lns-end
[Router2-l2tp1] allow l2tp virtual-template 1 remote lac-end
```

**e** Configure the username and password that are the same as those configured at the LAC side.

```
[Router2] local-user vpdnuser@3Com.com password simple Hello
```

**f** Enable tunnel authentication and configure the tunnel authentication password to 3Com.

```
[Router2-l2tp1] tunnel authentication
[Router2-l2tp1] tunnel password simple 3Com router
```

**g** Force to implement local CHAP authentication.

```
[Router2-l2tp1] mandatory-chap
```

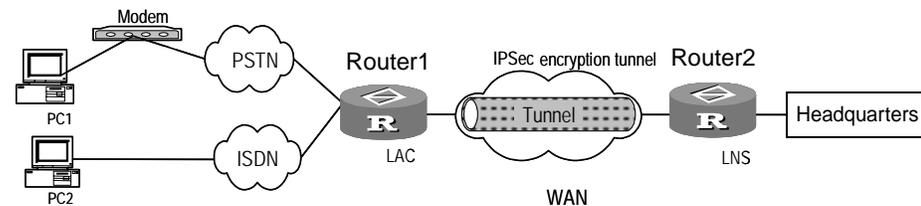
## Networking of VPN Protected by IPsec

### I. Networking requirements

To create an IPsec tunnel between the both ends of L2TP to transmit L2TP packets which are encrypted through IPsec, so as to guarantee the security for VPN.

### II. Networking diagram

**Figure 197** Networking of VPN protected by IPsec



### III. Procedures

#### 1 Configuration at the user side

Set up a dialup network whose number is the access number of Router1, and it receives the IP address assigned by the LNS server. Input "vpdnuser" as the username and "Hello" as the password in the dialup terminal window.

#### 2 Configuration at Router1 (LAC side)

**a** Configure the username and password.

```
[Router1] local-user vpdnuser password simple Hello
```

**b** Adopt AAA authentication.

```
[Router1] aaa-enable
[Router1] aaa authentication-scheme ppp default local
[Router1] aaa accounting-scheme optional
```

**c** Create an access control list and specify the encrypted L2TP data.

```
[Router1] acl 101
[Router1-acl-101] rule permit udp source 202.38.161.1 0.0.0.0
destination 202.38.161.2 0.0.0.0 destination-port equal 1701
```

**d** Create a transform view, use DES encryption and adopt a transport mode.

```
[Router1] ipsec proposal l2tptrans
[Router1-ipsec-proposal-l2tptrans] transform esp-new
[Router1-ipsec-proposal-l2tptrans] esp-new encryption-algorithm des
[Router1-ipsec-proposal-l2tptrans] esp-new auth sha1-hmac-96
[Router1-ipsec-proposal-l2tptrans] encapsulation-mode transport
```

**e** Create a crypto policy, use IKE negotiation mode and configure IKE pre-shared-key.

```
[Router1] ipsec policy l2tpmap 10 isakmp
[Router1-ipsec-policy-l2tpmap-10] ike pre-shared-key l2tp_ipsec
remote 202.38.160.2
[Router1-ipsec-policy-l2tpmap-10] match address 101
[Router1-ipsec-policy-l2tpmap-10] set peer 202.38.160.2
[Router1-ipsec-policy-l2tpmap-10] set transform l2tptrans
```

**f** Configure an IP address on Serial 0 interface and apply a IPSec policy.

```
[Router1] interface serial 0
[Router1-Serial0] ip address 202.38.160.1 255.255.255.0
[Router1-Serial0] ipsec policy l2tymap
```

**g** Configure a L2TP group and configure the related attributes.

```
[Router1] l2tp enable
[Router1] l2tp-group 1
[Router1-l2tp1] tunnel name lac-end
[Router1-l2tp1] start l2tp ip 202.38.160.2 fullusername vpdnuser
[Router1-l2tp1] undo tunnel authentication
```

**3** Configuration at Router2 (LNS side)**a** Enable AAA authentication.

```
[Router2] aaa-enable
[Router2] aaa authentication-scheme ppp default local
```

**b** Configure the username and password that should be the same as those configured at the LAC side.

```
[Router2] local-user vpdnuser password simple Hello
```

**c** Configure an address pool 1 in the range of 192.168.0.2 to 192.168.0.100.

```
[Router2] ip pool 1 192.168.0.2 192.168.0.100
```

**d** Configure an access control list and specify L2TP data.

```
[Router2] acl 101
[Router2-acl-101] rule permit udp source 192.168.0.0 0.0.0.255
destination 202.38.161.1 0.0.0.0
```

**e** Create the transform view, use DES encryption and adopt the transform mode.

```
[Router2] ipsec proposal l2tptrans
```

```
[Router2-ipsec-proposal-l2tptrans] transform esp-new
[Router2-ipsec-proposal-l2tptrans] esp-new encryption-algorithm des
[Router2-ipsec-proposal-l2tptrans] esp-new authentication-algorithm
sha1-hmac-96
[Router2-ipsec-proposal-l2tptrans] encapsulation-mode transport
```

- f Create the IPSec policy, use IKE negotiation mode and configure the IKE pre-shared-key.

```
[Router2] ipsec policy l2tpmap 10 isakmp
[Router2-ipsec-policy-l2tpmap-10] ike pre-shared-key l2tp_ipsec
remote 202.38.160.1
[Router2-ipsec-policy-l2tpmap-10] match address 101
[Router2-ipsec-policy-l2tpmap-10] set peer 202.38.160.1
[Router2-ipsec-policy-l2tpmap-10] set transform l2tptrans
```

- g Configure the IP address on Serial0 interface and apply the IPSec policy.

```
[Router2] interface serial 0
[Router2-Serial0] ip address 202.38.160.2 255.255.255.0
[Router2-Serial0] ipsec policy l2tpmap
```

- h Configure Virtual-Template 1.

```
[Router2] interface virtual-template 1
[Router2-Virtual-Template1] ip address 192.168.0.1 255.255.255.0
[Router2-Virtual-Template1] ppp authentication-mode chap
[Router2-Virtual-Template1] remote address pool 1
```

- i Configure a L2TP group and configure the related attributes.

```
[Router2] l2tp enable
[Router2] l2tp-group 1
[Router2-l2tp1] tunnel name lns-end
[Router2-l2tp1] allow l2tp virtual-template 1 remote lac-end
[Router2-l2tp1] undo tunnel authentication
```

---

## Troubleshooting L2TP

Before debugging VPN, please confirm that both LAC and LNS are on the same public network. The connectivity between them can be tested by **ping** command.

### Fault 1: The users fail to log in.

Troubleshooting:

- 1 Fail to establish the tunnel. The reasons are as follows:
  - At LAC side, the LNS address is improperly configured.
  - LNS (usually a router) is not configured to receive L2TP group of the peer of the tunnel. For details, refer to the description of the **allow l2tp** command.
  - Tunnel authentication fails. If the authentication is configured, make sure that the tunnel passwords of both sides are consistent with each other.
  - If the local end forcibly disconnects the connection and the peer fails to receive the corresponding "disconnect" message due to network transmission errors, a new tunnel connection immediately originated will not be established successfully. The reason is that the peer can only detect that the link is disconnected after a certain interval, and the tunnel connections originated by two sides with the same IP address are not allowed.
- 2 PPP negotiation fails. The reasons may be:

- Errors occur to user name and password set at LAC, or the corresponding user information is not set at LNS.
- LNS cannot allocate addresses, e.g., the address pool is set too small, or is not set at all.
- The types of tunnel password authentication are inconsistent. Given that the default authentication type of VPN connection created by Windows 2000 is MSCHAP, if the peer does not support MSCHAP, CHAP is recommended.

**Fault 2: After a tunnel is created, the data cannot be transmitted, for example, ping operation fails.**

Troubleshooting: The reasons may be as follows:

- The address of LAC is configured incorrectly: Generally, LNS distributes addresses, but LAC can also specify its own address. If the specified address and the address to be allocated by LNS are not in the same segment, this problem will occur. It is recommended that LNS allocate the addresses for LAC.
- Network congestion may occur to backbone network and a lot of packets are dropped. L2TP transmission is based on UDP (User Datagram Protocol) and UDP does not control message errors. If L2TP is adopted on the paths where line quality is not guaranteed, the **ping** command will not take effect occasionally.



# 44

## CONFIGURING GRE

This chapter covers the following topics:

- GRE Protocol Overview
- Configuring GRE
- Displaying and Debugging GRE
- GRE Configuration Example
- Troubleshooting GRE

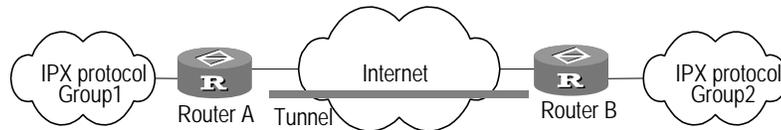
---

### GRE Protocol Overview

The Generic Routing Encapsulation (GRE) protocol encapsulates datagram of network layer protocols, such as IP and IPX, and enables these encapsulated datagrams to transmit in another network layer protocol, such as IP. GRE is a Layer 3 protocol that creates Virtual Private Network (VPN) tunnels. A tunnel is a virtual point-to-point connection and is a virtual interface that only supports point-to-point connections. It is necessary to encapsulate and de-encapsulate it when a message is transmitted on the tunnel. The interface provides a channel where the encapsulated datagram can be transmitted. The interface also encapsulates and de-encapsulates the datagram at both ends of a tunnel.

**Encapsulation** As shown in Figure 198, after receiving an IPX datagram, the interface connecting “Group1” first delivers it to be processed by the IPX protocol which checks the destination address domain in the IPX header and determines how to route the packet.

**Figure 198** Typical networking diagram of GRE



If it is found that the destination address of the message will route through the network with network number 1f (virtual network number of the tunnel), the message will be transmitted to the tunnel port with network number 1f. After receiving the packet, the tunnel port will perform GRE and then, the packet will be processed by the IP module. After IP header is encapsulated, the packet will be processed by the corresponding network interface according to the destination address and router table.

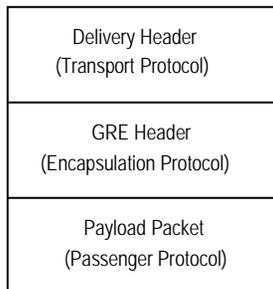
**De-encapsulation** The de-encapsulation is the opposite of encapsulation. When an IP message is received at a tunnel interface, its destination address is checked and if the router is the destination, then the IP header is removed and processed by the GRE protocol,

which examines the key, checksum or message sequence number. After the GRE header is removed, the IP message is processed by the IPX protocol in the same way as an ordinary datagram.

The system receives a datagram to be encapsulated and routed,. The datagram is first encapsulated in the GRE message so that the datagram is the payload of a GRE message. Then the datagram is encapsulated in an IP message. The IP layer forwards the message. The IP protocol that forwards the messages is often called a delivery protocol or transport protocol.

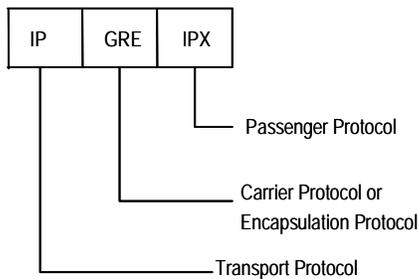
The form of an encapsulated message is shown in Figure 199:

**Figure 199** Encapsulated tunnel message format (Refer to RFC)



For example: The format of IPX transmission message that is encapsulated in an IP tunnel is as follows:

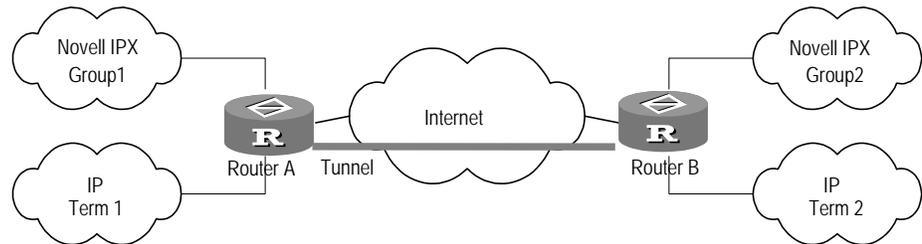
**Figure 200** Format of transmission message in the tunnel.



**GRE Services** GRE can fulfill the following services:

- 1 Implement the LAN protocol communication in WAN by encapsulating all kinds of LAN protocols into a WAN protocol.

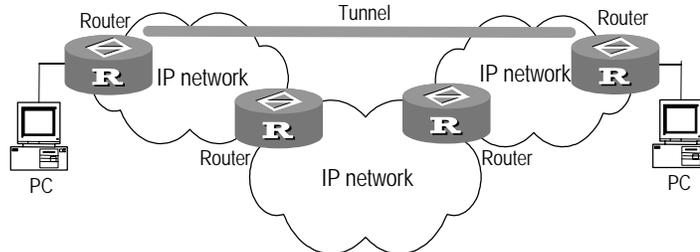
**Figure 201** Multi-protocol local network transmitting via single-protocol backbone network



In Figure 201, Group1 and Group2 are the local networks running the Novell IPX protocol. Term1 and Term2 is the local network running the IP protocol. The tunnel encapsulated by the GRE protocol is created between Router A and Router B. Thus Group1 and Group2 can communicate without affecting each other, as can Term1 and Term2.

- 2 Enlarge the operating range of the hop-limited network, such as IPX.

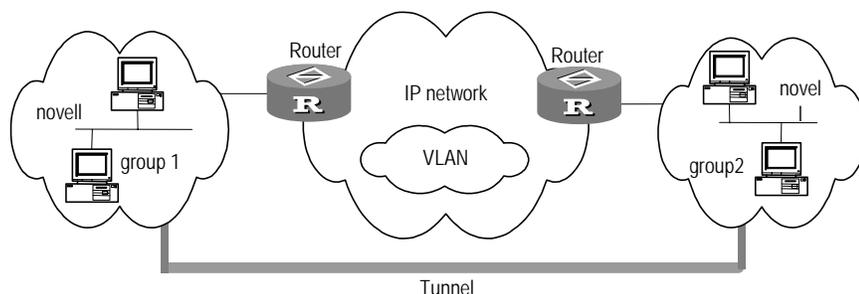
**Figure 202** Enlarge network operating range



When using RIP, if the hop count between two terminals in Figure 202 is more than 15, the two terminals cannot communicate with each other. If tunneling is used in the network, hop counts will not be incremented inside the tunnel, that is, hops can be hidden, which enlarges the operating range of the network.

- 3 Connect some discontinuous sub-networks to establish a VPN.

**Figure 203** Tunnel connecting discontinuous sub-networks



The two sub-networks group1 and group2 that are running the Novell IPX protocol are in different cities. With the tunnel available, the trans-WAN VPN can be established.

In addition, GRE also allows users to select and record an identification key word for the tunnel interface, a check of the encapsulated message, and the use of synchronous sequence numbers to ensure channel safety and correctness of transmission data.

Encapsulation and de-encapsulation on the GRE receiving side and transmitting side increases overhead cost and the increase in data volume caused by encapsulation also increases bandwidth cost. For these reasons, GRE decreases the forwarding rate of router data to some extent.

## Configuring GRE

GRE configuration includes:

- Creating a Virtual Tunnel Interface
- Setting the Source Address of a Tunnel Interface
- Setting the Destination Address of a Tunnel Interface
- Setting the Network Address of the Tunnel Interface
- Setting the Identification Key Word of the Tunnel Interface
- Setting the Tunnel Interface to Check with Checksum
- Setting the Tunnel Interface to Synchronize the Datagram Sequence Number

## Creating a Virtual Tunnel Interface

Perform the following tasks in the system view.

**Table 687** Create Virtual Tunnel Interface

| Operation                                              | Command                                      |
|--------------------------------------------------------|----------------------------------------------|
| Create virtual tunnel interface and enter tunnel view. | <b>interface tunnel <i>tunnel-number</i></b> |
| Cancel virtual tunnel interface.                       | <b>undo interface tunnel</b>                 |

By default, no virtual tunnel interface is created.

## Setting the Source Address of a Tunnel Interface

After a tunnel interface is created, the source address of tunnel channel must be configured. The source address is the address of the physical interface where the GRE packets are transmitted. The source address and destination address of the tunnel interface uniquely identifies a channel. These configurations must be implemented at both tunnel ends, and furthermore, the source address of one end must be the destination address of another end.

Perform the following settings in the tunnel interface view.

**Table 688** Set the Source Address of Tunnel Interface

| Operation                                                     | Command                         |
|---------------------------------------------------------------|---------------------------------|
| Set the source address of tunnel interface.                   | <b>source <i>ip-address</i></b> |
| Delete the configured source address of tunnel the interface. | <b>undo source</b>              |

By default, no source address of the tunnel interface is configured.

### Setting the Destination Address of a Tunnel Interface

After a tunnel interface is created, the destination address of the tunnel channel must be configured

The destination address is the address of the physical interface where the GRE packets are received. The source address and destination address of a tunnel interface uniquely identifies a channel. These configurations must be done at both tunnel ends. The source address of one end must be the destination address of the other end.

Perform the following settings in the tunnel interface view.

**Table 689** Designate the Destination Address of Tunnel Interface

| Operation                                              | Command                       |
|--------------------------------------------------------|-------------------------------|
| Designate the destination address of tunnel interface. | <b>destination ip-address</b> |
| Cancel the destination address of tunnel interface.    | <b>undo destination</b>       |

By default, no destination address of the tunnel interface is configured.

### Setting the Network Address of the Tunnel Interface

Two private networks are interconnected by a GRE tunnel. This kind of connection is like a virtual "direct" connection between two private networks. To establish a direct route between these two networks, you must configure the network address of the tunnel interface and make sure that the network addresses at both ends of the channel are in the same network segment. Thus, the system can produce a direct tunnel route automatically.

Perform the following settings in the tunnel interface view.

**Table 690** Set the Network Address of Tunnel Interface

| Operation                                   | Command                                                                                 |
|---------------------------------------------|-----------------------------------------------------------------------------------------|
| Set the IP address of tunnel interface.     | <b>ip address { ip-address mask / unnumbered interface-type interface-number }</b>      |
| Delete the IP address of tunnel interface.  | <b>undo ip address { ip-address mask / unnumbered interface-type interface-number }</b> |
| Set the IPX address of tunnel interface.    | <b>ipx network network-number</b>                                                       |
| Delete the IPX address of tunnel interface. | <b>undo ipx network</b>                                                                 |

By default, no network address for the tunnel interface is configured.

### Setting the Identification Key Word of the Tunnel Interface

It is stipulated in RFC 1701 that if the key field of the GRE header is set, the receiving side and transmitting side check the identification key word of the channel. Only when the set identification key words at both ends of the tunnel are totally identical can the check pass, or the message will be discarded.

Perform the configurations in the tunnel interface view.

**Table 691** Set the Identification Key Word of Tunnel Interface

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                                                         |                                  |
|---------------------------------------------------------|----------------------------------|
| Set the identification key word of tunnel interface.    | <b>gre key <i>key-number</i></b> |
| Cancel the identification key word of tunnel interface. | <b>undo gre key</b>              |

By default, no identification key word of the tunnel interface is configured.

### Setting the Tunnel Interface to Check with Checksum

It is stipulated in RFC 1701 that if the checksum field of the GRE header is set, the checksum is valid. The transmitting side calculates the checksums of GRE header and payload. The receiving side calculates the checksum of the received message and compares it with the checksum field in the message. If the two checksums are identical, the message will be processed, otherwise it will be discarded.

If only one end of the tunnel is configured to check with the checksum, the message will not be checked with checksum. Only when both ends of the tunnel are configured to check the checksum, the message will be checked with the checksum.

Perform the following tasks in the tunnel interface view.

**Table 692** Set Tunnel Interface to Check with Checksum

| Operation                                         | Command                  |
|---------------------------------------------------|--------------------------|
| Set tunnel interface to check with check sum.     | <b>gre checksum</b>      |
| Disable tunnel interface to check with check sum. | <b>undo gre checksum</b> |

By default, the tunnel interface to check with the field of checksum is disabled.

### Setting the Tunnel Interface to Synchronize the Datagram Sequence Number

It is stipulated in RFC 1701 that if the sequence-datagram in the GRE header is set, both the receiving side and the transmitting side will synchronize the sequence numbers. The synchronized message should be further processed, or it is discarded.

With the sequence numbers, the message is unreliable but in order. The receiving end establishes sequence numbers for the message, which is received by the local end and successfully de-encapsulated. The sequence numbers are integers between 0 and  $2^{32}-1$  and the sequence number of the first packet is 0. After the channel is established, the sequence numbers is accumulated and cyclically counted. If the receiving end receives a message whose sequence number is less than or equal to that of the message received the last time, the packet will be considered illegal. If the receiving end receives an out-of-order message, the packet will be discarded automatically.

Only when the synchronization mechanism to enable or disable sequence numbers is established at both ends of the tunnel, the channel can be established.

Perform the following tasks in the tunnel interface view.

**Table 693** Set the Tunnel to Synchronize Datagram Sequence Numbers

| Operation                                             | Command                       |
|-------------------------------------------------------|-------------------------------|
| Set tunnel interface to synchronize sequence numbers. | <b>gre sequence-datagrams</b> |

|                                                           |                                          |
|-----------------------------------------------------------|------------------------------------------|
| Disable tunnel interface to synchronize sequence numbers. | <code>undo gre sequence-datagrams</code> |
|-----------------------------------------------------------|------------------------------------------|

By default, the tunnel interface to synchronize datagram sequence numbers is disabled.

### Displaying and Debugging GRE

To view the working status of the tunnel interface, use the `display` command in all views.

**Table 694** Display and Debug GRE

| Operation                                       | Command                                                  |
|-------------------------------------------------|----------------------------------------------------------|
| Display the working status of tunnel interface. | <code>display interfaces tunnel [ tunnel-number ]</code> |

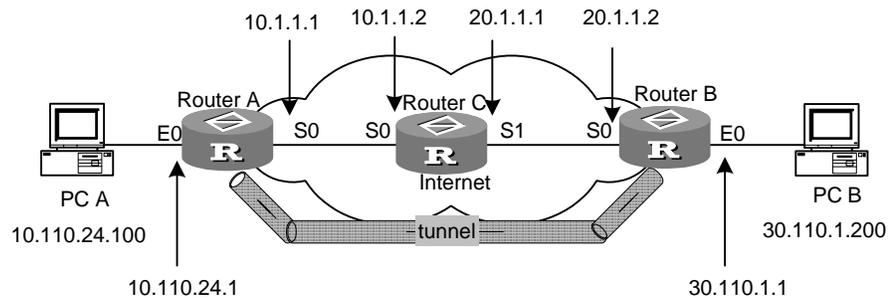
### GRE Configuration Example

#### Application of IP-over-IP GRE

VPN should be built across the WAN for the operation of Novell IPX's two subnets group1 and group2. It can be implemented by using GRE.

PC A communicates with PC B in GRE tunneling mode in the Internet. Router A and Router B are two ends of the GRE tunnel, while Router C is located in the GRE tunnel.

**Figure 204** Networking diagram of GRE application



- 1 Configure PC A and PC B:
  - a Configure the IP address of PC\_A to 10.110.24.100, add a default gateway in the network attribute (i.e., default route), or use the following command in DOS mode.
 

```
C:\WINDOWS> route add 0.0.0.0 mask 0.0.0.0 10.110.24.1
```
  - b Configure the IP address of PC\_B to 30.110.1.200, add a default gateway in the network attribute (i.e., default route), or use the following command in DOS mode.
 

```
C:\WINDOWS> route add 0.0.0.0 mask 0.0.0.0 30.110.1.1
```
- 2 Configure Router A:
  - a Configure the IP address of Serial0 interface.
 

```
[RouterA] interface serial 0
[RouterA-Serial0] ip address 10.1.1.1 255.255.255.0
```

- b** Configure the IP address of Ethernet0 interface.

```
[RouterA-Serial0] exit
[RouterA] interface ethernet 0
[RouterA-Ethernet0] ip address 10.110.24.1 255.255.255.0
```

- c** Create a virtual Tunnel interface and configure the IP address, source address and destination address.

```
[RouterA-Ethernet0] exit
[RouterA] interface tunnel 0
[RouterA-Tunnel0] ip address 1.1.1.1 255.255.255.0
[RouterA-Tunnel0] source 10.1.1.1
[RouterA-Tunnel0] destination 20.1.1.2
```

- d** Configure the routes to 20.1.1.0 network and 30.110.1.0 network.

```
[RouterA] ip route-static 20.1.1.0 255.255.255.0 serial 0
[RouterA] ip route-static 30.110.1.0 255.255.255.0 tunnel 0
```

### 3 Configure Router B:

- a** Configure the IP address of Serial0.

```
[RouterB] interface serial 0
[RouterB-Serial0] ip address 20.1.1.2 255.255.255.0
```

- b** Configure the IP address of Ethernet0 interface.

```
[RouterB-Serial0] exit
[RouterB] interface ethernet 0
[RouterB-Ethernet0] ip address 30.110.1.1 255.255.255.0
```

- c** Create a virtual Tunnel interface, and configure the IP address, source address and destination address.

```
[RouterB-Ethernet0] exit
[RouterB] interface tunnel 0
[RouterB-Tunnel0] ip address 1.1.1.2 255.255.255.0
[RouterB-Tunnel0] source 20.1.1.2
[RouterB-Tunnel0] destination 10.1.1.1
```

- d** Configure the routes to 20.1.1.0 network and 30.110.1.0 network.

```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 Serial 0
[RouterB] ip route-static 10.110.24.0 255.255.255.0 tunnel 0
```

### 4 Configure Router C:

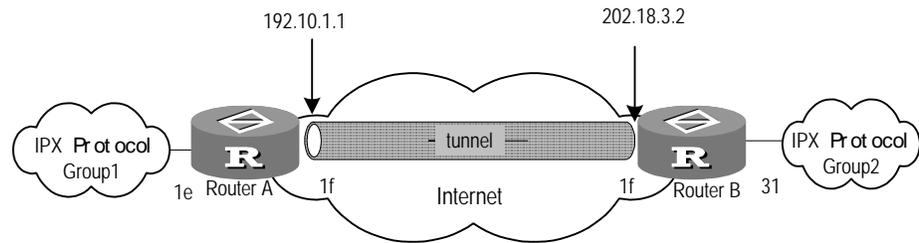
- a** Configure the IP address of Serial0 interface.

```
[RouterC] interface serial 0
[RouterC-Serial0] ip address 10.1.1.2 255.255.255.0
[RouterC-Serial0] interface serial 1
[RouterC-if-Serial1] ip address 20.1.1.1 255.255.255.0
```

#### Application of IPX-over-IP GRE

The two subnets group1 and group2 that running Novell IPX protocol need to set up a virtual private network across a LAN using GRE technology.

Figure 205 Networking of GRE



## 1 Configure Router A:

### a Activate IPX.

```
[RouterA] ipx enable node a.a.a
```

### b Configure the IP address and IPX address of Ethernet0.

```
[RouterA] interface ethernet 0
[RouterA-Ethernet0] ip address 10.1.1.1 255.255.255.0
[RouterA-Ethernet0] ipx network 1e
```

### c Configure the IP address of Serial0 interface.

```
[RouterA] interface serial 0
[RouterA-Serial0] ip address 192.10.1.1 255.255.255.0
```

### d Create a virtual tunnel interface, and configure the IP address, source address and destination address.

```
[RouterA] interface tunnel 0
[RouterA-Tunnel0] ip address 10.1.2.1 255.255.255.0
[RouterA-Tunnel0] ipx network 1f
[RouterA-Tunnel0] source 192.10.1.1
[RouterA-Tunnel0] destination 202.18.3.2
```

### e Configure the static route to Novell Group2.

```
[RouterA] ipx route 31 1f.b.b.b tick 2000 hop 15
```

## 2 Configure Router B:

### a Activate IPX.

```
[RouterB] ipx enable node b.b.b
```

### b Configure the IP address and IPX address of Ethernet0 interface.

```
[RouterB] interface ethernet 0
[RouterB-Ethernet0] ip address 10.1.3.1 255.255.255.0
[RouterB-Ethernet0] ipx network 31
```

### c Configure the IP address of Serial0 interface.

```
[RouterB] interface serial 0
[RouterB-Serial0] ip address 202.18.3.2 255.255.255.0
```

### d Create a virtual Tunnel interface, and configure the IP address, source address and destination address.

```
[RouterB] interface tunnel 0
[RouterB-Tunnel0] ip address 10.1.2.2 255.255.255.0
[RouterB-Tunnel0] ipx network 1f
[RouterB-Tunnel0] source 202.18.3.2
[RouterB-Tunnel0] destination 192.10.1.1
```

### e Configure the static route to Novell Group.

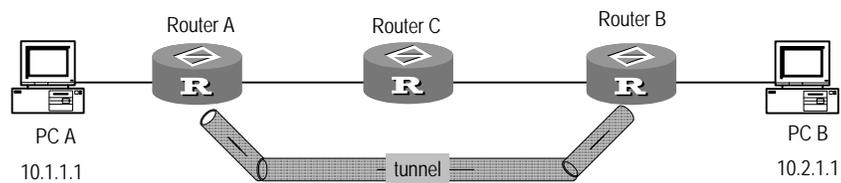
```
[RouterB] ipx route 1e 1f.a.a.a tick 30000 hop 15
```

## Troubleshooting GRE

The two interfaces at both ends of the tunnel are correctly configured and the ping operation is successful, but the ping operation between PC A and PC B fails.

Check whether there is a route passing through the Tunnel interface, that is, on Router A, the route to 10.2.0.0/16 passes through Tunnel0 interface; on Router B, the route to 10.1.0.0/16 passes through Tunnel0 interface (it is implemented by adding a static route).

**Figure 206** Networking of troubleshooting GRE



# X

## RELIABILITY

Chapter 45    Configuring a Standby Center

Chapter 46    Configuring VRRP



# 45

## CONFIGURING A STANDBY CENTER

This chapter covers the following topics:

- Standby Center Overview
- Configuring the Standby Center
- Displaying and Debugging the Standby Center
- Standby Center Configuration Examples

---

### Standby Center Overview

To enhance a network's reliability, 3Com routers provide perfect standby functions through the use of standby centers

- Interfaces that have standby are called main interfaces. Every physical interface or sub-interface on a router can serve as a main interface. A logic channel, such as X.25 or frame-relay virtual circuits, on any interface can also serve as a main interface.
- The interfaces serving as the standby for other interfaces are called standby interfaces. Any physical interface or logic channel on an interface of a router can serve as the standby interface of another interface or logic channel.
- One main interface can have several standby interfaces; if the main interface goes down work resumes on a standby interface, based on priority.
- Interfaces (such as ISDN BRI and ISDN PRI interfaces) that have multiple physical channels can provide standbys to multiple main interfaces by using dialer route.

Standby centers support the standby load sharing function. When the traffic of the all-active interfaces on the standby center reaches the set enable threshold, routers will start a standby interface with the highest priority to share the load with the started interfaces. When the traffic of all active interfaces on the standby center is less than the set disable threshold, routers close the standby interface with the lowest priority.

---

### Configuring the Standby Center

Standby center configuration includes:

- Entering the View of the Main Interface
- Specifying a Standby Interface and the Priority Used by the Main Interface
- Setting the Delay Time for Switchover between Main and Standby Interface
- Setting State-judging Conditions of the Logic Channel State
- Configuring Standby Load Sharing

### Entering the View of the Main Interface

On a 3Com router, not only every physical interface or sub-interfaces of the router, but every virtual circuit of X.25 or frame relay can work as a main interface. If the

main interface is a physical interface or sub-interface, use the following commands in system view to enter the view of the interface.

**Table 695** Enter the View of the Main Interface

| Operation                            | Command                      |
|--------------------------------------|------------------------------|
| Enter the view of the main interface | <b>interface type number</b> |

If the main interface is a virtual circuit, it should be treated differently depending on the type of the virtual circuit. First, specify its logic channel number in the view of the physical interface to which it is subordinate, then enter the corresponding logic channel view.

Use the following commands in the logical channel view.

**Table 696** Enter the Logic Channel View

| Operation                                                                         | Command                                                                                  |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Specify a logic channel number for an X.25 virtual circuit. (interface view)      | <b>x25 map protocol address x121-address<br/>x.121-address logic-channel number</b>      |
| Specify a logic channel number for a frame relay virtual circuit (interface view) | <b>fr map protocol address dlci dlci<br/>logic-channel number</b>                        |
| Specify a logic channel number for a dialer route (interface view)                | <b>dialer route protocol<br/>next-hop-address dialer-number<br/>logic-channel number</b> |
| Enter corresponding logic channel view. (system view)                             | <b>logic-channel number</b>                                                              |

### Specifying a Standby Interface and the Priority Used by the Main Interface

Any physical interface or logic channel, including a virtual circuit or dialer route, can work as a standby interface of the main interface.

Use the following commands in the view of the main interface.

**Table 697** Specify Standby Interface and Priority Used by the Main Interface

| Operation                                                                                      | Command                                           |
|------------------------------------------------------------------------------------------------|---------------------------------------------------|
| Specify a physical interface to back up the main interface; its priority can also be set here. | <b>standby interface type number [ priority ]</b> |
| Specify a logic channel to back up the main interface, its priority can also be set here.      | <b>standby logic-channel number [ priority ]</b>  |

If one main interface has multiple standby interfaces, repeat these operations. In addition, if the standby interface is a logic channel, the logic channel should be made to correspond to the actual virtual circuit or dialer route.

Please perform the following tasks in the views of the physical interface to which the virtual circuit or the dialer route belongs, and specify the corresponding logic channel number.

**Table 698** Establish a Corresponding Relation Between Logic Channel and Virtual Circuit or Dialer Route

| Operation                                               | Command                                                                             |
|---------------------------------------------------------|-------------------------------------------------------------------------------------|
| Specify a logic channel number for X.25 virtual circuit | <b>x25 map protocol address x121-address<br/>x.121-address logic-channel number</b> |

|                                                                |                                                                                          |
|----------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Specify a logic channel number for frame relay virtual circuit | <b>fr map protocol address dlci dlci<br/>logic-channel number</b>                        |
| Specify a logic channel number for Dialer Route                | <b>dialer route protocol<br/>next-hop-address dialer-number<br/>logic-channel number</b> |

### Setting the Delay Time for Switchover between Main and Standby Interface

When the state of the main interface changes from up to down, the system doesn't switch to a standby interface immediately, but waits for a preset time delay instead. The system switches to the standby interface only if the state of the main interface remains down after the delay times out. If the main interface recovers within the delay time, the system will not switch to the standby interface.

**Table 699** Set the Delay Time for the Switchover from the Main Interface to the Standby Interface

| Operation                                                                                          | Command                                   |
|----------------------------------------------------------------------------------------------------|-------------------------------------------|
| Set the delay time for the switchover from the main interface to the standby interface             | <b>standby timer enable-delay seconds</b> |
| Restore the default delay time for the switchover from the main interface to the standby interface | <b>undo standby timer enable-delay</b>    |

By default, the delay time for the switchover from the main interface to the standby interface is 0 second, meaning that the switchover is instantaneous.

When the state of the main interface changes from down to up, the system doesn't switch to the main interface immediately, but wait for a preset time delay instead. The system will switch back to the main interface only if the state of the main interface remains 'up' after the delay time runs out; if the main interface restores its down state again within the delay time, the system will not switch to the main interface.

Perform the following configurations in the view of the backed up main interface.

**Table 700** Set the Delay Time for the Switchover from the Standby Interface to the Main Interface

| Operation                                                                                          | Command                                    |
|----------------------------------------------------------------------------------------------------|--------------------------------------------|
| Set the delay time for the switchover from the standby interface to the main interface             | <b>standby timer disable-delay seconds</b> |
| Restore the default delay time for the switchover from the standby interface to the main interface | <b>undo standby timer disable-delay</b>    |

By default, the delay time for the switchover from the standby interface to the main interface is 0 second, meaning that the switchover is instantaneous.

### Setting State-judging Conditions of the Logic Channel State

When the main interface is a logic channel, the logic channel is regarded as down after a specified number of unsuccessful calls. After it switches over to the standby interface, regular inspections at specified time intervals must be made on the logic channel to check whether it has recovered.

If the main interface has multiple standby interfaces, of which one is a logic channel, it's necessary to judge whether the logic channel is down or up before opening it. If it is down, open the standby interface with the second highest

priority; after the logic channel changes to up, it's required to switch from the standby interface with the second highest priority to this logic channel.

Perform the following commands in the view of the logic channel.

**Table 701** Set the State-judging Conditions When the Main Interface is a Logic Channel

| Operation                                                                                                                                          | Command                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| Set the condition for judging the logic channel as down: the logical channel is regarded as down after the specified number of unsuccessful calls. | <b>standby state-down times</b> |
| <i>seconds</i> is set to make regular inspections so as to check whether the original logic channel has recovered its "up" state.                  | <b>standby state-up seconds</b> |

By default, *time* is set to 0 and *seconds* is set to 1 second.

### Configuring Standby Load Sharing

Conduct the following configuration under the interface view or logic channel view.

**Table 702** Configure Interface or Logic Channel Load Sharing

| Operation                                                                     | Command                                                          |
|-------------------------------------------------------------------------------|------------------------------------------------------------------|
| Configure the standby load sharing of interface or logic channel              | <b>standby threshold enable-threshold disable-threshold</b>      |
| Disable the standby load sharing configuration of interface and logic channel | <b>undo standby threshold enable-threshold disable-threshold</b> |

By default, the standby load sharing function of interface is not enabled.

### Displaying and Debugging the Standby Center

Please perform the following configuration in all views.

**Table 703** Display and Debug Standby Center

| Operation                            | Command                                     |
|--------------------------------------|---------------------------------------------|
| Turn on the standby center debugging | <b>debugging standby { event   packet }</b> |

### Standby Center Configuration Examples

This section describes several different configurations for standby centers with a suggested procedure for each configuration

#### Standby Between Interfaces

Take interface Serial 2 as the standby interface for interface Serial 1.

- 1 Enter the view of Serial 1.  
[Router]**interface serial 1**
- 2 Set Serial 2 as its standby interface.  
[Router-Serial1]**standby interface serial 2**
- 3 Set the time for switchover between main and standby interfaces as 10 seconds.  
[Router-Serial1]**standby timer enable-delay 10**  
[Router-Serial1]**standby timer disable-delay 10**

**Multiple Standby Interfaces** Take both interfaces Serial 1 and Serial 2 as the standby interface of interface Serial 0, and use interface Serial 1 as a preference.

- 1 Enter the view of Serial 0.  

```
[Router] interface serial 0
```
- 2 Set interfaces Serial 1 and Serial 2 as the standby interfaces, their priorities being 30 and 20, respectively.  

```
[Router-Serial0] standby interface serial 1 30
[Router-Serial0] standby interface serial 2 20
```

**Logical Channel Standby Interface** In this example, set interface Serial 1 as the standby interface for an X.25 virtual circuit on interface Serial 0.

- 1 Configure interface Serial 0 so that it encapsulates X.25 and specify its IP address and X.121 address.  

```
[Router] interface serial 0
[Router-Serial0] link-protocol x25
[Router-Serial0] ip address 1.1.1.2 255.0.0.0
[Router-Serial0] x25 x121-address 1
```
- 2 Match an X.25 virtual circuit on interface Serial 0 with logic channel 10.  

```
[Router-Serial0] x25 map ip 2.2.2.3 x121-address 2 logic-channel 10
```
- 3 Enter the view of logic channel 10.  

```
[Router-Serial0] logic-channel 10
```
- 4 Specify interface Serial 1 as the standby interface of this logic channel.  

```
[Router-logic-channel10] standby interface serial 1
```
- 5 Set the time interval as 10 seconds for judging the logic channel as up.  

```
[Router-logic-channel10] standby state-up 10
```

**Multiple Standby Interfaces with a Logic Channel** Take both logic channel 3 on interface Serial 1 and interface Serial 2 as the standby interfaces of logic channel 5 on interface Serial 0.

- 1 Configure that interface Serial 0 encapsulates X.25 and specify its IP address and X.121 address.  

```
[Router] interface serial 0
[Router-Serial0] link-protocol x25
[Router-Serial0] ip address 1.1.1.2 255.0.0.0
[Router-Serial0] x25 x121-address 1
```
- 2 Match an X.25 virtual circuit on interface Serial 0 with logic channel 5.  

```
[Router-Serial0] x25 map ip 2.2.2.3 x121-address 2 logic-channel 5
```
- 3 Configure that interface Serial 1 encapsulates X.25 and specify its IP address and X.121 address.  

```
[Router-Serial0] interface serial 1
[Router-Serial1] link-protocol x25
[Router-Serial1] ip address 3.3.3.4 255.0.0.0
[Router-Serial1] x25 x121-address 3
```
- 4 Match logic channel 3 with an X.25 virtual circuit on interface Serial 1.  

```
[Router-Serial1] x25 map ip 4.4.4.5 x121-address 4 logic-channel 3
```

- 5 Enter the view of logic channel 5 and set logic channel 3 and interface Serial 1 as its standby interfaces, their priorities being 50 and 20 respectively.

```
[Router-Serial1] logic-channel 5
[Router-logic-channel5] standby logic-channel 3 50
[Router-logic-channel5] standby interface serial 2 20
```

# 46

## CONFIGURING VRRP

This chapter covers the following topics:

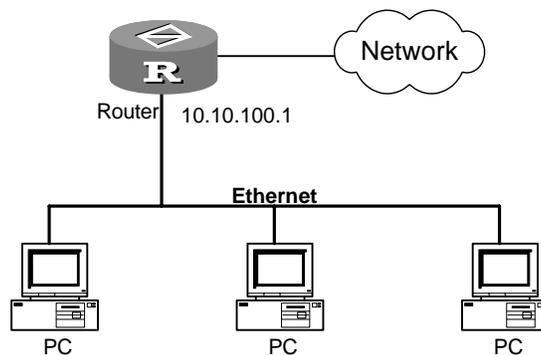
- VRRP Overview
- Configuring VRRP
- Displaying and Debugging VRRP
- VRRP Configuration Examples
- Troubleshooting VRRP

---

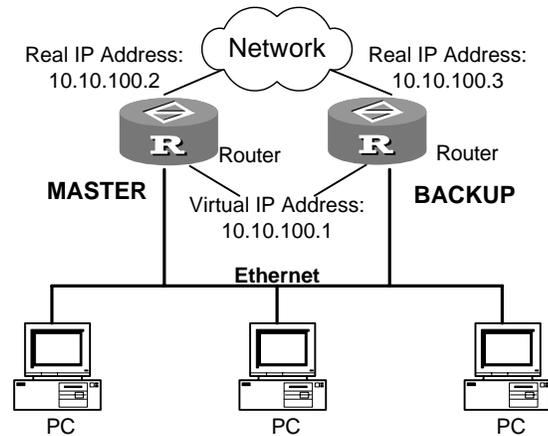
### VRRP Overview

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant protocol. In general, a default route (the next hop is 10.100.10.1) is configured for a network host so that packets sent by the host with destination addresses not in the local network segment go through the default route to Router 1 to implement communication between the host and the external network. When Router 1 breaks down, in this network segment all the hosts that regard Router 1 as the default route next-hop stop the communication with the external network.

**Figure 207** LAN networking scheme



To solve this problem, VRRP is designed for LANs with multi-casting and broadcasting capabilities, such as Ethernet. VRRP combines a group of LAN routers including a MASTER router and several BACKUP routers into a virtual router, called a standby group.

**Figure 208** Virtual router diagram

This virtual router has its own IP address: 10.100.10.1 (it can be the same as the interface address of a router within the standby group). The routers within the standby group have their own IP addresses (10.100.10.2 for the master routers and 10.100.10.3 for the backup routers). The host within the LAN only knows the IP address of this virtual router but not the specific IP addresses of the master router and the backup router. They configure their own default routes as the IP address of this virtual router. Therefore, hosts within the network communicate with the external network through this virtual router. If a master router in the virtual group breaks down, another backup router functions as the new master router to continue serving the host with routing to avoid interrupting the communication between the host and the external networks.

For the details of VRRP, refer to RFC 2338.

---

## Configuring VRRP

- Configuring VRRP includes tasks that are described in the following section:s
- Add Virtual IP Address Adding a Virtual IP Addressress
- Configuring Router Priority in a Standby Group
- Configuring Preemption Mode and Delay of Standby Group Routers
- Configuring the Authentication Method and Authentication Key
- Configure Standby Group Timer
- Monitoring the Specified Interface

### Adding a Virtual IP Address

Add one IP address of the standby group network-segment to this standby group (also called a virtual router).

Perform the following configuration in Ethernet interface view:

**Table 704** Add Virtual IP Address

| Operation                 | Command                                                               |
|---------------------------|-----------------------------------------------------------------------|
| Add Virtual IP Address    | <b>vrrp vrid virtual_router_id<br/>virtual-ip ip-address</b>          |
| Delete virtual IP address | <b>undo vrrp vrid virtual_router_id<br/>virtual-ip [ ip-address ]</b> |

The standby group numbers ranges from 1 to 255. The virtual IP address should be the address of the network segment where the interface resides. It can be an unused IP address in the network segment, or the router's own IP address. When the virtual IP address is the router's own IP address, this router is called an IP address owner. When the first IP address is added to a standby group, the system establishes this standby group. Whenever this command is executed after that, the system only adds this address to the virtual IP address list of this standby group. One router interface can be added into 14 standby groups at the same time, while one standby group can configure up to 16 virtual IP addresses. Before performing other configurations for one standby group, this command must be used first to establish this standby group.

Multiple virtual IP addresses (multiple virtual routers) can be configured in one standby group. All the virtual addresses take effect at the same time, and the computers in the LAN can choose any of the virtual routers as their gateway. The **undo vrrp virtual-ip** form of the command can delete one existing standby group or delete one virtual IP address from the virtual address list on a standby group.

After the last virtual IP address has been deleted from the standby group, this standby group is also deleted. Then this standby group no longer exists on this interface and all the configurations of this standby group are no longer valid.

### Configuring Router Priority in a Standby Group

The status of each router in a standby group can be determined by its priority in VRRP. The router with the highest priority becomes the master. Those with the same priority are judged by comparing the master IP addresses of their interfaces.

The range of priority is 0 to 255 (the bigger the number, the higher the priority) with 100 as the default. However the range to be configured is from 1 to 254. Priority 0 is reserved for special use by the system and 255 is reserved for the IP address owner.

Perform the following configuration in Ethernet interface view:

**Table 705** Configure Router Priority in Standby Group

| Operation                                   | Command                                                  |
|---------------------------------------------|----------------------------------------------------------|
| Configure the priority of the standby group | <b>vrrp vrid virtual_router_id priority<br/>priority</b> |
| Restore the default value of the priority   | <b>undo vrrp vrid virtual_router_id<br/>priority</b>     |



*The priority for IP address owners cannot be configured and it always remains 255.*

### Configuring Preemption Mode and Delay of Standby Group Routers

Once a router in the standby group becomes the master router, so long as it still functions properly, other routers, even configured with higher priority later, cannot become the master router unless they are configured with preemption mode. The router in preemption mode becomes the master router if it finds its own priority is higher than that of the present master router. Accordingly, the former master router becomes the backup router.

Along with preemption mode, delay can also be configured. This delays the coming of the point when the backup router becomes the master router. The purpose for this is: in an unstable network if the backup router has not received the packets from the master router punctually, it will become the master router (failure of backup to receive the packets may be due to network congestion, not due to malfunction of the master router). Therefore, a delay insures the reception of the packet from the master router and thus avoids frequent state switches.

The default mode is preemption without delay. The delay is set in seconds, ranging from 1 to 255.

Perform the following configuration in Ethernet interface view:

**Table 706** Configure Preemption Mode and Delay of Standby Group Routers

| Operation                                                  | Command                                                                 |
|------------------------------------------------------------|-------------------------------------------------------------------------|
| Configure the preemption mode and delay for standby group. | <b>vrrp vrid virtual_router_id preempt-mode [ timer-delay seconds ]</b> |
| Delete preemption mode                                     | <b>undo vrrp vrid virtual_router_id preempt-mode</b>                    |

### Configuring the Authentication Method and Authentication Key

VRRP provides simple character authentication method.

In a secure network, authentication can be configured to No, which means no authentication will be conducted by the router to the VRRP packets being sent out. And the router receiving the VRRP packets will take them as true and legal without any authentication. In this case no authentication key is needed.

In a network under possible security threat, the authentication method can be configured to **simple**. That means the router sending out the VRRP packets fills the authentication key into the VRRP packets, while the router receiving the VRRP packet will compare the authentication key of the packet with the locally configured authentication key. If they are the same, the packet will be taken as a true and legal one. Otherwise, it will be regarded as an illegal packet to be discarded. In this case, an authentication key of less than 8 bits will be configured.

Perform the following configuration in Ethernet interface view:

**Table 707** Configure Authentication Method and Authentication Key

| Operation                                              | Command                                        |
|--------------------------------------------------------|------------------------------------------------|
| Configure authentication method and authentication key | <b>vrrp authentication-mode simple [ key ]</b> |
| Disabled VRRP authentication                           | <b>undo vrrp authentication-mode simple</b>    |



*The same authentication method and authentication key should be configured for the standby group of an interface.*

### Configure Standby Group Timer

The master router of a VRRP standby group notifies its normal operation state to the routers within the group by sending them VRRP packets regularly (*adver\_interval*). If the backup routers fail to receive the VRRP packets over a certain period of time (*master\_down\_interval*), they reach the conclusion that the master routers are not functioning properly and will change their own state to master.

The user can adjust the master routers' sending interval (*adver\_interval*) of VRRP packets by configuring the timer command. The *master\_down\_interval* of the backup routers are three times that of the *adver\_interval*. Too much network traffic or the differences of different router timers will result in abnormal *master\_down\_interval* and state switchover. Such problems can be solved through prolonging the *adver\_interval* and configuring delay time.

Perform the following configuration in interface view:

**Table 708** Configure VRRP Timer

| Operation                               | Command                                                          |
|-----------------------------------------|------------------------------------------------------------------|
| Configure VRRP timer                    | <code>vrrp vrid virtual_router_id timer-advertise seconds</code> |
| Restore the default value of VRRP timer | <code>undo vrrp vrid virtual_router_id timer-advertise</code>    |

By default *adver\_interval* is set 1 seconds, namely, the default value of *adver\_interval* is 1 second, while the default value of *master\_down\_interval* is 3 seconds.

### Monitoring the Specified Interface

The interface monitoring function of VRRP expands backup function: when the interface of the router is unavailable, it is regarded that the router is not stable, hence it should not act as a master router. After the interface monitoring function is set, the router's priority will be adjusted dynamically according to the state of the interface that is under monitoring. Once the monitored interface becomes unavailable, the priority value of this router is reduced, so that another router with a more stable interface state in the same backup group can act as a master router more easily.

Perform the following configuration in Ethernet interface view:

**Table 709** Configure Monitoring Interface

| Operation                                        | Command                                                                                             |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Set to monitor the specified interface           | <code>vrrp vrid virtual_router_id track interface_type interface_number [ reduced priority ]</code> |
| Cancel the monitoring of the specified interface | <code>undo vrrp vrid virtual_router_id track interface_type interface_number</code>                 |

By default *interface-priority* is 10.

**Table 710** Display and Debug VRRP

| Operation                      | Command                                  |
|--------------------------------|------------------------------------------|
| Display VRRP State Information | <b>display vrrp</b>                      |
| Enable the debugging of VRRP   | <b>debugging vrrp { packet   state }</b> |

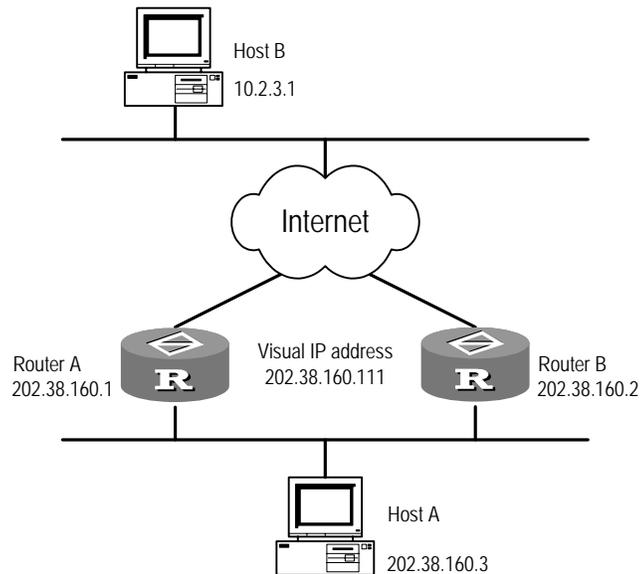
## VRRP Configuration Examples

This section describes several different configurations of VRRP with a suggested procedure for each configuration

### VRRP Single Standby Group

Host A uses the VRRP standby group which combines router A and router B as its default gateway to visit host B on the Internet.

A VRRP standby group consists of the following parts: standby group number 1, virtual IP address 202.38.160.111, router A as the MASTER and router B as the backup with preemption all. Networking diagram

**Figure 209** VRRP application illustration

#### 1 Configure router A:

```
[Router-Ethernet0] vrrp vrid 1 virtual-ip 202.38.160.111
[Router-Ethernet0] vrrp vrid 1 priority 120
```

#### 2 Configure router B:

```
[Router-Ethernet0] vrrp vrid 1 virtual-ip 202.38.160.111
```

The standby group can be used immediately after configuration. The default gateway of host A can be set as 202.38.160.111.

Under normal conditions, router A functions as the gateway, but when router A is turned off or malfunctioning, router B will function as the gateway instead.

The configuration of preemption mode is aimed for router A to resume its gateway function as the master when it recovers.

## VRRP Monitoring Interface

As shown in Figure 209, even when router A is still functioning, it may want router B to function as a gateway when the Internet interface connected with it does not function properly. This can be implemented by configuring the monitoring interface.

To facilitate explanation, the standby group number is set as 1 with configuration of authorization key and timer added (which are unnecessary in this application).

### 1 Configure router A:

```
[Router-Ethernet0] vrrp vrid 1 virtual-ip 202.38.160.111
[Router-Ethernet0] vrrp vrid 1 priority 120
[Router-Ethernet0] vrrp authentication-mode simple 3Com Router
[Router-Ethernet0] vrrp vrid 1 timer-advertise 5
[Router-Ethernet0] vrrp vrid 1 track serial0 reduced 30
```

### 2 Configure router B:

```
[Router-Ethernet0] vrrp vrid 1 virtual-ip 202.38.160.111
[Router-Ethernet0] vrrp authentication-mode simple 3Com Router
[Router-Ethernet0] vrrp vrid 1 timer-advertise 5
```

Under normal conditions, router A functions as the gateway, but when the interface Serial0 of router A is malfunctioning, its priority will be reduced by 30, lower than that of router B so that router B will preempt to function as master for gateway services instead.

When Serial0, the interface of router A, recovers, this router will resume its gateway function as the master.

## Multiple Standby Groups Configuration

One 3Com router is allowed to function as the standby router for many standby groups. See Figure 209.

Such a multi-backup configuration can implement load balancing. Some hosts (like host A) use hot standby group 1 as their gateways, some other hosts (like host B) use hot standby group 2 as their gateways. In this way, both data stream balancing and mutual backup are implemented.

### 1 Configure router A:

```
[Router-Ethernet0] vrrp vrid 1 virtual-ip 202.38.160.111
[Router-Ethernet0] vrrp vrid 1 priority 120
[Router-Ethernet0] vrrp vrid 2 virtual-ip 202.38.160.112
```

### 2 Configure router B:

```
[Router-Ethernet0] vrrp vrid 1 virtual-ip 202.38.160.111
[Router-Ethernet0] vrrp vrid 2 virtual-ip 202.38.160.112
[Router-Ethernet0] vrrp vrid 2 priority 120
```

---

## Troubleshooting VRRP

As the configuration of VRRP is not very complicated, almost all the malfunctions can be located through checking the information of configuration and debugging. Explanations are made of common failures trouble-shooting in the following part.

**The console frequently displays messages about configuration mistakes.**

This shows that a mistaken VRRP packet has been received. One reason may be inconsistent configuration of another router within the standby group. Another reason may be the attempt of some devices to send out illegal VRRP packets.

The first possibility can be solved through modifying the configuration. The second possibility is caused by the malicious attempt of some devices so non-technical measures should be attempted.

**Many master routers exist within the same standby group.**

There are also 2 reasons. One is short coexistence of many master routers, which is normal and needs no manual intervention. Another is the long coexistence of many master routers, which may be caused by failure to receive VRRP packets between master routers, or the reception of illegal packets.

To solve these problems, try to ping the many master routers. If that fails, it indicates faults in the links between routers and it is necessary to check the links. If they can be pinged through, it indicates that the problems may be caused by an inconsistent configuration. For the configuration of the same VRRP standby group, complete consistency for the number of virtual IP addresses, each virtual IP address, timer interval and authentication method must be guaranteed.

**There is frequent switchover of the VRRP state.**

Such problems are generally caused by standby group timer intervals that are too short. To solve this problem, extend this interval or configure the preemption delay.

# XI

## QoS

- Chapter 47 QoS Overview
- Chapter 48 Traffic Policing, Traffic Shaping and Line Rate
- Chapter 49 Congestion Management
- Chapter 50 Congestion Avoidance



This chapter covers the following topics:

- What Is QoS?
- Three Types of QoS Services
- Benefits of QoS for the Network Service

---

## What Is QoS?

In the traditional IP network, all the packets are treated identically. Each router has to handle these packets a following first in first out (FIFO) policy. That is, it makes best effort to transmit the packets to the destination without considering the throughput, delay, jitter, drop rate of the packets, etc. This may be advantageous or disadvantageous, depending on the conditions of the network. With the rapid development of the computer networks, the voice, image, and important data that are sensitive to the bandwidth, delay and jitter are simultaneously transmitted over the network, which enrich the network resources. However, at the same time, there are more strict requirements for the network transmission data quality. They expect that a certain service guarantee in terms of the throughput, delay, delayed jitter, and packet loss ratio of the packets can be obtained, and that different services may be provided on the basis of the client types. One way to solve these problems is to increase the bandwidth of the network, however, the increase in bandwidth is so limited and so expensive that it only relieves this problem to some extent. The provision of QoS is the basic requirements for future IP networks.

Quality of Service (QoS) refers to a series of technology integrations to obtain the expected service level with respect to the throughput, delayed jitter, delay, and packet loss ratio for users. In short, QoS is the network service that provides different service qualities that meet various kinds of demands.

---

## Three Types of QoS Services

Generally, the services of QoS are usually divided into the following three types:

- **Best-effort service:** This is the default service model provided by IP. It uses a FIFO (first in, first out) queue, offers the most primitive service of "routing-forwarding", and provides no guarantee for delay and reliability. It can satisfy most early networks' requirement (e.g., FTP, E-mail), but cannot provide high quality services for the developing voice and multimedia services.
- **Integrated service:** This model is usually applied on the edge routers. In this model, before sending a packet, it is necessary to apply for network resource and service quality through signal. After the confirmation of Resource Reservation Protocol (RSVP), the packets can be sent, and the size of the traffic is not larger than the preset traffic parameters.

- **Differentiated service:** This is a kind of multi-service model oriented to different demands. It sorts the services into classes, and provides different qualities of services according to the various classes without the support of signal. Differentiated service adopts the following technologies:
  - Traffic policing: Performing the traffic policing for one or more or all flows.
  - Traffic shaping: Performing the traffic shaping for one or more or all flows.
  - Queue management: Performing congestion management for the queues on the interface by employing the technologies such as FIFO, Priority Queue (PQ), Customized Queue (CQ), Weighted Fair Queue (WFQ), Class-based Weighted Fair Queue (CBWFQ).
  - Congestion avoidance: It is a traffic control mechanism that, by monitoring the usage of the network resources (such as the queue or memory buffer), removes the network overload by dropping packets on its own initiative to adjust the network traffic in case of network congestion.

The QoS of the 3Com router is implemented based on the differentiated service, and has the following functions:

- **Packet classification:** The services with different service quality requirements are classified in the network edge. It is processed according to different packet classifications in the core network.
- **Traffic policing:** Two token buckets are used to indicate the allowable burst levels. Tokens are placed into each bucket at the same rate (CIR). The CBS (the C bucket) is generally smaller than EBS (the E bucket). When traffic conformance is being evaluated, if the C bucket has sufficient tokens, the traffic is said to conform to allowable burst levels. If the C Bucket is short of tokens but the E bucket has sufficient tokens, the traffic partially conforms to allowable burst levels. If both the C and E buckets are short of tokens, the traffic does not conform to the allowable burst levels.
- **Traffic shaping:** Performs the shaping on the flows that do not conform to the predetermined traffic characteristics, to facilitate the bandwidth matching. It may perform the shaping on each flow or all flows on the interface.
- **Interface Line Rate:** Provides a management approach to the network bandwidth by limiting the physical interface bandwidth.
- **Congestion management:** Provides various queue mechanisms to relieve and dispatch the congested packets when the interface congestion occurs.
- **Congestion avoidance:** Takes measures to avoid the congestion by estimating the congestion status of the network. The congestion avoidance may reduce the packet loss ratio and improve the efficiency of the network availability.

---

### Benefits of QoS for the Network Service

QoS can provide controllable and predictable services for network applications and network traffic. Using QoS in the network can realize:

- Control of network resources. The user can control the usage of network resources. For example, the user may limit the bandwidth resource consumed in the FTP transmission on a connection, or provide higher priority for the data that are more important.

- Adjustable network service. If the user is ISP, by using QoS, the adjustable network services of different priority levels can be provided to various types of clients.
- Secure network services for specific data flows. For example, it can ensure that the multimedia data flows and voice flows sensitive to the delay will acquire the service in time.



---

## Traffic Classification Overview

Traffic classification means classifying packets into multiple priority levels or multiple service types according to the ToS (Type of Service) of IPv4 packet header. The other two values are reserved for other uses. After the packets are classified, QoS will be applied to different classifications respectively.

The network administrator sets the packet classification rules which define the specific flow according to the source address, source port number, protocol number, destination address, destination port number. Packet classification rules can also perform the classification based on the MAC address.

The specific classification examples are as follows:

- All the packets received from the specified interface are set to the highest priority.
- All FTP traffic is classified at a low priority.
- Video traffic sent from specific IP addresses are classified at a medium priority level.

The traffic flow to the specific destination addresses are classified at a high priority level.

---

## Traffic Policing Overview

An Internet service provider (ISP) must control the traffic and load sent by users in the network. For an enterprise network, if the control can be performed on the traffics of some applications, it must be an effective method for controlling the network conditions.

The typical function of traffic policing is to limit traffic that enters the network to an allowable range by supervising its specification. If the packet traffic of a certain connection is too large, the packet is dropped or the priority level of the packet is specified. For example, an HTTP packet may be limited to less than 50% of the network bandwidth to save network resources and protect the benefits of operators.

The committed access rate (CAR) is a technology that polices the network traffic that enters an ISP, including the flow classification service of the policed traffic. CAR classifies the packets by using the ToS field of the IP v4 header, and takes actions for different classes of traffic. Such actions may be:

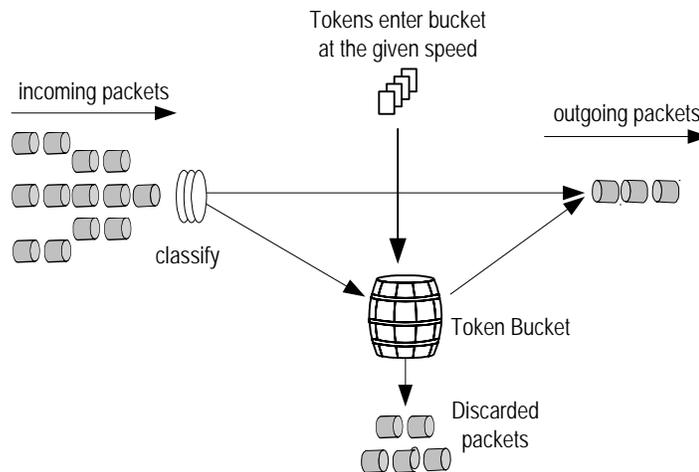
- Forwarding directly — CAR continues to forward the packets that "conform to" the traffic specifications.

- Dropping directly — CAR drops the packets that do not "conform to" the traffic specifications.
- Forwarding after modifying the packet priority level — The packets with the estimated result of "partial conformance" are forwarded after they are marked as the lower priority level flows.
- Entering the next level of policing — Traffic policing may be stacked level by level, and each level concerns and polices more specific targets. A downstream network can receive the estimated result from an upstream network, or it can be classified according to its own standard.

Traffic policing uses the Token Bucket algorithm, and each service has tokens which are transmitted at a specified rate. If the reaching speed of the user packets is faster than the speed at which the tokens are transmitted, it is necessary to take measures for the data exceeding the specified rate, for example, they are marked and allowed to pass through the network only when the network is not congested and they are dropped first when the network is congested. These data packets can also be dropped directly, which is completely dependent on the agreement and rules between the operators and users.

**Token bucket feature** The token bucket may be regarded as a container that stores tokens. The system puts tokens into the bucket at the set speed. When the bucket is full of tokens, the excessive tokens overflow, and the number of the tokens in the bucket does not increase.

**Figure 210** Schematic diagram of packet line classification and traffic policing



**Measuring the traffic by the token bucket** Evaluating the traffic specification by the token bucket is based on whether the number of the tokens in the token bucket is enough for packet forwarding. If the bucket has sufficient tokens to forward packets, the traffic does not exceed the specification, otherwise, it exceeds the specification. Usually, one token is associated with one bit of forwarding authority.

Three main parameters are used in the evaluation of the traffics:

- Time Interval: Evaluates the traffic in every other period. This parameter is set by the system. For every evaluation, if the bucket has sufficient tokens to be used by one or more packets, it is considered "in conformance". If the bucket

does not have sufficient tokens, it is considered "out of conformance". "Conformance" indicates that the traffic does not exceed the limit--at this time, the number of tokens that correspond to the "conformance" limit can be used and "nonconformance" indicates that the number of tokens that are being used is beyond the specification.

- Burst size: Indicates the capacity of the token bucket. It is usually set to committed burst size (CBS) which is the allowable maximum traffic size in every evaluation time interval. The burst size must be set to a size larger than the maximum length of the packet.
- Average rate: Specifies the rate at which tokens are put into the bucket. It is usually set to the committed information rate (CIR) or the allowable average speed of the flows.

**Complex evaluation** If there is only one token bucket, the evaluation result is limited to "conformance" and "nonconformance".

To evaluate more complex situations and implement more flexible adjusting and controlling rules, two token buckets can be set. For example, the committed access rate (CAR) has three parameters:

- Committed Information Rate (CIR): The long period average rate, at which the service quality of the transmitted data can be completely guaranteed.
- Committed Burst Size (CBS): The burst data traffic size before the amount of some traffic exceeds the line rate. At this rate, the service quality of the data can be guaranteed.
- Excess Burst Size (EBS): The burst data traffic size before the amount of all traffic exceeds the line rate. At this rate, the service quality of the data cannot be guaranteed.

With two token buckets, the rates for putting in the tokens are the same, that is, CIR. While they are in different size--respectively CBS and EBS ( $CBS < EBS$ , both of the buckets are briefly called C bucket and E bucket respectively), which refer to the different allowable burst levels. Every time for evaluation, based on the cases of "C bucket has sufficient token", "C bucket is short of tokens and E bucket has sufficient tokens" and "both C and E buckets are short of tokens", the evaluation results are "conformance", "partial conformance", and "nonconformance".

---

## Committed Access Rate (CAR)

The functions provided by the committed access rate (CAR) technology include the execution of classification service and the execution of traffic policing by line rate. It is an approach to perform traffic policing. With CAR classification service, you can sort the packets into different classes, and handle the packets of different classes in different ways.

The user can use the priority fields in the ToS domain of the IP packet header to define up to six types of services. The rules used to classify the packets can be based on the following features:

- Physical port
- Source IP address
- Source MAC address

- Destination IP address
- Destination MAC address
- Application port
- IP protocol type
- Other standards that may be identified through the access list and extended access list.

The packets can also be classified based on the external conditions of the network. For example, the client types may classify the packets. After the packet is classified, the user can apply the ACL or CARL on a specified interface and set the corresponding actions for the interface, such as rate limiting (to specify CIR, CBS, EBS), discard, resetting priority and direct forwarding.

CAR adopts the following two types of rules:

- IP access control list (standard access control list or extended access control list)
- CAR rule list (CARL, when defining CARL, you can perform traffic classification according to IP priority and MAC address).

The CAR rules can be independent of each other. That is, each CAR rule reacts to a certain type of the packets separately. A cascade of CAR rules can also be used in which a packet is matched with successive CAR rules.

Multiple CAR rules can be used on an interface. The router can attempt to match the CAR rules in configured order until it matches one successfully. If no matched rules are found, rate limiting is not implemented.

## CAR Configuration

CAR configuration includes:

- Defining Rules
- Applying the CAR Policy on the Interface
- Displaying and Debugging CAR

### Defining Rules

On the network border, it is necessary to classify the packets. The classification standards can set varied priorities for the varied classifications of either all the packets received from a specified interface or a group of packets defined by the **rule** command. Inside a network, the modified priority can be used as the classification standard. At the same time, for the packets of each category, different processing can be defined for those exceeding and those not exceeding the traffic limit in a unit time.

Please perform the following configurations in the system view.

**Table 711** Define CAR Rules

| Operation           | Command                                                                            |
|---------------------|------------------------------------------------------------------------------------|
| Define the CAR rule | <code>qos carl carl-index { precedence precedence-value / mac mac-address }</code> |
| Delete the CAR rule | <code>undo qos carl carl-index</code>                                              |

| Operation                                  | Command                                                                                                                                                                                                                                                                                      |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enter the acl view                         | <code>acl acl-number [ match-order config   auto ]</code>                                                                                                                                                                                                                                    |
| Configure the extended access control list | <code>rule { normal   special } { permit   deny } pro-number [source source-addr source-wildcard   any ] [ destination dest-addr dest-wildcard   any ] [source-port operator port1 [ port2 ] ] [destination-port operator port1 [ port2 ] ] [icmp-type icmp-type icmp-code] [logging]</code> |

By default, no CAR rule of ACL list is established.



*For the same carl-index, only one CAR rule can be defined. The later defined CAR rule will overwrite the earlier CAR rule. However, multiple CAR rules with different carl-index may be defined.*

*Before the CAR rule is configured, fast forwarding must be disabled.*

### Applying the CAR Policy on the Interface

The CAR policy can take effect on the incoming and outgoing directions of the interface. For the packets conforming to CAR rules or ACL rules, the CAR policy can limit their rates.

Perform the following configurations on the interface view.

**Table 712** Apply the CAR Rule on the Interface

| Operation                                                  | Command                                                                                                                                                                         |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apply the CAR policy or ACL rule on the interface          | <code>qos car { inbound   outbound } { any   acl acl-index   carl carl-index } cir committed-rate cbs burst-size ebs excess-burst-size conform action exceed action</code>      |
| Delete the CAR policy or ACL rule applied to the interface | <code>undo qos car { inbound   outbound } { any   acl acl-index   carl carl-index } cir committed-rate cbs burst-size ebs excess-burst-size conform action exceed action</code> |

By default, no CAR policy or ACL is applied to any interface.

On one interface (**inbound** or **outbound** directions), multiple CAR policies can be applied. However, on each interface (both **inbound** and **outbound** directions), a total of 100 CAR policies can be applied. Up to 100 CAR policies can be applied on one interface (**inbound** and **outbound** directions).

You must disable fast forwarding before applying the CAR policies.

## Displaying and Debugging CAR

**Table 713** Display and Debug CAR

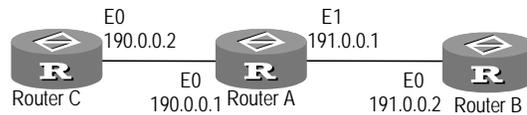
| Operation                                                                                            | Command                                                |
|------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Display one or all carl                                                                              | <code>display qos carl [ carl-index ]</code>           |
| Display the parameter configuration and operation statistic information of CAR on various interfaces | <code>display qos car [ interface type number ]</code> |

### CAR Configuration Examples

#### Applying a CAR Policy to all Packets

- The CAR policy is applied to all the packets that are input to router A Ethernet0, directly forwarding the packets that meet the conditions and dropping the packets that do not meet the conditions.
- The CAR policy is applied to all the packets that are output from router A Ethernet1, directly forwarding the packets that meet the conditions and dropping the packets that do not meet the conditions.

**Figure 211** Networking diagram of configuring the CAR policy to be applied to all packets



#### 1 Configure Router A:

CAR policy is applied to all the packets that are input to router A Ethernet 0

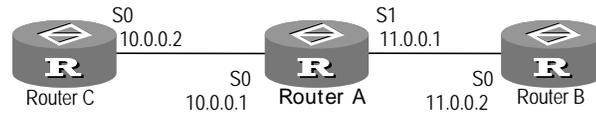
```
[RouterA-Ethernet0] ip address 190.0.0.1 255.255.255.0
[RouterA-Ethernet0] qos car inbound any cir 8000 cbs 15000 ebs 8000
conform pass exceed discard
```

CAR policy is applied to all the packets that are output from router A Ethernet 1

```
[RouterA-Ethernet1] ip address 191.0.0.1 255.255.255.0
[RouterA-Ethernet1] qos car outbound any cir 8000 cbs 15000 ebs 8000
conform pass exceed discard
```

#### Configure the Priority Level Based CAR Policy

- The packet that is input to router A serial interface 0 are matched with the priority level based on CAR policy, directly forwarding the packet that meets the conditions and dropping the packet that does not meet the conditions.
- The packet that is output from router A serial interface 1 is matched with the priority level based on CAR policy, directly forwarding the packet that meets the conditions and dropping the packet that does not meet the conditions.

**Figure 212** Networking diagram of configuring the priority level based CAR policy**1** Configure Router A:

The CAR policy is applied to the packet inputted to router A serial interface 0 and matching priority level 1.

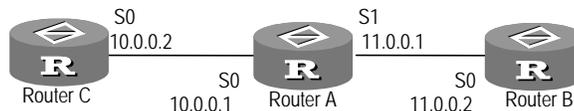
```
[RouterA] qos carl 1 precedence 1
[RouterA] acl 1
[RouterA-acl-1] rule permit source 10.0.0.0 0.0.0.255
[RouterA-acl-1] interface serial 0
[RouterA-Serial0] ip address 10.0.0.1 255.255.255.0
[RouterA-Serial0] qos car inbound acl 1 cir 8000 cbs 15000 ebs 8000
conform pass exceed discard
```

The CAR policy is applied to the packet outputted from Router A serial interface 1 and matching priority level is 2

```
[RouterA] qos carl 2 precedence 2
[RouterA] acl 2
[RouterA-acl-2] rule permit source 10.0.0.0 0.0.0.255
[RouterA-acl-2] interface serial 0
[RouterA-Serial0] ip address 11.0.0.1 255.255.255.0
[RouterA-Serial0] qos car outbound acl 2 cir 8000 cbs 15000 ebs 8000
conform pass exceed discard
```

**Configure the CAR Policy Based on the MAC Address**

The packet input to router A serial interface 0 (the source address of the packet is 00e0.34b0.7676) is matched with the CAR policy based on MAC address. A packet that meets the conditions after its priority level value is changed to 7 will be sent continuously and dropped if it does not.

**Figure 213** Networking diagram of configuring CAR policy based on the MAC address**1** Configure Router A:

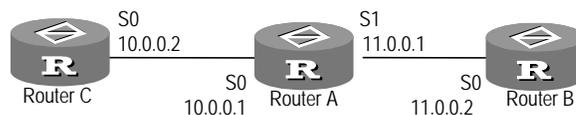
The packet that is inputted to router A serial interface 0 is matched with the CAR policy based on MAC address

```
[RouterA] qos carl 1 mac 00-e0-34-b0-76-76
[RouterA] acl 1
[RouterA-acl-1] rule permit source 10.0.0.0 0.0.0.255
[RouterA-acl-1] interface serial 0
[RouterA-Serial0] ip address 10.0.0.1 255.255.255.0
[RouterA-Serial0] qos car inbound acl 1 cir 8000 cbs 15000 ebs 8000
conform pass exceed discard
```

### Apply a CAR Policy on the Packets that Match ACL

- The CAR policy is applied to the packet that is input to router A serial interface 0 and that matches the specific ACL rule, directly forwarding the packet that meets the conditions and dropping the packet that does not meet the conditions.
- The CAR policy is applied to the packet that is output from router A serial interface 0 and that matches the specific ACL rule, directly forwarding the packet that meets the conditions and dropping the packet that does not meet the conditions.

**Figure 214** Configure the CAR rule to be applied to the packet that matches the ACL policy



#### 1 Configure Router A:

The CAR policy is applied to the packet input to router A serial interface 0 and matching the ACL

```
[RouterA] acl 1
[RouterA-acl-1] rule permit source 10.0.0.2 0.0.0.0
[RouterA-acl-1] interface serial 0
[RouterA-Serial0] ip address 10.0.0.1 255.255.255.0
[RouterA-Serial0] qos car inbound acl 1 cir 8000 cbs 15000 ebs 8000
conform pass exceed discard
```

The CAR policy is applied to the packet that is output from router A serial interface 1 and matches ACL

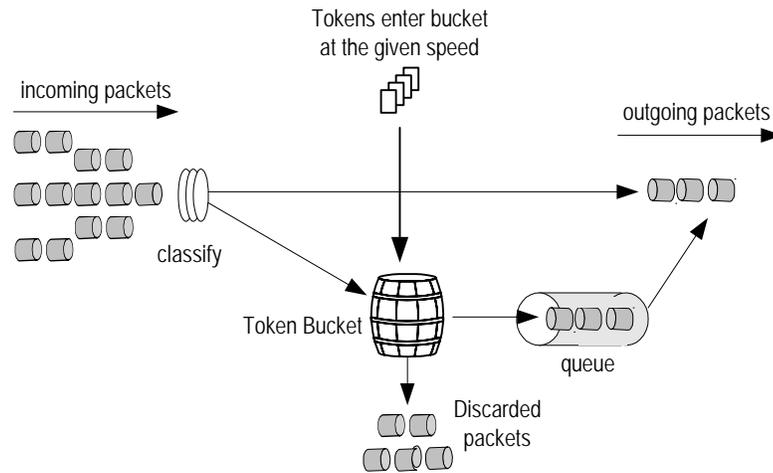
```
[RouterA] acl 1
[RouterA-acl-1] rule permit source 11.0.0.1 0.0.0.0
[RouterA-acl-1] rule permit source 11.0.0.2 0.0.0.0
[RouterA-acl-1] interface serial 0
[RouterA-Serial0] ip address 11.0.0.1 255.255.255.0
[RouterA-Serial0] qos car inbound acl 1 cir 8000 cbs 15000 ebs 8000
conform pass exceed discard
```

---

## Traffic Shaping

Generic Traffic Shaping (GTS) restricts packets that are sent from an interface at relative uniform speed by limiting the traffic and burst of a certain connection from a network. This is usually carried out with buffer and token bucket that is used to control the transmission speed. Even buffering the packets that exceed a specified traffic and sending them after a specified time can make the speed of the packets.

The processing of the packet by GTS is shown in Figure 215.

**Figure 215** Schematic diagram of GTS processing

If an interface does not use the rule defined by **rule** to classify the packet, the interface has only one queue. If GTS uses the rule defined by **rule** to classify the packet, it maintains a separate queue for every type of flow. In every interface, GTS can select either of the following two methods:

- Processing all the flows of the interface: At this time, if the sending queue of this interface is empty, and the traffic of the packets in unit time does not exceed the limitation, the packet is sent immediately, otherwise, the packet enters the sending buffered queue of the interface.
- Processing different flows of the interface: Different flows are compared with *acl-number*. When they are matched with the rule and the interface sending queue is empty, and the traffic of the packet in unit time does not exceed the limitation, the packet is sent immediately, otherwise, the packet enters the sending buffered queue of the interface.

To reduce the unnecessary loss of the packet, GTS processing is performed on the packet in the upstream router egress, and the packet that exceeds the GTS traffic characteristics are buffered on the interface buffer. When the network congestion is removed, GTS again takes out the packet from the buffer queue and continues to send. Thus, the packets sent to the downstream router will all conform to the traffic specification of the router to reduce the drop of the packet in the downstream router. If GTS processing is not performed in the upstream router egress, all the packets that exceed the CAR specified traffic of the downstream router would be dropped by the downstream router.

**Configuring GTS** Traffic shaping configuration includes:

- Configuring shaping parameters for a specified flow
- Configuring shaping parameters for all flows

### Configuring shaping parameters for a specified flow

Shaping a special kind of flow means shaping merely the flows that match the rules.

Please perform the following settings in the interface view.

**Table 714** Configure Shaping Parameters for a Specified Flow

| Operation                                             | Command                                                                                                                          |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Configure the shaping parameters for a specified flow | <code>qos gts acl acl-index cir committed-rate [ cbs burst-size [ ebs excess-burst-size [ queue-length queue-length ] ] ]</code> |
| Cancel shaping parameters for a specified flow        | <code>undo qos gts acl acl-index</code>                                                                                          |

By default, the traffic shaping is not performed on the interface.



*This command may be repeatedly used to set different shaping parameters for different flows.*

*This command cannot be used together with the `qos gts any` command in the same interface.*

### Configuring shaping parameters for all flows

Shaping all the flows means shaping all the flows passing this interface.

Please perform the following settings in the interface view.

**Table 715** Configure Shaping Parameters for all Flows

| Operation                                  | Command                                                                                                                |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Configure shaping parameters for all flows | <code>qos gts any cir committed-rate [ cbs burst-size [ ebs excess-burst-size [ queue-length queue-length ] ] ]</code> |
| Cancel the shaping parameters of the flow  | <code>undo qos gts any</code>                                                                                          |

By default, the traffic shaping is not performed on the interface.

This command cannot be used along with the `qos gts acl` command on the same interface. You must disable fast forwarding before configuring all the traffic shaping parameters.

### Displaying and Debugging Traffic Shaping

**Table 716** Display and Debug Traffic Shaping

| Operation                                                                           | Command                                                |
|-------------------------------------------------------------------------------------|--------------------------------------------------------|
| Display the GTS configuration conditions and statistic information of the interface | <code>display qos gts [ interface type number ]</code> |

### GTS Configuration Example

#### 1 Configure the ACL.

```
[Router] acl 110
[Router-acl-110] rule permit udp source any destination any
```

Shape the flows matching 110 on Ethernet interface 0.

```
[Router-acl-110] interface ethernet0
[Router-Ethernet0] qos gts acl 110 cir 2000000 cbs 120000 ebs 120000
```

Shape all the flows on Ethernet interface 1.

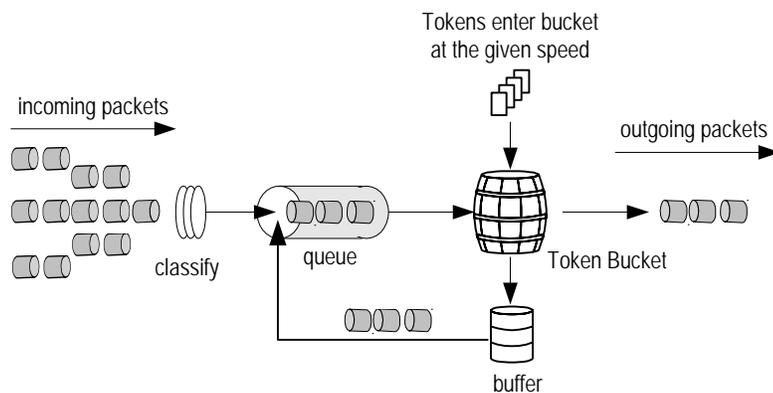
```
[Router] interface ethernet1
[Router-Ethernet1] qos gts any cir 45000000 cbs 5800000 ebs 5800000
```

## Physical Interface Line Rate

By using the physical interface line rate (LR), the total rate for sending packets (including the emergency packet) on a physical interface can be limited.

LR also uses the token bucket to perform the traffic control. If LR is configured in an interface of the router, the LR token bucket first processes all the packets sent by this interface. If the token bucket has sufficient tokens, the packet can be sent; otherwise, the packet enters the QoS queue for congestion management. Thus, the packet traffic through this physical interface can be controlled.

**Figure 216** Schematic diagram of LR processing



As the token bucket is used to control the traffic, when there is any token in the token bucket, the burst transmission of the packet is allowed. When there is no token in the token bucket, the packet cannot be sent until a new token is generated in the token bucket. Thus, there is a limitation that packet traffic cannot be larger than the generating speed of the token, therefore, it realizes that the traffic is limited and burst traffic is allowed to pass through at the same time.

Compared with CAR, LR can limit all the packets passing through the physical interface. CAR is implemented in the IP layer and is ineffective on the packets that are not processed by the IP layer. It is simple to use LR when the user only requires the limitation of all packets.

## LR Configuration

To configure the physical interface line rate, perform the following configurations in the interface view.

**Table 717** Configure the Physical Interface Line Rate

| Operation                                          | Command                                                                             |
|----------------------------------------------------|-------------------------------------------------------------------------------------|
| Configure the physical interface bandwidth         | <code>qos lr cir committed-rate [ cbs burst-size [ ebs excess-burst-size ] ]</code> |
| Delete the configured physical interface bandwidth | <code>undo qos lr</code>                                                            |

By default, the line rate is not performed on the physical interface.

**Displaying and Debugging LR****Table 718** Display and Debug LR

| <b>Operation</b>                                                                   | <b>Command</b>                                  |
|------------------------------------------------------------------------------------|-------------------------------------------------|
| Display the LR configuration conditions and statistic information of the interface | <b>display qos lr [ interface type number ]</b> |

# 49

## CONGESTION MANAGEMENT

This chapter covers the following topics:

- What is Congestion?
- Congestion Management Policy Overview
- Selecting Congestion Management Policies
- Operating Principle of the Congestion Management Policies
- Configuring Congestion Management
- Congestion Management Configuration Examples

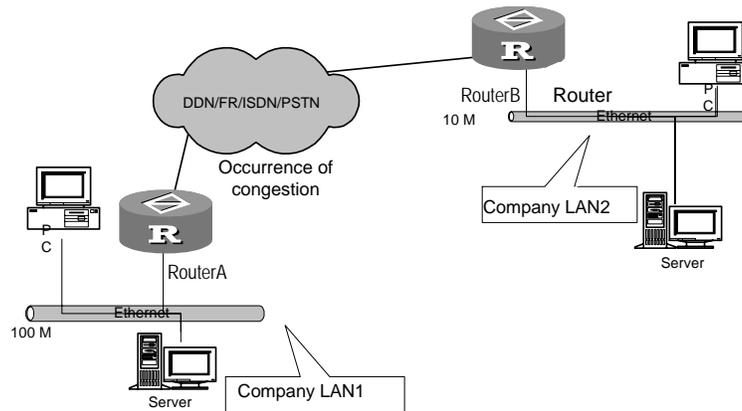
---

### What is Congestion?

For a network unit, when the speed of the data packet is faster than the speed at which this interface sends the data packet, congestion occurs on the interface. If not enough memory space can be provided to store these data packets, some of them will be lost. The loss of the data packet can cause the host or router that is sending the data packet to resend this data packet because of a timeout which can cause a communication failure.

There are many factors causing congestion. For example, when the data packet flow enters the router through the high-speed link and is then transmitted through the low speed link, congestion can occur. When the data packet flow enters the router simultaneously from multiple interfaces and is transmitted from one interface or the processor slows down, congestion may occur.

As shown in Figure 217, two LANs of one company are connected with each other through the low speed link. When a user on LAN 1 sends a large number of data packets to a user on LAN 2, it may cause congestion on the interface through which router A of LAN 1 is connected to the low speed link. If an important application is running between the servers of both LANs, while an unimportant application is running between two PCs, the important application will be influenced.

**Figure 217** Schematic diagram of the congested network

## Congestion Management Policy Overview

When the congestion occurs, if not enough memory space is provided to buffer the packets, some of the packets will be lost. The loss of the packets may cause the host or router that is sending the packet to resend this packet because of overtime, re-congesting and resending, and so on, thereby causing a vicious circle. Therefore, some policies are used to manage network congestion. When congestion occurs, the router takes some policies to dispatch the data packets, deciding which data packets may be sent first and which ones may be discarded. These policies are called the congestion management policy.

For the congestion management, the queuing mechanism is generally used. When congestion occurs, the packet is queued at the router egress by a given policy. During dispatching, the order for sending the packet out of the queue is decided by a given policy.

### FIFO Queuing

In the FIFO mode, the concept of no communication priority and classification is adopted. During the use of FIFO, the sending order of data packet from the interface depends on the order in which the data packet arrives at this interface, at this time, the queuing and de-queuing orders of the packet are the same.

FIFO provides the basic storage and transmission capabilities.

### Priority Queuing

In Priority Queueing (PQ) mode, you can flexibly specify the priority queues which the packets enter according to the fields packet length, source address, and destination address in the packets header and the interface into which the packets will come. The packets belonging to a higher priority queue can be sent first. In this way, the most important data can be handled first.

### Custom Queuing

In the Custom Queueing (CU) model, according to the user's requirements, the traffic can be classified in terms of TCP/UDP port number, ACL and interface type. Each type of traffic is allocated with a certain percent of bandwidth. When network congestion occurs, the traffic that has high demands on delay (such as voice) can obtain reliable service. If a type of traffic cannot occupy all the reserved bandwidth, other types of traffic will occupy the reserved bandwidth automatically, thus making full use of the resource.

For the interface with the lower rate, customizing the queue for it can guarantee that the data flows passing through this interface may also obtain the network services to certain extent.

### Weighted Fair Queuing

Weighted Fair Queuing (WFQ) provides a dynamic and fair queuing mode, which distinguishes the traffic based on the priority/weight and decides the bandwidth size of each session according to the session situation. Thus, it guarantees that all communications can be fairly treated according to the weight allocated to them. The foundation based on which WFQ classifies the traffic includes the source address, destination address, source port number, destination port number, and protocol type.

---

### Selecting Congestion Management Policies

3Com routers implement the four congestion management policies (FIFO, PQ, CQ and WFQ) discussed previously, in the Ethernet interface and serial interface (encapsulated PPP, FR, HDLC), which may satisfy the requirements for various service qualities to a certain extent.

FIFO implements the no priority policy of the data packet in user data communication, which is not needed to determine the priority or type of the communication. However, when using the FIFO policy, some low priority data in abnormal operation may consume most of available bandwidths and occupy the entire queue, which causes the delay of the burst data source, and the important communication may be thereby discarded.

PQ can assure some communication transmission with higher priority. That is, the strict priority sequence is conducted at the cost of transmission failure of data packets with lower priority. For example, the packets in the lower priority queue may not be transmitted in the worst case where the available bandwidth is very limited and emergency communication occurs frequently.

CQ reserves a certain percent of available bandwidth for each type of specified traffic, so that the interface running at a low rate can obtain network service even if congestion occurs. The size of this queue is determined by deciding the total number of the data packets configured in the queue to control access to the bandwidth.

WFQ uses the fair queuing algorithm to dynamically divide the communications into messages. The message is a part of a session. With the use of WFQ, the interactive communication with a small capacity can obtain the fair allocation of the bandwidth, as the same as the communication with a large capacity (such as file transmission).

Table 719 compares between the four different policies:

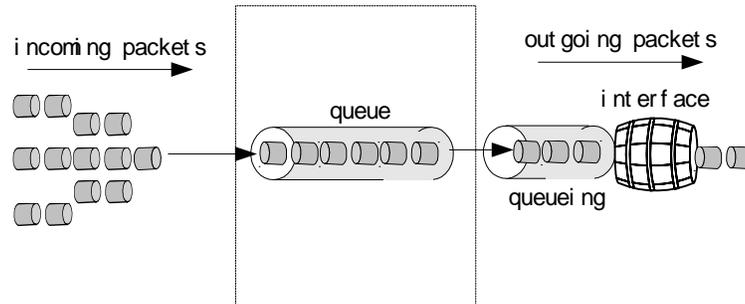
**Table 719** Comparison of Several Congestion Management Policies

|      | Number of queues                        | Advantage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Disadvantage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FIFO | 1                                       | <ol style="list-style-type: none"> <li>1. It does not need to be configured and is easy to use.</li> <li>2. The processing is simple with small delay.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                     | <ol style="list-style-type: none"> <li>1. No matter how urgent they are, all the packets, voice or data, will enter the FIFO (First In, First Out) queue. The bandwidth used for sending packets, delay time, drop rate are decided by the arrival sequence of the packets.</li> <li>2. It has no restriction on the uncoordinated data sources (such as the packet transmission of UDP), and the unmatched data sources will cause the damage of the coordinated data source bandwidth (such as the TCP packet transmission).</li> <li>3. The delay of the real time application sensitive to time (such as VoIP) cannot be guaranteed.</li> </ol> |
| PQ   | 4                                       | The absolute priority can be provided to various service data, and the delay of the real time application sensitive to time (such as VoIP) can be guaranteed. The bandwidth occupation of the packet with the priority service may have the absolute priority.                                                                                                                                                                                                                                                                        | <ol style="list-style-type: none"> <li>1. It needs to be configured, and the processing speed is slow.</li> <li>2. If the bandwidth of the packet with high priority is not restricted, it will cause that the packet with low priority cannot obtain the bandwidth.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                     |
| CQ   | 1                                       | <ol style="list-style-type: none"> <li>1. The packets of various services may be allocated with the bandwidths based on the bandwidth proportion.</li> <li>2. When there is no packet, the available bandwidth occupied by the existing types of packets can be automatically increased.</li> </ol>                                                                                                                                                                                                                                   | It needs to be configured, and the processing speed is slow.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| WFQ  | It is decided by users (256 by default) | <ol style="list-style-type: none"> <li>1. It is easily configured.</li> <li>2. The bandwidth of the coordinated (interactive) data source (such as the TCP packet transmission) can be protected.</li> <li>3. The delayed jitter can be reduced.</li> <li>4. The small packet has priority.</li> <li>5. The flows with various priority levels may be allocated with different bandwidths.</li> <li>6. When the traffic is reduced, the available bandwidth occupied by the existing flows may be automatically increased.</li> </ol> | The processing speed is slower than FIFO.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

### Operating Principle of the Congestion Management Policies

For congestion management, queuing technology is used. When congestion occurs, the data packet is queued at the router by a policy. When dispatching, the order for sending the data packet is decided by the policy.

**Figure 218** Schematic diagram of the first in first out queue



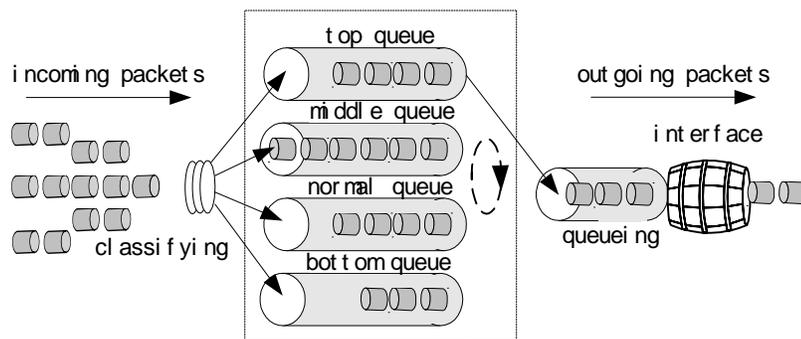
**First-In, First-Out (FIFO) Queuing**

As shown in Figure 218, the data packets are input to the first-in, first-out (FIFO) queue according to the priority order of their arrivals. Data packets that first arrive are first transmitted, and the data packets that later arrive are transmitted later. All the packets that will be transmitted from the interface are input to the end of the FIFO queue of the interface in the priority order of their arrivals. At the time when the interface transmits the packets, the packets are transmitted in order, starting from the head of the FIFO queue. During the transmission process of all packets, there is no difference and no guarantee is provided for the quality of the packet transmission. Therefore, a single application can occupy all the network resources, seriously affecting the transmission of key service data.

**Priority Queuing (PQ)**

As shown in Figure 219, the PQ queue is used to provide strict priority levels for important network data. It can flexibly specify the priority order according to the network protocol (such as IP or IPX), the interface into which the data are input, the length of the packet, and the source address, destination address, and other features.

**Figure 219** Schematic diagram of the priority queuing



When the packets arrive at the interface, all of them are first classified (up to 4 classifications), and then they are input to the ends of respective queues according to the classifications of the packets. Upon the transmission of the packets, according to different priority levels, the packets in the low priority queue are not transmitted until all the packets in the high priority queues are transmitted. Thus, it is guaranteed that, at the network unit where the PQ is utilized, the most important data can be processed the soonest and the packets of the higher priority queues have very low delay. Both packet performance exponents of loss

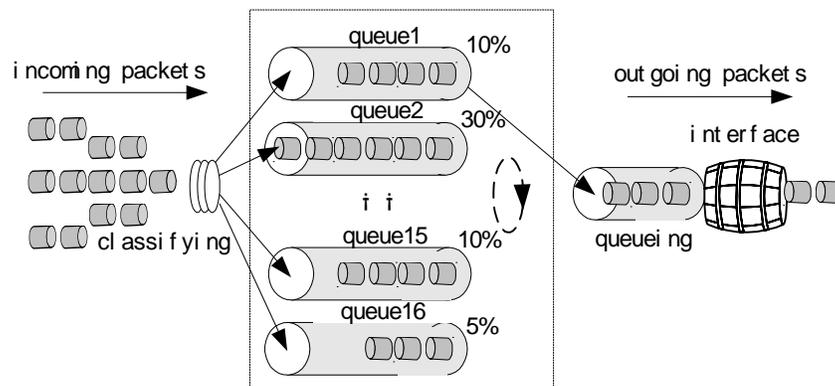
rate and throughput rate can be guaranteed to a certain extent in case of network congestion.

The key service (such as ERP) data packets may be put into the higher priority queue, while the non-key service (such as E-Mail) data packets are put into the lower priority queue, so that the data packets of the non-key service are transmitted in the idle intervals during the processing of the key service data. In this way, the priority of the key service is guaranteed and network resources are optimized. However, it brings the problem that the data packets in the lower priority queue may be blocked in the packet queue of the transmission interface for a long period because of the existence of the data packets in the higher priority queue.

### Custom Queuing (CQ)

As shown in Figure 220, custom queuing (CQ) divides the data packets into 17 classifications (corresponding to 17 queues of CQ) according to a given policy, and data packets are input to respective CQ queues based on their own classifications following the FIFO policy. In 17 queues of CQ, the queue 0 is the system queue, and queues 1 to 16 are the user queues. The users can configure the proportional relationship of the occupied interface bandwidth between various user queues. When dispatching the queue, the data packets in the system queue are first transmitted. Before the system queue is empty, a certain number of data packets from user queues 1 to 16 are not extracted and sent out according to the predetermined configured proportion using polling method.

**Figure 220** Schematic diagram of the custom queuing



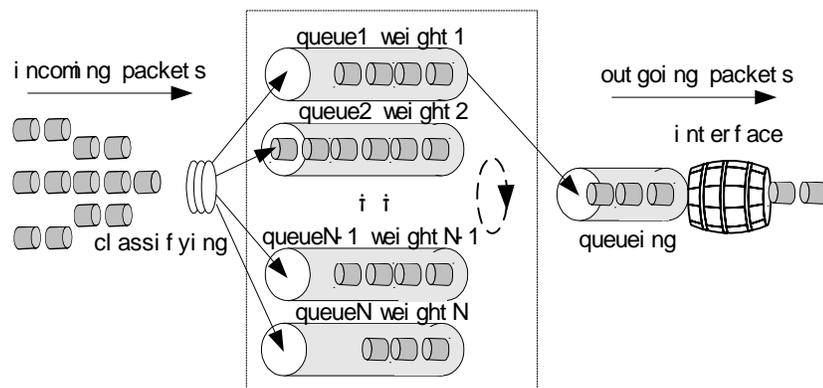
PQ assigns the absolute priority to the data packets with higher priority compared to data packets with the lower priority level. In this way, though the priority transmission of the key service data can be guaranteed, when a number of data packets with higher priority need to be transmitted, all bandwidths may be occupied, causing the data packets with lower priority to be completely blocked. With the use of CQ, such a case can be avoided. CQ has total of 7 queues. Queue 0 is the system queue that is first dispatched, and the queues 1 to 16 are the user queues that are dispatched by a polling method based on the bandwidth settings. The users may configure the proportional relationship of the occupied bandwidth between the queues and the enqueueing policy of the packets. Thus, the data packets of various services can be provided with different bandwidths, to guarantee that the key services can be provided with more bandwidth. In addition, it is not likely that non-key services may not be allocated with the bandwidth.

In the network shown in Figure 217, it is assumed that the server of LAN 1 transmits the data of the key service to the server of LAN 2, and the PC of LAN 1 transmits the data of the non-key service to PC of LAN 2. If the serial interface to be connected with the WAN is configured for congestion management with CQ, and the data flows of the key services between the servers are input to queue A, while the data flows of the non-key services are input to queue B, the proportional relationship of the occupied interface bandwidth between queue A and queue B is configured as 3:1 (for example, during dispatching, queue A may continuously transmit 6000 bytes of data packets every time, while queue B may continuously transmit 2000 bytes of data packets every time). Thus, CQ will treat the data packets of both different services differently. Each time queue A is dispatched, the data packets are continuously transmitted, before the transmitted bytes are not less than 6000 or queue A is empty, the next user queue will not be dispatched. When queue B is dispatched, the condition to stop dispatching is that the continuously transmitted bytes are not less than 2000 or queue B is empty. Therefore, when congestion occurs and there are data packets in queues A and B ready to be transmitted, in the view of the statistic results, the proportion between the bandwidths allocated to the key services and the bandwidths allocated to the non-key services is approximately 3:1.

**Weighted Fair Queuing (WFQ)**

Weighted fair queuing (WFQ), is based on the guarantee of fair bandwidth delay, and reflects the weighted value that is dependent on the PI priority carried in the IP packet header. As shown in Figure 221, weighted fair queuing classifies the packets based on the flows (identical source IP address, destination IP address, source port number, destination port number, protocol number, and ToS packets that belong to the same flow), with each flow allocated to one queue. When dequeuing, WFQ allocates the available bandwidth of the egress to each flow. The smaller the value of the priority is, the less the allocated bandwidth is. The larger the value of the priority is, the more the allocated bandwidth is.

**Figure 221** Schematic diagram of weighted fair queuing



The occupied bandwidth proportion of each flow is:

$$\frac{(\text{its own priority level} + 1)}{(\text{the sum of all of them (the priority levels of the flows} + 1))}$$

For example, there are 5 types of traffic on an interface, and their priority levels are 0,1,2,3 and 4 respectively, the total quota of the bandwidth is the sum of each priority plus 1, that is  $1 + 2 + 3 + 4 + 5 = 15$ . The percentage of the bandwidth

occupied by each traffic is (each priority + 1)/ the sum of each priority plus 1, that is, 1/15, 2/15, 3/15, 4/15 and 5/15.

For example, there are total 4 flows currently, and the priority levels of three of them are 4, and that of one of them is 5, and then the total number of the allocated bandwidth is:

$$(4 + 1) \times 3 + (5 + 1) = 21$$

Then, the bandwidths of the three flows with the priority levels of 4 are 5/21, and the bandwidth of the flows with the priority level of 5 is 6/21.

## Configuring Congestion Management

This section describes the following types of congestion management:

- Configuring FIFO Queuing
- Configuring Priority Queuing
- Configuring Custom Queuing (CQ)
- Configuring WFQ

### Configuring FIFO Queuing

To configure FIFO queuing, perform the following configurations in the interface view.

**Table 720** Configure the First In First Out Queuing

| Operation                                          | Command                                         |
|----------------------------------------------------|-------------------------------------------------|
| Configure the length of FIFO queue                 | <code>qos fifo queue-length queue-length</code> |
| Recover the default value of the FIFO queue length | <code>undo qos fifo queue-length</code>         |

By default, the length of the FIFO queue is 75, with the value ranging 1 to 1024.

### Configuring Priority Queuing

Priority queuing configuration includes:

- Configuring priority queuing
- Applying the priority-list queuing group to the interface
- Specifying the queue length of the priority-list queuing

#### Configuring priority queuing

The priority queuing classifies the packets according to a given policy, and all the packets are divided into 4 classifications, each of which corresponds to one of the 4 queues of PQ respectively. Then the packet is input to the corresponding queue according to its classification. The 4 PQ queues are: high priority queue (**top**), medium priority queue (**middle**), normal priority queue (**normal**) and low priority queue (**bottom**) with priority levels decreased sequentially. Upon the transmission of packets, they are sequentially transmitted according to their priority orders, that is, the packets in the **top** queue are first transmitted, then the packets in the **middle** queue are transmitted, and then the packets in the **normal** queue are transmitted, and finally the packets in the **bottom** queue are transmitted.

The priority queuing includes up to 16 groups (the value range of *pql-index* is 1 to 16), each of which specifies which types of data packets input which queue, the

lengths of various queues, and the number of bytes that may be continuously transmitted by polling of every queue.

The priority queue may be configured according to the following methods:

## 1 Configure the priority queue according to the network layer protocol

Based on packet length, TCP/UDP port number, whether or not matching ACL, you can classify data packets, so that they can enter the queues with different priority.

Perform the following configurations in system view.

**Table 721** Configure the Priority Queue According to the Network Layer Protocol

| Operation                                                            | Command                                                                                                          |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Configure the priority queue according to the network layer protocol | <code>qos pql pql-index protocol protocol-name queue-option queue { top   middle   normal   bottom }</code>      |
| Delete the classification policy in the priority queue               | <code>undo qos pql pql-index protocol protocol-name queue-option queue { top   middle   normal   bottom }</code> |

By default, no priority queue is established.

Among them, *pql-index* is the group number of the priority queue, and *protocol-name* is the protocol name, the current value may be IP.

With *protocol-name* as IP, value of *queue-option* is listed in the following table:

**Table 722** Values of Queue-Option with Protocol as IP

| queue-option                              | Meaning                                                                                                                         |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Empty                                     | All IP packets can be processed into queue                                                                                      |
| <code>acl acl-number (1-199)</code>       | All IP packet fragments can be processed into priority queue                                                                    |
| fragments                                 | IP packets defined by the <i>acl-number</i> (normal) can be processed into priority queue                                       |
| <code>greater-than bytes (0-65535)</code> | IP packet with a length less than a certain value can be processed into queue                                                   |
| <code>less-than bytes (0-65535)</code>    | IP packet with a length greater than a certain value can be processed into queue                                                |
| <code>tcp port (0-6553)</code>            | With the source or destination TCP port of IP packet being the specified port, the packet can be processed into queue.          |
| <code>udp port (0-65535)</code>           | With the source or destination UDP port of IP packet being the specified port, the packet can be processed into priority queue. |

## 2 Configure the priority-list queuing according to the interface

The data packets can be classified according the different types of interfaces into which the data packets are input, and be input into different priority queues.

Please perform the following configurations in the system view

**Table 723** Configure the Priority-List Queuing According to the Interface

| Operation                                                      | Command                                                                                                                   |
|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Configure the priority-list queuing according to the interface | <code>qos pql pql-index inbound-interface interface-type interface-number queue { top   middle   normal   bottom }</code> |

|                                                        |                                                                                 |
|--------------------------------------------------------|---------------------------------------------------------------------------------|
| Delete the classification policy in the priority queue | <b>undo qos pql pql-index inbound-interface interface-type interface-number</b> |
|--------------------------------------------------------|---------------------------------------------------------------------------------|

By default, no priority queue is established.

### 3 Configure the default priority-list queuing.

The data packets that are not matched with any policy in the priority queue (both protocol type and interface type are not matched) will be allocated to the default priority queue.

Please perform the following configurations in the system view.

**Table 724** Configure the Default Priority-List Queuing

| Operation                                          | Command                                                                   |
|----------------------------------------------------|---------------------------------------------------------------------------|
| Configure the default priority-list queuing        | <b>qos pql pql-index default-queue { top   middle   normal   bottom }</b> |
| Recover the default priority of the priority queue | <b>undo qos pql pql-index default-queue</b>                               |

By default, no default priority queue is established.

Multiple policies may be defined for the group of the priority queues, which is then applied to an interface. When the data packet arrives at the interface, the data packet is matched by the system according to the configured policy. The data packet is inputted into the specified queue if it matches with the policy. If the data packet does not match with any policy, it is inputted into the default priority queue. If the default priority queue is not configured, the default priority queue group is 16 with the priority level as **normal**.

### Applying the priority-list queuing group to the interface

To put the priority queue into function, the configured priority queue group must be applied to the specific interface. Every interface can only use one priority queue group, but one priority queue can be applied to multiple interfaces. Multiple different priority queues group can be established to apply to different interfaces.

Perform the following configurations in the interface view.

**Table 725** Apply the Priority-List Queuing Group to the Interface

| Operation                                                        | Command                     |
|------------------------------------------------------------------|-----------------------------|
| Apply the priority-list queuing group on the interface           | <b>qos pq pql pql-index</b> |
| Cancel applying the priority-list queuing group on the interface | <b>undo qos pq</b>          |

By default, the interface utilizes the FIFO queue.

### Specifying the queue length of the priority-list queuing

The queue length of each priority queue (the maximum number of the data packets that may be accommodated) can be specified.

Perform the following configurations in the system view.

**Table 726** Configure the Queue Length of the Priority-List Queuing

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                                                         |                                                                                                   |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Configure the queue length of the priority-list queuing | <code>qos pql pql-index queue { top   middle   normal   bottom } queue-length queue-length</code> |
| Recover the default value of the priority queue length  | <code>undo qos pql pql-index queue { top   middle   normal   bottom } queue-length</code>         |

*queue-length* is the queues lengths of the 4 priority levels. They range 1 to 1024 packets.

The default length of each priority queue is shown in the following table:

**Table 727** Default Length Value of the Priority Queue

| Queue  | Length |
|--------|--------|
| top    | 20     |
| middle | 40     |
| normal | 60     |
| bottom | 80     |

**Displaying and debugging the priority queue**

**Table 728** Display and Debug the Priority Queue

| Operation                                                                                      | Command                                                |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Display the priority queue configuration conditions and statistic information of the interface | <code>display qos pql [ interface type number ]</code> |
| Display the content of the priority list                                                       | <code>display qos pql</code>                           |

**Configuring Custom Queuing (CQ)**

Custom queuing configuration includes:

- Configuring custom-list queuing
- Applying the custom-list queuing group to the interface
- Configuring the queue length of the custom-list queuing
- Configuring the number of the continuously transmitted bytes of the custom queue
- Displaying and debugging the custom-list queue

**Configuring custom-list queuing**

Custom queuing includes up to 16 groups (the value range of *cql-index* is 1 to 16), each of which specifies which types of data packets are input to each queue, the lengths of various queues, and the number of bytes that can be continuously transmitted by polling every queue. Every time the packets are transmitted, the packets in queues 1 to 16 are transmitted sequentially, and the number of the transmitted bytes for every transmission is not less than the number of the specified bytes in this queue, until this queue is empty.

Multiple custom queues can be configured, and the data packet will be matched by the system according to the specified sequence order in the policy list. If it is found that the data packet is matched with a policy, the entire searching process comes to an end.

The custom queue may be configured according to the following methods:

**Configure the custom queue according to the network layer protocol**

The data packets can be classified according to different protocol types, and be input to different custom queues.

Perform the following configurations in the system view.

**Table 729** Configure the Custom Queue According to the Network Layer Protocol

| Operation                                                          | Command                                                                                    |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Configure the custom queue according to the network layer protocol | <code>qos cql cql-index protocol protocol-name queue-option queue queue-number</code>      |
| Delete the classification policy in the custom queue               | <code>undo qos cql cql-index protocol protocol-name queue-option queue queue-number</code> |

Among them, *cql-index* is the group number of the custom queue; *queue-number* is the queue number with the value ranging 0 to 16. *protocol-name* may be ip, and the value range of *queue-option* is the same as that of the priority queue.

**Configure custom-list queuing according to the interface** The data packets can be classified according to different types of the router interfaces into which the data packets are inputted, and be inputted into different custom queues.

Perform the following configurations in the system view.

**Table 730** Configure the Custom-Lst Queuing According to the Interface

| Operation                                                    | Command                                                                                             |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Configure the custom-list queuing according to the interface | <code>qos cql cql-index inbound-interface interface-type interface-number queue queue-number</code> |
| Delete the policy in the custom queue                        | <code>undo qos cql cql-index inbound-interface interface-type interface-number</code>               |

**Configure the default custom-list queuing** The data packets that are not matched with any policy in the custom queue will be allocated to the default custom queue.

Perform the following configurations in the system view.

**Table 731** Configure the Default Custom-List Queuing

| Operation                                                 | Command                                                   |
|-----------------------------------------------------------|-----------------------------------------------------------|
| Configure the default custom-list queuing                 | <code>qos cql pql-index default-queue queue-number</code> |
| Recover the default queue number of the custom-list queue | <code>undo qos cql pql-index default-queue</code>         |

Multiple policies can be defined for the group of the custom-list queues, which is then applied to an interface. When the data packet arrives at the interface, the data packet is matched by the system according to the configured policy, and the data packet is input to the specified custom queue if it matches with the policy. If the data packet does not match with any policy, it is input to the default queue. If the default custom-list queue is not configured, the priority level is **normal**.

### Applying the custom-list queuing group to the interface

To put the custom-list queue into operation, the configured custom-list queue must be applied to the specific interface. Every interface can only use one custom queue, but one custom queue can be applied to multiple interfaces. Multiple different custom queues may be established to apply to different interfaces.

Perform the following configurations in the interface view.

**Table 732** Apply Custom-List Queuing to the Interface

| Operation                                                                | Command                     |
|--------------------------------------------------------------------------|-----------------------------|
| Apply the custom-list queuing group on the interface                     | <b>qos cq cql cql-index</b> |
| Cancel the application of the custom-list queuing group on the interface | <b>undo qos cq</b>          |

By default, the interface uses the FIFO queue.

### Configuring the queue length of the custom-list queuing

The queue length of each priority queue (the maximum number of the data packets that can be accommodated) can be specified.

Perform the following configurations in the system view.

**Table 733** Configure the Queue Length of the Custom-List Queuing

| Operation                                                 | Command                                                               |
|-----------------------------------------------------------|-----------------------------------------------------------------------|
| Configure the queue length of the custom-list queuing     | <b>qos cql cql-index queue queue-number queue-length queue-length</b> |
| Recover the default value of the custom-list queue length | <b>undo qos cql cql-index queue queue-number queue-length</b>         |

By default, the length of the custom-list queue is 20, and the range of the value is 1 to 1024.

### Configuring the number of the continuously transmitted bytes of the custom queue

The number of bytes of the continuously transmitted packets (the total number of the accommodated bytes) may be specified for each custom queue.

Perform the following configurations in the system view.

**Table 734** Configure the Number of the Continuously Transmitted Bytes of the Custom Queuing

| Operation                                                                             | Command                                                        |
|---------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Configure the number of the continuously transmitted bytes of the custom queuing      | <b>qos cql cql-index queue queue-number serving byte-count</b> |
| Recover the default value of the continuously transmitted bytes of the custom queuing | <b>undo qos cql cql-index queue queue-number serving</b>       |

By default, the number of bytes transmitted by respective queues in every polling is 1500, and the range of the value is 1 to 16777215.

*byte-count*: When the router dispatches the user queue of CQ, it continuously extracts and sends the data packets from this queue, until the number of the transmitted bytes is not less than the *byte-count* value configured for this queue or the queue is empty, the next user queue of CQ is to be transmitted. Therefore, the *byte-count* value will affect the proportional relationship of the occupied interface bandwidth between various user queues of CQ, and determine how long the router will dispatch the next queue of CQ.

If the *byte-count* value is too small, the router will go to the next queue after at least one data packet is transmitted, and the bandwidths allocated to various queues may be far from the expected result. If the *byte-count* is too large, it may cause the too long delay of the switching between the queues.

### Displaying and debugging the custom-list queue

**Table 735** Display and Debug the Custom-List Queue

| Operation                                                                                    | Command                                          |
|----------------------------------------------------------------------------------------------|--------------------------------------------------|
| Display the custom queue configuration conditions and statistic information of the interface | <b>display qos cql [ interface type number ]</b> |
| Display the content of the custom list.                                                      | <b>display qos cql</b>                           |

### Configuring WFQ

To configure weighted fair queuing, perform the following configurations in the interface view.:

- Configuring Weighted fair queuing
- Displaying and debugging the weighted fair queue

### Configuring Weighted fair queuing

**Table 736** Configure Weighted Fair Queuing

| Operation                                                               | Command                                                                              |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Configure the weighted fair queuing                                     | <b>qos wfq [ queue-length max-queue-length [ queue-number total-queue-number ] ]</b> |
| Recover the default queue congestion management policy of the interface | <b>undo qos wfq</b>                                                                  |

By default, the adopted congestion management policy is FIFO.

By default, *max-queue-length* is 64 packets. *discard-threshold* can range from 1 to 1024 packets. *total-queue-number* is 256 dynamic queues by default. It can be the following values: 16, 32, 64, 128, 256, 512, 1024, 2048 and 4096.

### Displaying and debugging the weighted fair queue

**Table 737** Display and Debug the Weighted Fair Queue

| Operation                                                                                         | Command                                          |
|---------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Display the custom-list queue configuration conditions and statistic information of the interface | <b>display qos wfq [ interface type number ]</b> |

---

## Congestion Management Configuration Examples

### PQ Configuration Example

- 1 Define the access control table, and allow the packets from 10.10.0.0 network segment to pass through.

```
[Router] acl 1
[Router-acl-1] rule permit source 10.10.0.0
```

- 2 Define one policy for the group 1 of the priority queue: The IP packet that meets the *acl-number* value being 1 is inputted into the queue with the priority level of **top**.

```
[Router] qos pql 1 protocol ip acl 1 queue top
```

- 3 Set the length of the group 1 **top** queue of the priority queue to 10, while the lengths of other queues utilize the default values.

```
[Router] qos pql 1 queue top queue-length 10
```

- 4 Apply the priority queue 1 to Serial 0.

```
[Router-Serial0] qos pq pql 1
```

- 5 One policy is defined for the group 2 of the priority queue, so that all the IP packets from the Serial 1 interface are inputted into the queue with the priority level of **middle**.

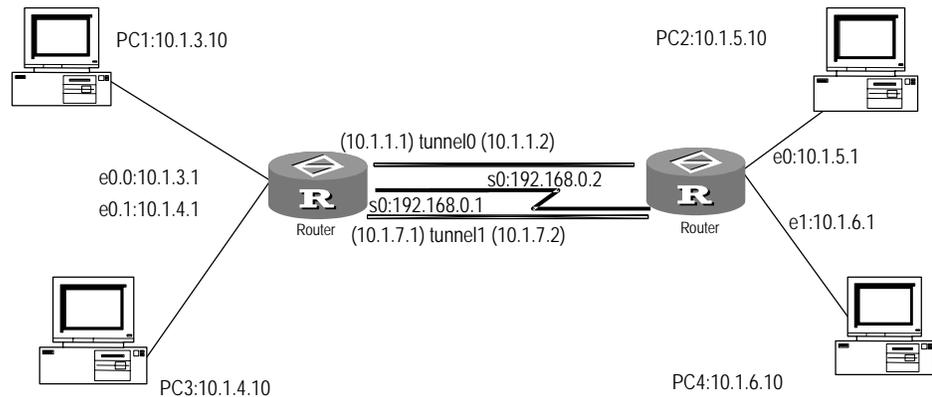
```
[Router] qos pql 2 inbound-interface serial 0 queue middle
```

- 6 Apply the priority queue 2 to Serial 1.

```
[Router-Serial0] qos pq pql 2
```

### CQ Configuration Example

Establish two parallel Tunnel channels (encapsulated GRE) that correspond to the same physical line in WAN. The proportional allocation of the physical line bandwidth should be implemented for the services on both tunnels.

**Figure 222** Networking diagram of CQ typical configuration

## 1 Configure Router A

```
[RouterA] acl 105
[RouterA-acl-105] rule normal permit ip source 10.1.4.0 0.0.0.255
destination 10.1.5.0 0.0.0.255
[RouterA-acl-105] rule normal deny ip source any destination any
[RouterA-acl-105] acl 107
[RouterA-acl-107] rule normal permit ip source 192.168.0.2 0.0.0.0
destination 192.168.0.1 0.0.0.0
[RouterA-acl-108] rule normal permit ip source 192.168.1.2 0.0.0.0
destination 192.168.1.1 0.0.0.0
```

### a Configure the CQ queue

```
[RouterA] qos cql 1 queue 1 queue-length 100
[RouterA] qos cql 1 queue 1 serving 5000
[RouterA] qos cql 1 queue 2 queue-length 100
[RouterA] qos cql 1 queue 2 serving 1000
[RouterA] qos cql 1 protocol ip acl 107 queue 1
[RouterA] qos cql 1 protocol ip acl 108 queue 2
```

### b Configure Serial0 master/slave addresses

```
[RouterA-Serial0] ip address 192.168.0.1 255.255.255.252
[RouterA-Serial0] ip address 192.168.1.1 255.255.255.252 sub
```

### c Apply the CQ queue 1 to Serial0

```
[RouterA-Serial0] qos cq cql
```

### d Configure Tunnel0

```
[RouterA-Tunnel0] ip address 10.1.1.1 255.255.255.0
[RouterA-Tunnel0] source 192.168.0.1
[RouterA-Tunnel0] destination 192.168.0.2
```

### e Configure Tunnel1

```
[RouterA-Tunnel1] ip address 10.1.7.1 255.255.255.0
[RouterA-Tunnel1] source 192.168.1.1
[RouterA-Tunnel1] destination 192.168.1.2
```

## 2 Configure Router B

### a Configure the access control list

```
[RouterB] acl 105
```

```
[RouterB-acl-105]rule normal permit ip source 10.1.5.0 0.0.0.255
destination 10.1.4.0 0.0.0.255
[RouterB-acl-105] rule normal deny ip source any destination any
[RouterB-acl-105]acl 107
[RouterB-acl-107]rule normal permit ip source 192.168.0.1 0.0.0.0
destination 192.168.0.2 0.0.0.0
[RouterB-acl-107]acl 108
[RouterB-acl-107]rule normal permit ip source 192.168.1.1 0.0.0.0
destination 192.168.1.2 0.0.0.0
```

**b** Configure the CQ queue

```
[RouterB] qos cql 1 queue 1 queue-length 100
[RouterB] qos cql 1 queue 1 serving 5000
[RouterB] qos cql 1 queue 2 queue-length 100
[RouterB] qos cql 1 queue 2 serving 1000
[RouterB] qos cql 1 protocol ip acl 107 queue 1
[RouterB] qos cql 1 protocol ip acl 108 queue 2
(CQ restricts the traffic in Tunnel0 that is larger than that in
tunnell1, and CQ is effective at the exit)
```

**c** Configure Serial0 master/slave addresses

```
[RouterB-Serial0] ip address 192.168.0.2 255.255.255.252
[RouterB-Serial0] ip address 192.168.1.2 255.255.255.252 sub
```

**d** Apply the CQ queue 1 to Serial0

```
[RouterB-Serial0] qos cq cql 1
```

**e** Configure Tunnel0

```
[RouterB-Tunnel0] ip address 10.1.2.1 255.255.255.0
[RouterB-Tunnel0] source 192.168.0.2
[RouterB-Tunnel0] destination 192.168.0.1
```

**f** Configure Tunnel1

```
[RouterB-Tunnel1] ip address 10.1.7.2 255.255.255.0
[RouterB-Tunnel1] source 192.168.1.2
[RouterB-Tunnel1] destination 192.168.1.1
```

## WFQ Configuration Example

- 1 Configure a WFQ queue with congestion discard threshold as 64 packets and 512 dynamic queues.

```
[Router] interface ethernet 0
[Router-Ethernet0] qos wfq queue-length 64 queue-number 512
```



This chapter covers the following topics:

- Congestion Avoidance Overview
- WRED Configuration
- Displaying and Debugging Congestion Avoidance
- Congestion Avoidance Configuration Example

---

### **Congestion Avoidance Overview**

The purpose of the congestion avoidance technology is to monitor the network traffic flow, predict the congestion and effectively prevent the congestion occurring at the bottleneck of the network. In a number of the congestion avoidance mechanisms, Random Early Detection (RED) technology is widely used.

Excessive congestion can create damage on the network resource, and measures must be taken to avoid it. Here, the so-called congestion avoidance refers to a traffic control mechanism that, by monitoring the usage of the network resources (such as the queue or memory buffer), removes the network overload by dropping packets on its own initiative to adjust the network traffic in case of the network congestion.

Compared to the end-to-end flow control, stream control here has wide-range meaning, it affects more service stream load in the router. Of course, when the router discards the packet, it does not reject the cooperation with the flow control action, such as the TCP flow control, of the source end, so as to adjust the traffic of the network to a rational load status in a more efficient way. The combination of a good drop policy and source end flow control mechanism always pursue the maximization of the network throughput and service efficiency and the minimization of the packet drop and delay.

### **Traditional Drop Policy**

The traditional drop policy utilizes the tail-drop method. The tail-drop applies to all the traffic flow. It can not distinguish the service level. During the occurrence of the congestion, the data packet of the queue tail will be dropped, until the congestion is settled.

The host running the TCP protocol responds to numerous drops by reducing the packet transmission rate. When the congestion is cleared, the transmission rate of the data packet is increased. In this way, tail-drop can cause the TCP Global Synchronization. When the queue drops multiple TCP packets simultaneously, it causes multiple TCP connections to come into congestion avoidance and slow startup states simultaneously, and reduces and adjusts the traffic at the same time, then the traffic peak occurs as the same time as the reduction of the congestion,

and it causes the sudden increase and decrease of the network traffic, and the line traffic always fluctuates between the states of few or none and full.

**RED and WRED**

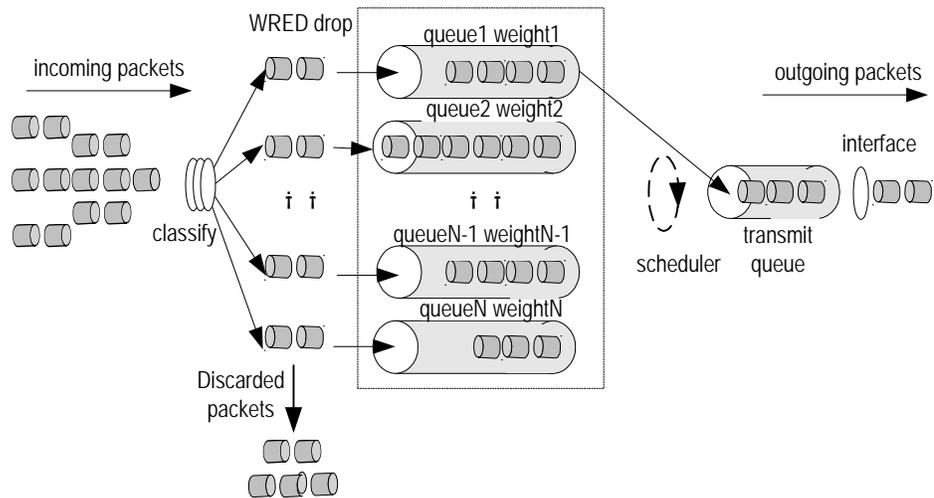
RED and WRED can avoid global synchronization of TCP by dropping packets randomly. When the packets of a TCP connection are dropped, and transmission slows down, other TCP connections can still send packets at high rates, thus improving the utilization of the bandwidth.

RED and WRED avoids the TCP global synchronization phenomenon through the random drop packets--when the packet of a TCP connection is dropped and the transmission speed is reduced, other TCP connections still have the higher transmission speeds. Thus, it is always the case that some TCP connection performs the faster transmission, increasing the use ratio of the line bandwidth.

Both RED and WRED compare between the queue length, and minimum and maximum thresholds, to perform the drop (this is to set the absolute length of the queue). It will cause the unfair treatment on the burst data flow and be disadvantageous for the transmission of the data flow. Therefore, when comparing the minimum and maximum thresholds, and when dropping, the average lengths of the queue are adopted (this is to set the relative value of the length between the queue threshold and the average length). The average length of the queue is the result of the low pass filtering of the queue length, it reflects the variation trend of the queue, and is not sensitive to the burst change of the queue length, so as to avoid the unfair treatment on the burst data flows.

The relationship between WRED and queue mechanism is shown in Figure 223

**Figure 223** Schematic diagram of the relationship between WRED and queue mechanism



In the RED class algorithm, a pair of minimum threshold and maximum threshold is set for each queue, and the following specification is set:

- When the length of the queue is less than the minimum threshold, no packet is dropped.
- When the length of the queue is larger than the maximum threshold, all incoming packets are dropped.

- When the length of the queue is between the minimum threshold and maximum threshold, the WRED algorithm is used to calculate and determine whether the packet is dropped. The specific method is that each incoming packet is allocated with a random number, which is compared with the drop probability of the current queue, if it is larger than the drop probability, the packet is dropped. The longer the queue is, the higher the drop probability is--but there is a maximum drop probability.

When WRED and WFQ is cooperated, the flow based WRED can be implemented. During the classification, different flows have their own queues, for the flow with small traffic, as its queue length is always smaller, the drop probability will be smaller, too. However, as the flow with large traffic will have larger queue length, more packets are discarded, protecting the benefit of the flow with smaller traffic.

Different from RED, the random number generated by WRED is based on the IP priority, it considers the benefit of the high priority packets, and relatively reduce the drop probability of the high priority packets. The 3Com router takes WRED as its congestion avoidance policy.

## WRED Configuration

WRED configuration includes:

- Enable the WRED Function of the Interface
- Configure Weight Factors when Calculating WRED Average Queue Length
- Set the Priority Parameters for WRED

### Enable the WRED Function of the Interface

WRED must first be enabled, and then other parameters related to WRED can be configured.

Please perform the following configurations in the interface view.

**Table 738** Enable WRED

| Operation                                  | Command                    |
|--------------------------------------------|----------------------------|
| Enable the WRED function of the interface  | <code>qos wred</code>      |
| Disable the WRED function on the interface | <code>undo qos wred</code> |

By default, the system disables WRED so the queue avoids congestion by using the tail-drop policy.



*WRED can only operate with WFQ, and cannot be used separately or cooperated with other queue. Therefore, before the startup of WRED, WFQ must have been applied to the interface.*

*Enabling WRED can be effective only in all physical interfaces, while this command is ineffective in the logic interface.*

### Configure Weight Factors when Calculating WRED Average Queue Length

Please perform the following configurations in the interface view.

**Table 739** Configure the WRED Weighted Factor for Calculating the WRED Average Queue Length

| Operation | Command |
|-----------|---------|
|-----------|---------|

|                                                                                                      |                                             |
|------------------------------------------------------------------------------------------------------|---------------------------------------------|
| Configure the WRED weighted factor for calculating the WRED average queue length.                    | <b>qos wred weighting-constant exponent</b> |
| Recover the default value of the WRED weighted factor for calculating the WRED average queue length. | <b>undo qos wred weighting-constant</b>     |

*exponent* is the filtering coefficient for calculating the average queue length, and the range of the value is 1 to 16, and the default value is 9.



*When exponent=0 and the queue length exceeds the threshold, WRED will act accordingly. When exponent is higher, WRED will act slowly to the change of queue status.*

*This configuration should be performed after enabling WRED in the interface view.*

### Set the Priority Parameters for WRED

You can set WRED drop lower threshold value, upper threshold value, and drip probability denominator according to packet priority. The reciprocal value of the denominator *discard-prob* will be taken as the maximum drop probability. The system will handle the queues according to the length of the queues.

- If the queue length is lower than the *low-limit*, no packet will be dropped.
- If the queue length is between *low-limit* and *high-limit*, the drop probability will increase with the queue length till it is almost equal to the reciprocal value of *discard-prob*.
- If the queue length is equal to or greater than *high-limit*, all the packets will be dropped.

Please perform the following configurations in the interface view.

**Table 740** Configure the Related Parameters for the Packets of Specific IP Priority

| Operation                                                                                    | Command                                                                                                                |
|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Configure the related parameters for the packets of specific IP priority                     | <b>qos wred ip-precedence ip-precedence low-limit low-limit high-limit high-limit discard-probability discard-prob</b> |
| Recover the default values of the related parameters for the packets of specific IP priority | <b>undo qos wred ip-precedence ip-precedence</b>                                                                       |

*ip-precedence* is the IP precedence, and the range of the value is 0 to 7.

*low-limit* and *high-limit* are the minimum and maximum thresholds respectively. The default values are 10 and 30 respectively, and the range of the value is 1 to 1024.

*discard-prob* is the drop probability denominator and its default value is 10. The reciprocal of *discard-prob* will be the maximum drop probability. The range of this parameter is 1 to 255.

It should be noted that this configuration can only be performed after WRED is enabled in interface view.

**Displaying and Debugging Congestion Avoidance**

**Table 741** Display and Debug Congestion Avoidance

| Operation                                                                            | Command                                           |
|--------------------------------------------------------------------------------------|---------------------------------------------------|
| Display the WRED configuration conditions and statistic information of the interface | <b>display qos wred [ interface type number ]</b> |

**Congestion Avoidance Configuration Example**

- 1 Configure a WFQ queue.  

```
[Router] interface ethernet 0
[Router-Ethernet0] qos wfq
```
- 2 Enable WRED.  

```
[Router-Ethernet0] qos wred
```
- 3 Configure the exponent to calculate the average WRED queue length.  

```
[Router-Ethernet0] qos wred weighting-constant 1
```
- 4 Configure the lower threshold, upper threshold, and drop probability denominator of the WRED queue with precedence 0 to be 10, 1024 and 30 respectively.  

```
[Router-Ethernet0] qos wred ip-precedence 0 low-limit 10 high-limit 1024 discard-probability 30
```



# XII

## DIAL-UP

Chapter 51    Configuring DCC

Chapter 52    Configuring Modem



This chapter covers the following topics:

- DCC Overview
- Configuring DCC
- Displaying and Debugging DCC
- DCC Configuration Examples
- Troubleshooting DCC

---

## DCC Overview

Dial Control Center (DCC) is the routing technique adopted when the routers interconnect via a PSTN (Public Switched Telephone Network) or ISDN (Integrated Services Digital Network). In DCC, the routers are interconnected through PSTN. The connections are established through dialing when data transmissions are required. A DCC dialing is required to set up a link for transmitting information. When the link becomes idle, the link established by DCC will be automatically disconnected.

Under certain circumstances, routers establish connections for communications to satisfy specific requirements. Therefore, the data transmission are time-independent, burst and in small size. 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 become unavailable for any reasons, DCC uses the designated backup channels to carry out the communications to assure the required services are timely completed.

Frame Relay network through a leased line. To reduce the cost, you can adopt frame relay over ISDN to access the frame relay network through ISDN line. Meanwhile, ISDN network can act as the backup of frame relay network.

## Terms in DCC Configuration

The following terms are commonly used in DCC configurations:

- Physical interface: The physical interface that actually exists, like the serial, BRI, asynchronous, and AM interfaces.
- Dialer interface: Logical interface set 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.

## DCC Configuration Methods

3Com routers provide two DCC configuration methods: circular DCC, and resource-shared DCC. With distinguishing features, these two methods are applicable to different applications. In applications, the participating parties of a call can flexibly select either method as needed. In other words, one party can adopt circular DCC while the other party adopt resource-shared DCC to originate a call.

### Circular DCC

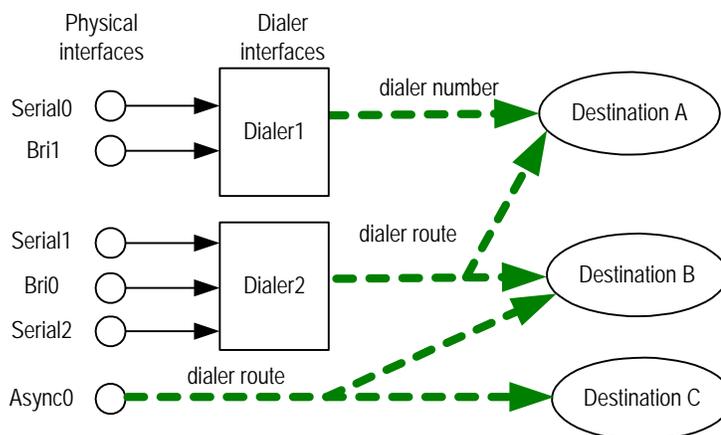
Circular DCC has the following features:

- A logical dial (dialer) interface can use the services provided by multiple physical interfaces (such as Serial0). 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 by 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 can only be associated with one dialing destination address.

In addition, all the B channels on an ISDN BRI interface 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 circular DCC is restricted due to the static binding between the dialing destination addresses and the physical interface configuration.

### Association between the physical interfaces and dialer interfaces in circular DCC

**Figure 224** Association between the physical interfaces and dialer interfaces in Circular DCC



As shown in Figure 224, 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.

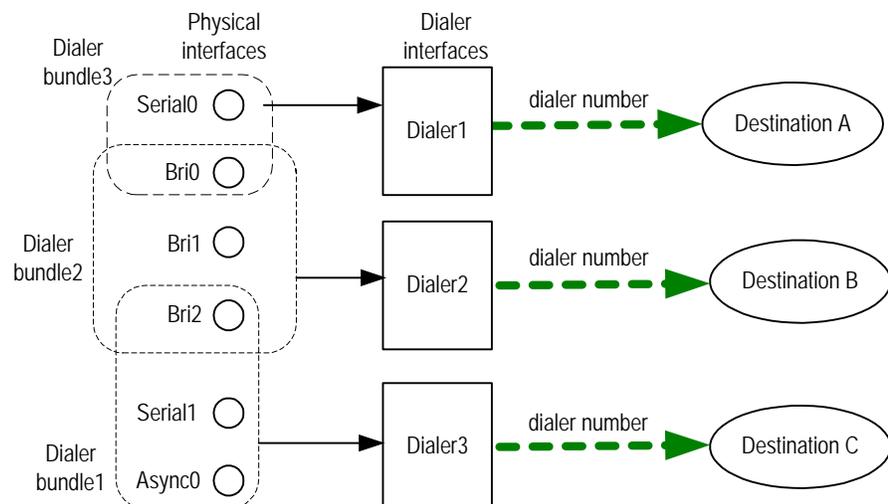
As shown in Figure 224, physical interfaces Serial1, Bri0 and Serial2 belong to Dialer2, and on Dialer2 there are the maps of the string dialed and destination addresses.

### Resource-Shared DCC

Compared to circular DCC, resource-shared DCC is simpler, and is more flexible due to the separation of logical and physical configurations. Specifically, resource-shared 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 dial (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 based on RS-attributes set in implementing resource-shared DCC. 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).
- Resource-Shared DCC parameters cannot be directly configured on a physical interface. The physical interface can implement resource-shared DCC 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 resource-shared DCC

**Figure 225** Association of the physical interfaces, dialer bundles and dialer interfaces in Resource-Shared DCC



As shown in Figure 225, a physical interface can belong to multiple dialer bundles and hence serve multiple dialer interfaces, but each dialer interface associates with only one destination address. Each dialer interface can use only one dialer bundle that contains multiple physical interfaces having different priorities.

In Figure 225, Dialer2 uses Dialer bundle2, and physical interfaces Bri0, Bri1 and Bri2 are members of Dialer bundle2. These physical interfaces have different priorities. Suppose that Bri0 in Dialer bundle2 is assigned with the priority 100, Bri1 with 50, and Bri2 with 75. Since the priority of Bri0 is higher than that of Bri1 and Bri2, Bri0 will be selected first when Dialer2 selects a physical interface from Dialer bundle2.

### **DCC Features Available with 3Com Routers**

3Com routers provide flexible and practical dial interface solutions, as described in the following sections.

#### **Basic DCC features**

Basic DCC features include support for:

- Multiple 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.
- Link layer protocols, such as PPP and Frame Relay, on dial interfaces (physical or dialer interfaces)
- Network layer protocols, such as IP, IPX and Bridge on dial interfaces.
- Dynamic routing protocols, such as RIP and OSPF, on dial interfaces.
- Flexible dial interface standby modes
- Modem control on asynchronous dial interfaces for managing various modems.

#### **Implementing callback through DCC**

In callback, the “called party” originates a return call to the “calling party”. In this case, 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 immediately disconnects and originates a return call.

DCC callback can bring the following advantages:

- Enhances security: When placing a return call, the server dials the calling number configured at the local end. Hence, the insecurity resulted from the distribution of user name and password can be avoided.
- Changes the charge bearer. This is useful for saving cost if the call rates in two directions are different.
- Consolidates the call charge bills, which facilitates the settlement.

3Com routers provide the PPP callback and ISDN caller identification callback features. The PPP callback conforms to and can be adopted to a RFC1570 system regardless of whether the client and server own fixed network addresses, or that the client accepts the network address that is dynamically assigned.

## Preparing to Configure DCC

### Determine 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 the functions carried out by each router.
- Determine the transmission medium, PSTN or ISDN.

### Prepare 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 or other modes) to be used on the dial interface.
- Configure the network protocol (IP, IPX) to be used on the dial interface.
- Configure the routing protocol (RIP, OSPF, or other protocols) to be supported on the dial interface.
- Select a DCC configuration method (circular DCC or resource-shared DCC).

### Configure the local parameters of DCC

Follow the configuration procedure to configure the basic DCC parameters according to the selected DCC configuration method, (circular DCC or resource-shared DCC) to enable the initial DCC implementation. Configure MP binding, PPP callback, ISDN caller identification callback, ISDN leased line, auto-dial, or a combination of these, 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 adjustments to the attribute parameters of the DCC dial interface.

## Configuring DCC

Configuring DCC includes tasks that are described in the following sections:

- Configuring DCC Prepared Parameters
- Configuring Circular DCC
- Configuring Resource-Shared DCC
- Configuring MP Binding for DCC
- Configuring PPP Callback
- Configuring ISDN Caller Identification Callback
- Configuring Special DCC Functions
- Configuring Attributes of DCC Dial Interface

### Configuring DCC Prepared Parameters

Regardless of which method is used, circular DCC or resource-shared DCC, the following two basic DCC configuration tasks should be performed:

- Configuring the mode of the physical interface
- Configuring link layer and network and routing protocols on the interface

### Configuring the mode of the physical interface

For a synchronous/asynchronous serial interface, configure the physical interface to operate in asynchronous and dial mode if it is connected to an asynchronous modem. If the physical interface is connected to a synchronous modem, configure the physical interface to operate in synchronous and dial mode. For an ISDN BRI or PRI interface, this step can be ignored.

Perform the following configuration in dial interface (synchronous/asynchronous serial interface) view.

**Table 742** Configure Physical Interface Mode

| Operation                                                                                         | Command                                                      |
|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| Configure a synchronous/asynchronous serial interface to work in asynchronous or synchronous mode | <b>physical-mode</b> { <b>async</b>   <b>sync</b> }          |
| Configure the asynchronous serial interface to work in dial mode                                  | <b>modem</b> [ <b>in</b>   <b>out</b>   <b>auto-answer</b> ] |

By default, a synchronous/asynchronous serial interface works in synchronous mode and an asynchronous serial interface works in dial (**modem**) mode.



*There is no need to configure the **physical-mode** command for the synchronous serial interface connected to a synchronous modem. The user only needs to configure the **modem** command for an AUX interface.*

### Configuring link layer and network and routing protocols on the interface

Set the link layer protocol in dial interface (physical or dialer interface) view through the **link-protocol** command, configure an IP or IPX address for the dial interface through the **ip address** or **ipx network** command, and perform other configurations in system view.

**Table 743** Configure Link Layer and Network and Routing Protocols on the Interface

| Operation                                       | Command                                                               |
|-------------------------------------------------|-----------------------------------------------------------------------|
| Set a link layer protocol on the dial interface | <b>link-protocol</b><br><b>linklayer-protocol-type</b>                |
| Configure an IP address for the dial interface  | <b>ip address ipaddress mask</b>                                      |
| Activate IPX                                    | <b>ipx enable ipx-address</b>                                         |
| Configure an IPX address for the dial interface | <b>ipx network network-number</b>                                     |
| Configure IPX static route                      | <b>ipx route network.node tick ticks hop hops [ preference value]</b> |
| Configure RIP route protocol                    | <b>rip</b>                                                            |
| Configure OSPF route protocol                   | <b>ospf [ enable ]</b>                                                |
| Configure BGP route protocol                    | <b>bgp as-number</b>                                                  |

The **linklayer-protocol-type** can be SLIP, PPP or Frame Relay. For configuration details, see the related section in *Operation Manual - Link Layer Protocol*, *Operation Manual - Network Protocol* and *Operation Manual - Routing Protocol*.



*For a dialer interface adopting Resource-Shared DCC to implement Frame Relay over ISDN, the B channel is encapsulated with PPP originally. Once the B channel is ready for communication, the protocol encapsulated on the interface dynamically*

becomes the same as that on the Dialer interface, which allows the same B channel to be used by different link layer protocols, improving flexibility. When the B channel is disconnected, the encapsulation protocol on the ISDN interface will be automatically restored to PPP.

### 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 through this link and clear all the data in the idle-timeout timer. If not, it originates 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 by 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 renominate 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 744** Configure Physical Interface Mode

| Operation                                                         | Command                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure a DCC dialer ACL                                        | <b>dialer-rule dialer-group { protocol-name { permit   deny }   acl acl-number }</b>                                                                                                                                                                                       |
| Delete the DCC dialer ACL                                         | <b>undo dialer-rule dialer-group</b>                                                                                                                                                                                                                                       |
| Configure a access control group for the dial interface           | <b>dialer-group dialer-group</b>                                                                                                                                                                                                                                           |
| Remove the dial interface from the specified access control group | <b>undo dialer-group</b>                                                                                                                                                                                                                                                   |
| Create and enter a ACL                                            | <b>acl acl-number</b>                                                                                                                                                                                                                                                      |
| Configure a standard ACL                                          | <b>rule [ normal   special ] { deny   permit } source { any   source-addr [ source-wildcard-mask ] }</b>                                                                                                                                                                   |
| Configure an extended ACL                                         | <b>rule [ normal   special ] { deny   permit } { tcp   udp } source { any   source-addr source-wildcard-mask } source-port [ operator port-number ] destination { any   destination-addr destination-wildcard-mask } destination-port [ operator port-number ] [ log ]</b> |

By default, neither DCC dialer ACL, nor the access control group assigned with a dial interface is configured.



Assure that the commands `dialer rule dialer-group` and `dialer-group dialer-group` adopt the same dialer-group.

Do not concurrently configure the functional arguments of the `protocol-name` and `acl-number` for the same `dialer rule` command when configuring a dialer ACL.

## Configuring Circular DCC

If Circular 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, a 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 configuration 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 Circular DCC configurations introduced below.

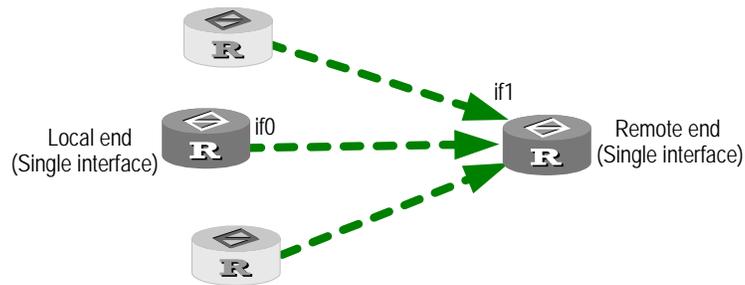


In the circular DCC implementation of DCC, the two dial parties can configure Password Authentication Protocol (PAP) or Challenge-Handshake Authentication Protocol (CHAP) authentication. However, the other party must configure authentication if one party has done that. For security of the dialing ID, you should configure authentication in actual networking applications. For configuration methods, see the section in Operation Manual - Link Layer Protocol and note the following items at the same time:

- 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.

### 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 Figure 226, a local interface originates a call to a single remote end.

**Figure 226** An interface placing a call to a remote end

As shown in this figure, the single local interface interface0 (if0) originates a DCC call to the single remote interface if1. Since the call originates at a single remote end the dialer string can be configured using the **dialer number** or **dialer route** command. When the call originates from the single interface at the local end, the dialer circular group can be used to configure the DCC. The user can choose to configure either PAP or CHAP authentication on the interface.

Perform the following configuration in dial interface (physical or dialer interface) view.

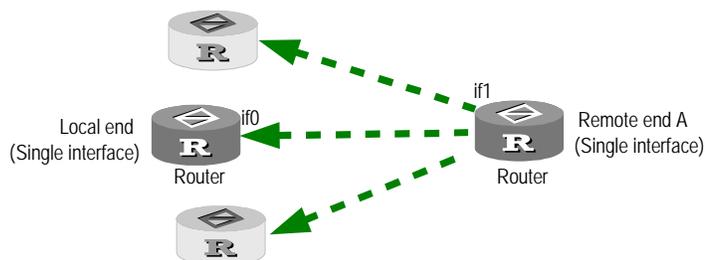
**Table 745** Configure a Local Interface to Originate Calls to a Remote End

| Operation                                           | Command                              |
|-----------------------------------------------------|--------------------------------------|
| Enable Circular DCC                                 | <b>dialer enable-circular</b>        |
| Configure a dialer number for calling a remote end  | <b>dialer number [ dial-number ]</b> |
| Delete the dialer number for calling the remote end | <b>undo dialer number</b>            |

By default, Circular 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.

### Configure 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 227** An interface receiving a call from a remote end

As shown in this 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. You can choose to configure either PAP or CHAP authentication.

Perform the following configuration in dial interface (physical or dialer interface) view.

**Table 746** Configure a local interface to receive calls from a remote interface

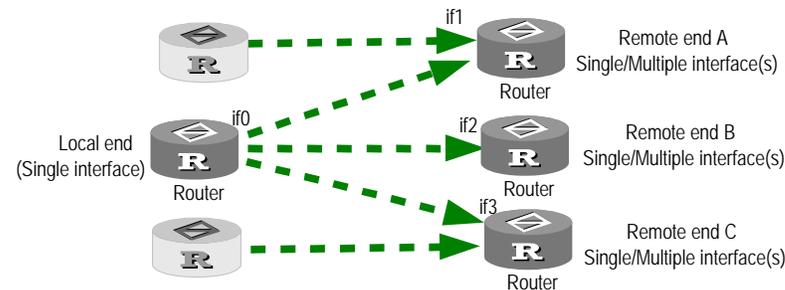
| Operation           | Command                       |
|---------------------|-------------------------------|
| Enable Circular DCC | <b>dialer enable-circular</b> |

By default, Circular DCC is enabled on ISDN BRI and PRI interfaces, but disabled on other interfaces (serial, asynchronous, AUX, etc.) and you should manually configure the **dialer enable-circular** command.

### 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 Figure 228, a local interface originates calls to multiple remote ends (the picture components of inverse color represent the routers irrelevant with the specific networking):

**Figure 228** 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 originate 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 747** Configure a Local Interface to Originate Calls to Multiple Remote Ends

| Operation                                                                                  | Command                                                       |
|--------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Enable Circular DCC                                                                        | <b>dialer enable-circular</b>                                 |
| Configure destination address(es) and dialer number(s) for calling one or more remote ends | <b>dialer route protocol<br/>next-hop-address dial-number</b> |

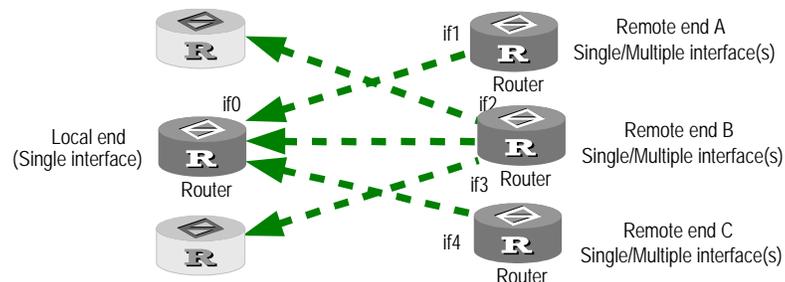
|                                                                                             |                                                          |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Delete the destination address(es) and dialer number(s) for calling one or more remote ends | <code>undo dialer route protocol next-hop-address</code> |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------|

By default, Circular 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.

### 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 Figure 229, a local interface receives calls from multiple remote ends.

**Figure 229** An interface receiving calls from multiple remote ends



As shown in this 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 the `local-user password` command to set up the user name and password to allow for dial in the system view, and then perform other configuration steps in the dial interface (physical or dialer interface) view.

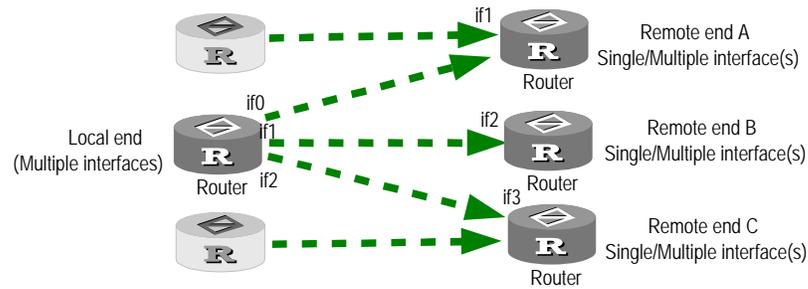
**Table 748** Configure a Local Interface to Receive Calls from Multiple Remote Ends

| Operation           | Command                             |
|---------------------|-------------------------------------|
| Enable Circular DCC | <code>dialer enable-circular</code> |

By default, circular 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.

### 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 230** Multiple interfaces placing calls to multiple remote ends

As shown in Figure 230, the local interfaces interface0 (if0), if1, and if2 originate DCC calls to the remote interfaces if1, if2 and if3. For allowing calls to originate from 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 will use the IP address of the dialer interface in making the calls. The argument *number* of the **dialer circular-group number** command configured in physical interface view must be the same as the *number* used in the **interface dialer number** command configured in the view of the dialer interface to properly associate the physical interface. ISDN BRI or PRI interface is regarded as the dialer circular group for the B channels connected through either of these interfaces. At the same time, they can be regarded as the physical interfaces by other dialer circular groups.

Use the **interface dialer** command to create a dialer interface in global view, add it to the specified dialer circular group through the **dialer circular-group** command, and perform other configuration processes in dialer interface view.

**Table 749** Configure Multiple Local Interfaces to Originate Calls to Multiple Remote Ends

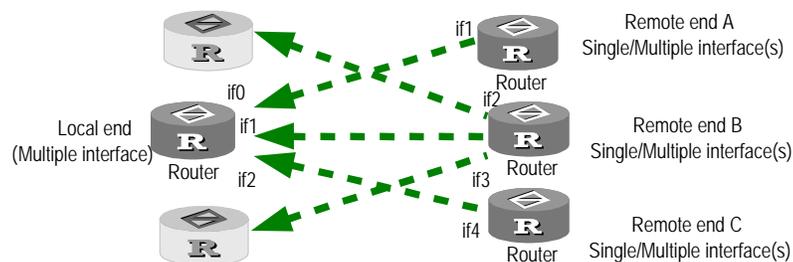
| Operation                                                                                               | Command                                                       |
|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Enable Circular DCC                                                                                     | <b>dialer enable-circular</b>                                 |
| Configure the destination address(es) and the dialer number(s) for calling one (or more) remote end(s). | <b>dialer route protocol<br/>next-hop-address dial-number</b> |
| Delete the destination address(es) and dialer number(s) for calling one (or more) remote ends.          | <b>undo dialer route protocol<br/>next-hop-address</b>        |
| Create a dialer interface and enter the dialer interface view.                                          | <b>interface dialer number</b>                                |
| Delete the existing configurations of the dialer interface                                              | <b>undo interface dialer number</b>                           |
| Bundle a physical interface with the specified dialer circular group                                    | <b>dialer circular-group number</b>                           |
| Remove the physical interface from the specified dialer circular group                                  | <b>undo dialer circular-group</b>                             |
| Configure the priority of the physical interface in the dialer circular group.                          | <b>dialer priority priority</b>                               |
| Restore the default priority of the physical interface in the dialer circular group.                    | <b>undo dialer priority</b>                                   |

By default, circular 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 assigned to physical interface 1, and this is added to a dialer circular group.

### 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 Figure 231, multiple local interfaces receive calls from multiple remote ends (the picture components of inverse color represent the routers irrelevant with the networking):

**Figure 231** Multiple interfaces receiving calls from multiple remote ends



As shown in Figure 231, 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 the **local-user password** command to configure the user name and password permitted to dial in system view, and perform other configurations in dial interface (physical or dialer interface) view.

**Table 750** Configure Multiple Local Interfaces to Receive Calls From Multiple Remote Ends

| Operation                                                              | Command                             |
|------------------------------------------------------------------------|-------------------------------------|
| Enable Circular DCC                                                    | <b>dialer enable-circular</b>       |
| Create a dialer interface and enter the dialer interface view          | <b>interface dialer number</b>      |
| Delete the existing configuration of the dialer interface              | <b>undo interface dialer number</b> |
| Add a physical interface to the specified dialer circular group        | <b>dialer circular-group number</b> |
| Delete the physical interface from the specified dialer circular group | <b>undo dialer circular-group</b>   |

By default, circular 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.

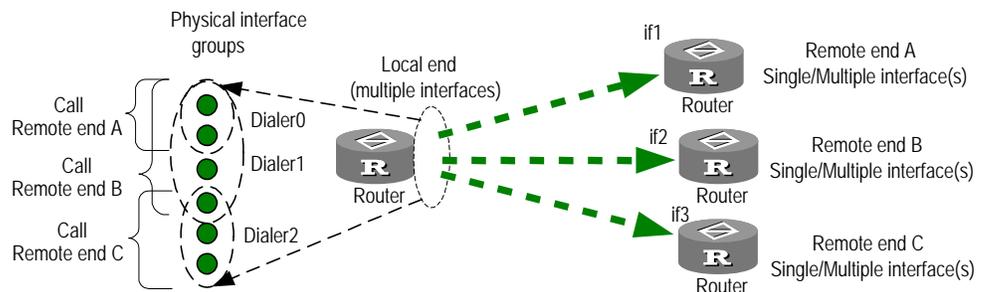
### Configuring Resource-Shared DCC

Each RS-attribute set consists of a dialer interface, the attributes of the interface, and a dialer bundle. Specifically,

- Only one dialer number can be defined for a dialer interface. Since this dialer 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 user can set the number of B channels that will be used through setting dialer bundles.
- All the calls aimed to the same destination segment use the same RS-DCC set.

Due to the separation between logical and physical interface configurations, resource-shared 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.

**Figure 232** Multiple interfaces placing calls to multiple remote ends in the Resource-Shared DCC implementation



As shown in Figure 232, different dialer interfaces are used for placing calls to different remote ends. (That is, one dialer interface only corresponds to one remote end.) Through adding a physical interface to the bundle of some dialer interfaces, the interface can originate calls as needed.

When configure resource-shared 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.



*When configuring resource-shared 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.*

Resource-Shared DCC configuration includes:

- Enabling Resource-Shared DCC
- Configuring the dialer interface and dialer number
- Creating dialer bundle and assigning physical interfaces to it

- Configuring dialing authentication for resource-shared DCC

### Enabling Resource-Shared DCC

Before enabling the resource-shared DCC, please use the command **undo dialer enable-circular** to disable circular DCC first, then enable the resource-shared DCC by using **dialer bundle** command.

Perform the following configuration in dialer interface view.

**Table 751** Enable Resource-Shared DCC

| Operation                                                                           | Command                            |
|-------------------------------------------------------------------------------------|------------------------------------|
| Disable Circular DCC                                                                | <b>undo dialer enable-circular</b> |
| Enable Resource-Shared DCC and configure the dialer bundle used by Dialer interface | <b>dialer bundle number</b>        |
| Disable Resource-Shared DCC and delete the dialer bundle.                           | <b>undo dialer bundle</b>          |

By default, circular DCC has been enabled on ISDN BRI and PRI interfaces, so you need to configure the **undo dialer enable-circular** command when enable resource-shared DCC. Circular DCC has been disabled on other interfaces (serial, asynchronous, AUX, etc). Resource-shared DCC are disabled by default, and no dialer bundle is created.

### 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, then perform other configurations in dialer interface view.

**Table 752** Configure a Dialer Interface and Dialer Number

| Operation                                                      | Command                             |
|----------------------------------------------------------------|-------------------------------------|
| Create a dialer interface, and enter the dialer interface view | <b>interface dialer number</b>      |
| Delete the existing configuration of the dialer interface      | <b>undo interface dialer number</b> |
| Configure a dialer number for calling a remote end             | <b>dialer number dial-number</b>    |
| Delete the dialer number for calling a remote end              | <b>undo dialer number</b>           |

By default, no dialer interface is created.

### Creating dialer bundle and assigning physical interfaces to it

To implement the resource-shared 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 to enable the resource-shared DCC function simultaneously, which is mentioned above.

Perform the following configuration steps in physical interface view.

**Table 753** Create a Dialer Bundle and Assigning the Physical Interfaces to it

| Operation                                               | Command                                                  |
|---------------------------------------------------------|----------------------------------------------------------|
| Add a physical interface to the specified dialer bundle | <b>dialer bundle-member number [ priority priority ]</b> |
| Delete the physical interface from the dialer bundle    | <b>undo dialer bundle-member number</b>                  |

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.

### Configuring dialing authentication for resource-shared DCC

To implement the resource-shared DCC, the called party must identify the calling parties through authentication through the communications between the physical interfaces and the dialer interfaces. Therefore, PAP or CHAP authentication must be configured.

Use the **dialer user** command in dialer interface view then use the **local-user password** command in the system view to perform other configuration steps in dial interface (physical or dialer interface) view.

**Table 754** Configure Multiple Interfaces to Receive Calls From Multiple Remote Ends

| Operation                                                                                      | Command                                                                  |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Configure the remote user name                                                                 | <b>dialer user username</b>                                              |
| Delete the remote user name                                                                    | <b>undo dialer user</b>                                                  |
| Configure the link layer protocol to PPP                                                       | <b>link-protocol ppp</b>                                                 |
| Configure an authentication mode                                                               | <b>ppp authentication-mode { pap   chap }</b>                            |
| Configure the interface to send the local user name and password for PAP authentication        | <b>ppp pap local-user username password { cipher   simple } password</b> |
| Configure the user name that the local end will send to the remote end for CHAP authentication | <b>ppp chap user username</b>                                            |
| Configure the password that the local end will send to the remote end for CHAP authentication  | <b>ppp chap password { cipher   simple } password</b>                    |
| Configure the user name and password that the remote end is allowed to dial in                 | <b>local-user username password { cipher   simple } password</b>         |



*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. While Frame Relay is encapsulated on a Dialer interface, because of no username negotiation procedure, the called end will distinguish Dialer interfaces according to the received number dialed by calling end, hence the command **dialer user** is optional and the command **dialer number** is a must.*

## Configuring MP Binding for DCC

In DCC applications, the user can configure a traffic threshold for links. Setting the traffic threshold to 0 means that the max bandwidth of all the channels is enabled and there is no flow control. If the traffic threshold is in the range 1 to 100, MP binding will adjust the allocated bandwidth by the actual traffic percentage. Specifically, if the percentage of the actual traffic on a link to the bandwidth exceeds the defined traffic threshold, the system will automatically enable the second link, and implement MP binding on these two links. If the percentage of the actual traffic on these two links to the bandwidth exceeds the defined traffic threshold, the system will enable the third link, and implement MP binding, so on and so forth. Thereby, an appropriate traffic can be ensured for the DCC links. On the contrary, if 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. Thereby, the utility rate of the DCC links can be kept within an appropriate range.

### Configuring MP binding in circular DCC

In a circular DCC, if a physical interface is a serial, asynchronous interface or an AUX interface, then a dialer circular group must be used to implement MP binding. (That is, it is required to configure the **dialer threshold** command on dialer interfaces.) If a physical interface is an ISDN BRI or PRI interface, the user can either use a dialer circular group or directly configure MP binding on the physical interface.

After the **dialer threshold** command is configured on a dialer interface, if the percentage of the traffic on a physical interface (or B channels) to the bandwidth exceeds the traffic threshold, the circular DCC will enable another physical interface in the dialer circular group and implement MP binding on these links. If the command is configured on an ISDN BRI or PRI physical interface, circular DCC will select available B channels on the physical interface to implement MP binding. But if all channels are busy, MP binding will be failed.

Use the **dialer threshold** command to configure traffic-percentage threshold in dial interface (ISDN BRI, PRI or dialer interface) view, and then perform other configurations in physical interface view.

**Table 755** Configure MP Binding in Circular DCC

| Operation                                                                                                      | Command                                                          |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Bundle a physical interface with the specified dialer circular group.                                          | <b>dialer circular-group number</b>                              |
| Set the traffic-percentage threshold for MP binding                                                            | <b>dialer threshold traffic-percentage [ in-out   in   out ]</b> |
| Restore the default traffic-percentage threshold of MP binding (that is, no flow control will be implemented). | <b>undo dialer threshold</b>                                     |
| Enable PPP encapsulation.                                                                                      | <b>link-protocol ppp</b>                                         |
| Configure MP binding on the physical interface.                                                                | <b>ppp mp [ interface virtual-template number ]</b>              |

By default, neither MP binding nor traffic-percentage threshold is configured. That is, MP binding is not supported.

### Configuring MP binding in resource-shared DCC

If an interface is a serial, asynchronous interface or an AUX interface, then the resource-shared DCC will enable another physical interface in the dialer bundle of the dialer interface whenever the percentage of traffic on the physical interface to the bandwidth exceeds the traffic threshold. At the same time, it implements MP binding on these links. If the physical interface is an ISDN BRI or PRI interface, the resource-shared DCC will first select the available B channels on the interface, and then the B channels on other ISDN interfaces to implement MP binding.

Use the **link-protocol ppp** or **ppp mp** command to configure PPP encapsulation and MP binding in dial interface (physical or dialer interface) view, and use the **dialer threshold** command to configure a traffic-percentage threshold for MP binding in dialer interface view.

**Table 756** Configure MP Binding in Resource-Shared DCC

| Operation                                                                                                      | Command                                                          |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Set a traffic-percentage threshold for MP binding                                                              | <b>dialer threshold traffic-percentage [ in-out   in   out ]</b> |
| Restore the default traffic-percentage threshold of MP binding (that is, no flow control will be implemented). | <b>undo dialer threshold</b>                                     |
| Enable PPP encapsulation                                                                                       | <b>link-protocol ppp</b>                                         |
| Configure MP binding on interfaces                                                                             | <b>ppp mp [ interface virtual-template number ]</b>              |

By default, neither MP binding, nor traffic-percentage threshold is configured. That is, MP binding is not supported.

### 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.



*Configure PPP callback after completing the basic configuration of Circular DCC or Resource-Shared 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.*

### Configuring PPP callback in the circular DCC implementation

#### 1 Configure PPP callback client in the circular 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 the **local-user password** command to configure the user name in system view, and perform the other configurations in dial interface (physical or dialer interface) view.

**Table 757** Implement PPP Callback (Client Configuration) in Circular DCC

| Operation                                                                                     | Command                                                                  |
|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Configure PPP encapsulation                                                                   | <b>link-protocol ppp</b>                                                 |
| Configure the local end to send the user name and password for PAP authentication             | <b>ppp pap local-user username password { cipher   simple } password</b> |
| Configure the local user name sent to the remote end for CHAP authentication                  | <b>ppp chap user username</b>                                            |
| Configure the password that the local end will send to the remote end for CHAP authentication | <b>ppp chap password { cipher   simple } password</b>                    |
| Configure the user name and password that the remote end is allowed to dial in                | <b>local-user username password { cipher   simple } password</b>         |
| Configure the local end to be the PPP callback client                                         | <b>ppp callback client</b>                                               |
| Disable the local end to be the PPP callback client                                           | <b>undo ppp callback client</b>                                          |
| Configure the destination addresses and dial number(s) for calling one (or more) remote ends  | <b>dialer route protocol next-hop-address dial-number</b>                |
| Configure the dial number for a Windows NT server to originate return calls to the router     | <b>ppp callback ntstring dial-number</b>                                 |
| Delete the dial number that a Windows NT server needs for placing return calls to the router  | <b>undo ppp callback ntstring</b>                                        |

By default, the system does not enable callback function and is not configured with any Windows NT server callback dial number.

## 2 Configure the PPP callback server in the circular 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 **local-user callback-number** 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 **local-user callback-number** command to configure the callback user and callback dial number in system view, and perform other configurations in dial interface (physical or dialer interface) view.

**Table 758** Implement PPP Callback (Server Configuration) in Circular DCC

| Operation                                                                                      | Command                                               |
|------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Configure PPP encapsulation                                                                    | <b>link-protocol ppp</b>                              |
| Configure an authentication mode                                                               | <b>ppp authentication-mode { pap   chap }</b>         |
| Configure the user name that the local end will send to the remote end for CHAP authentication | <b>ppp chap user username</b>                         |
| Configure the password that the local end will send to the remote end for CHAP authentication  | <b>ppp chap password { cipher   simple } password</b> |

| Operation                                                                                      | Command                                                                 |
|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Configure the callback user and callback number                                                | <b>local-user username callback-number telephone-number</b>             |
| Configure the local end to be the PPP callback server                                          | <b>ppp callback server</b>                                              |
| Disable the local end to be the PPP callback server                                            | <b>undo ppp callback server</b>                                         |
| Configure the PPP callback reference                                                           | <b>dialer callback-center [ user ] [ dial-number ]</b>                  |
| Disable the callback server function of the router                                             | <b>undo dialer callback-center</b>                                      |
| Configure the destination address(es) and dial number(s) for calling one (or more) remote ends | <b>dialer route protocol next-hop-address user username dial-number</b> |

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.



*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 **local-user callback-number** command to configure a callback dial number to associate with the callback user name, and hence determine the callback reference.*

### Configuring PPP callback in the resource-shared DCC implementation

#### 1 Configure the PPP callback client in the resource-shared 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 resource-shared DCC are used to implement PPP callback, the PPP authentication configuration at client end is the same as that of circular DCC, except that the client in resource-shared DCC implementation must use the **dialer number** command to configure a dial number. See “Configure PPP callback client in the circular DCC implementation” in *Dial-up*.

Perform the following configuration in dialer interface view.

**Table 759** Implement PPP Callback (Client Configuration) in Resource-Shared DCC

| Operation                                                                                    | Command                                  |
|----------------------------------------------------------------------------------------------|------------------------------------------|
| Configure the local end to be the PPP callback client                                        | <b>ppp callback client</b>               |
| Disable the local end to be the PPP callback client                                          | <b>undo ppp callback client</b>          |
| Configure the dialer number for calling a remote end                                         | <b>dialer number dial-number</b>         |
| Configure the dial number for a Windows NT server to originate return calls to the router    | <b>ppp callback ntstring dial-number</b> |
| Delete the dial number that a Windows NT server needs for placing return calls to the router | <b>undo ppp callback ntstring</b>        |

By default, the system does not enable callback function and is not configured with any Windows NT server callback dial number.

## 2 Configure the PPP callback server in the resource-shared DCC implementation

When resource-shared DCC are adopted to implement PPP callback, the PPP authentication configuration at server end is the same as that of circular DCC, except that the server in the resource-shared DCC implementation can only originate a return call according to the dial number configured in the **local-user callback-number** command. See "Configure the PPP callback server in the circular DCC implementation" in *Dial-up*.

Use the **local-user callback-number** command to configure the callback user and callback dial number in system view, and perform other configurations in dialer interface view.

**Table 760** Implement PPP Callback (Server Configuration) in Resource-Shared DCC

| Operation                                             | Command                                                     |
|-------------------------------------------------------|-------------------------------------------------------------|
| Configure the callback user and callback number       | <b>local-user username callback-number telephone-number</b> |
| Configure the local end to be the PPP callback server | <b>ppp callback server</b>                                  |
| Disable the local end to be the PPP callback server   | <b>undo ppp callback server</b>                             |
| Configure the PPP callback reference                  | <b>dialer callback-center dial-number</b>                   |
| Disable the callback server function of the router    | <b>undo dialer callback-center</b>                          |

By default, the system does not enable the callback function.

## 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.

### Features of ISDN caller identification callback

In the applications of ISDN caller identification callback, the callback server can process a 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** command configured with the keyword **callback**.

The best 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.

Confirm which **dialer call-in** at server end is associated with the incoming call

- In circular 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 resource-shared 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 for the dialer interfaces on it.

### Configuring ISDN caller identification callback in the circular DCC implementation

To configure ISDN caller identification callback client in the circular DCC implementation, perform the following configuration in dial interface (physical or dialer interface) view.

**Table 761** Implement ISDN Caller Identification Callback (Client Configuration) in Circular DCC

| Operation                                                                                    | Command                                                             |
|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| Configure the destination addresses and dial number(s) for calling one (or more) remote ends | <b>dialer route protocol</b><br><b>next-hop-address dial-number</b> |

To configure the ISDN caller identification callback server in the circular DCC implementation perform the following configuration in dial interface (physical or dialer interface) view.

**Table 762** Implement ISDN Caller Identification Callback (Server Configuration) in Circular DCC

| Operation                                                                                      | Command                                                             |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| Configure the local end to implement ISDN callback according to the ISDN caller identification | <b>dialer call-in remote-number [</b><br><b>callback ]</b>          |
| Disable the local end to implement ISDN callback according to the ISDN caller identification   | <b>undo dialer call-in remote-number [</b><br><b>callback ]</b>     |
| Configure the destination address(es) and dial number(s) for calling one (or more) remote ends | <b>dialer route protocol</b><br><b>next-hop-address dial-number</b> |

By default, callback according to ISDN caller identification is not configured.



*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.*

### Configuring ISDN caller identification callback in the resource-shared DCC implementation

To configure ISDN caller identification callback client in the resource-shared DCC implementation, perform the following configuration in dialer interface view.

**Table 763** Implement ISDN Caller Identification Callback (Client Configuration) in Resource-Shared DCC

| Operation                                          | Command                              |
|----------------------------------------------------|--------------------------------------|
| Configure the dial number for calling a remote end | <b>dialer number [ dial-number ]</b> |

To configure the ISDN caller identification callback server in the resource-shared DCC implementation, perform the following configuration in dialer interface view.

**Table 764** Implement ISDN Caller Identification Callback (Server Configuration) in Resource-Shared DCC

| Operation                                                                                      | Command                                               |
|------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Configure the local end to implement ISDN callback according to the ISDN caller identification | <b>dialer call-in remote-number [ callback ]</b>      |
| Disable the local end to implement ISDN callback according to the ISDN caller identification   | <b>undo dialer call-in remote-number [ callback ]</b> |
| Configure the dialer number for calling a remote end                                           | <b>dialer number [ dial-number ]</b>                  |

By default, callback according to ISDN caller identification is not configured.



*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.*

## Configuring Special DCC Functions

### Configuring ISDN leased line

This function can only be used with circular DCC and must be implemented after circular DCC has been configured. ISDN leased line application is fulfilled through establishing semipermanent 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 765** Configure ISDN leased line for Circular DCC

| Operation                                             | Command                                       |
|-------------------------------------------------------|-----------------------------------------------|
| Configure a B channel for ISDN leased line connection | <b>dialer isdn-leased channel-number</b>      |
| Delete the B channel for ISDN leased line connection  | <b>undo dialer isdn-leased channel-number</b> |

By default, no B channel is configured for ISDN leased line connection.

### Configuring auto-dial

This function can only be used with circular DCC. With a circular 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 766** Configure Auto-Dial

| Operation                                                                                                  | Command                                                                                  |
|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Configure one (or more) remote destination address(es) and dialer number(s) that the router will auto-dial | <b>dialer route protocol</b><br><b>next-hop-address dialer-number</b><br><b>autodial</b> |
| Configure an auto-dial interval                                                                            | <b>dialer autodial-interval seconds</b>                                                  |
| Restore the default auto-dial interval                                                                     | <b>undo dialer autodial-interval</b>                                                     |

By default, auto-dial is not configured. If auto-dial function is enabled, the interval for auto-dial defaults to 300 seconds.

### Configuring dialer number circular standby

This function can only be used with circular DCC. When setting the same destination addresses using circular 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, 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 recalling.

Perform the following configuration in dial interface (physical or dialer interface) view.

**Table 767** Configure Dialer Number Circular Standby

| Operation                                                         | Command                                                                                  |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Configure one remote destination address(es) and dialer number(s) | <b>dialer route protocol</b><br><b>next-hop-address dialer-number</b><br><b>autodial</b> |

### Configuring Attributes of DCC Dial Interface

Circular DCC and resource-shared DCC also have some optional parameters to improve configuration flexibility improve DCC efficiency, and hence satisfies various requirements.

DCC dial interface attributes configuration includes:

- Configuring the Link Idle Time
- Configuring the link disconnection time before initiating the next call
- Configuring the link idle time when interface competition
- Configuring the timeout of call setting up
- Configuring the buffer queue length of the dialer

### Configuring the Link Idle Time

In the case that a dial interface originates a call, DCC can be set to disconnect the line after the amount of time for which the line stays idle. In the duration of the

idle time, no the packet which complies with the “permit” statements are transmitted over the line.

Perform the following configuration in dial interface (physical or dialer interface) view.

**Table 768** Configure the Link Idle Time

| Operation                                       | Command                                 |
|-------------------------------------------------|-----------------------------------------|
| Configure the link idle time                    | <b>dialer timer idle <i>seconds</i></b> |
| Restore the link idle time to the default value | <b>undo dialer timer idle</b>           |

By default, the link idle time is 120 seconds.

### Configuring the link disconnection time before initiating 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 769** Configure the Link Disconnection Time Before Initiating the Next Call

| Operation                                                                                | Command                                   |
|------------------------------------------------------------------------------------------|-------------------------------------------|
| Configure the link disconnection time before initiating the next call                    | <b>dialer timer enable <i>seconds</i></b> |
| Restore the link disconnection time before initiating the next call to the default value | <b>undo dialer timer enable</b>           |

By default, the link disconnection time is 20 seconds.

### Configuring the link idle time when interface competition

If all the channels are unavailable when DCC originates a new call, a condition of contention occurs. 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 770** Configure the Link Idle Time When Interface Competition

| Operation                                                                  | Command                                    |
|----------------------------------------------------------------------------|--------------------------------------------|
| Configure the link idle time when interface competition                    | <b>dialer timer compete <i>seconds</i></b> |
| Restore the link idle time when interface competition to the default value | <b>undo dialer timer compete</b>           |

By default, the link idle time is 20 seconds when the interface competition occurs.

### 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 a 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 771** Configure the Timeout of Call Setting Up

| Operation                                                   | Command                                         |
|-------------------------------------------------------------|-------------------------------------------------|
| Configure the timeout of call setting up                    | <b>dialer timer wait-carrier <i>seconds</i></b> |
| Restore the timeout of call setting up to the default value | <b>undo dialer wait-carrier</b>                 |

By default, the timeout of call setting up is 60 seconds.

### 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 held until a connection is established rather than discarded.

Perform the following configuration in dial interface (physical or dialer interface) view.

**Table 772** Configure the Buffer Queue Length of the Dial Interface

| Operation                                               | Command                                   |
|---------------------------------------------------------|-------------------------------------------|
| Configure the buffer queue length of the dial interface | <b>dialer queue-length <i>packets</i></b> |
| Remove the buffer queue length of the dial interface    | <b>undo dialer queue-length</b>           |

By default, no buffer queues are configured on dial interfaces.

## Displaying and Debugging DCC

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 **debugging** command in all views for the debugging.

**Table 773** Display and Debug DCC

| Operation                                                                  | Command                                                                    |
|----------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Display the dial interface information                                     | <b>display dialer interface [ <i>interface-type interface-number</i> ]</b> |
| Display the statically configured or dynamically formed dial number route. | <b>display dialer route [ <i>detail</i> ]</b>                              |
| Enable DCC debugging                                                       | <b>debugging dialer { <i>event</i>   <i>packet</i> }</b>                   |

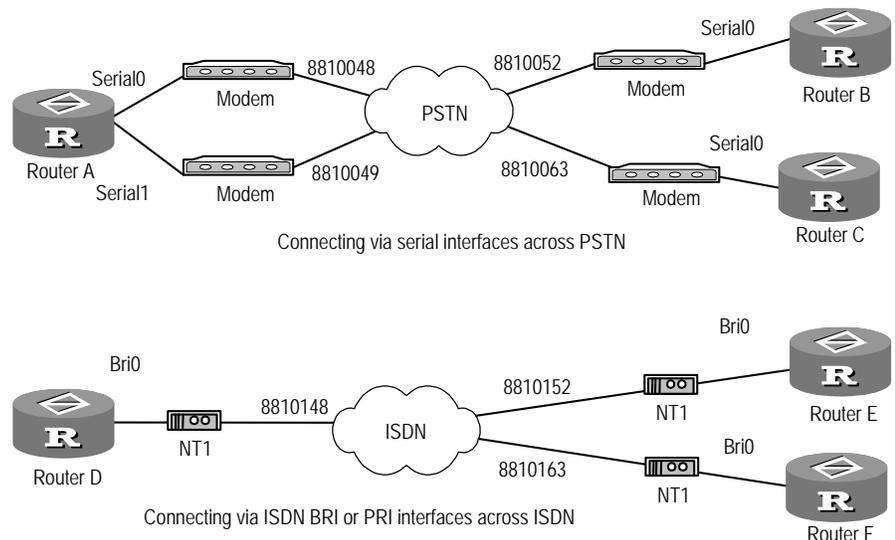
## DCC Configuration Examples

### DCC Applications in Common Use

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 Figure 233, when circular 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 resource-shared DCC are 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.

**Figure 233** Network of a DCC application in common use



### Solution 1

Establish a connection via the serial interface by using Circular 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:

```
[Router] dialer-rule 1 ip permit
[Router] interface dialer 0
[Router-Dialer0] ip address 100.1.1.1 255.255.255.0
[Router-Dialer0] dialer enable-circular
[Router-Dialer0] dialer-group 1
[Router-Dialer0] dialer route ip 100.1.1.2 8810052
[Router-Dialer0] dialer route ip 100.1.1.3 8810063
[Router-Dialer0] interface serial 0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
```

```
[Router-Serial0] dialer circular-group 0
[Router-Serial0] interface serial 1
[Router-Serial1] physical-mode async
[Router-Serial1] modem
[Router-Serial1] dialer circular-group 0
```

## 2 Configure RouterB:

```
[Router] dialer-rule 1 ip permit
[Router] interface serial 0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
[Router-Serial0] ip address 100.1.1.2 255.255.255.0
[Router-Serial0] dialer enable-circular
[Router-Serial0] dialer-group 1
[Router-Serial0] dialer route ip 100.1.1.1 8810048
[Router-Serial0] dialer route ip 100.1.1.1 8810049
```

## 3 Configure RouterC:

```
[Router] dialer-rule 1 ip permit
[Router] interface serial 0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
[Router-Serial0] ip address 100.1.1.3 255.255.255.0
[Router-Serial0] dialer enable-circular
[Router-Serial0] dialer-group 1
[Router-Serial0] dialer route ip 100.1.1.1 8810048
[Router-Serial0] dialer route ip 100.1.1.1 8810049
```

## Solution 2

Establish a connection via the serial interfaces by using Resource-Shared DCC, and configure the DCC parameters on the dialer interfaces.

### a Configure RouterA:

```
[Router] dialer-rule 1 ip permit
[Router] local-user userb password simple userb
[Router] local-user userc password simple userc
[Router] interface dialer 0
[Router-Dialer0] ip address 100.1.1.1 255.255.255.0
[Router-Dialer0] undo dialer enable-circular
[Router-Dialer0] dialer bundle 1
[Router-Dialer0] dialer user userb
[Router-Dialer0] dialer-group 1
[Router-Dialer0] ppp authentication-mode pap
[Router-Dialer0] ppp pap local-user usera password simple usera
[Router-Dialer0] dialer number 8810052
[Router-Dialer0] interface dialer 1
[Router-Dialer1] ip address 122.1.1.1 255.255.255.0
[Router-Dialer1] undo dialer enable-circular
[Router-Dialer1] dialer bundle 2
[Router-Dialer1] dialer user userc
[Router-Dialer1] dialer-group 1
[Router-Dialer1] ppp authentication-mode pap
[Router-Dialer1] ppp pap local-user usera password simple usera
[Router-Dialer1] dialer number 8810063
[Router-Dialer1] interface serial 0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
```

```

[Router-Serial0] dialer bundle-member 1
[Router-Serial0] dialer bundle-member 2
[Router-Serial0] link-protocol ppp
[Router-Serial0] ppp authentication-mode pap
[Router-Serial0] ppp pap local-user usera password simple usera
[Router-Serial0] interface serial 1
[Router-Serial1] physical-mode async
[Router-Serial1] modem
[Router-Serial1] dialer bundle-member 1
[Router-Serial1] dialer bundle-member 2
[Router-Serial1] link-protocol ppp
[Router-Serial1] ppp authentication-mode pap
[Router-Serial1] ppp pap local-user usera password simple usera

```

#### 4 Configure RouterB:

```

[Router] dialer-rule 2 ip permit
[Router] local-user usera password simple usera
[Router] interface dialer 0
[Router-Dialer0] ip address 100.1.1.2 255.255.255.0
[Router-Dialer0] undo dialer enable-circular
[Router-Dialer0] dialer bundle 1
[Router-Dialer0] dialer number 8810052
[Router-Dialer0] dialer user usera
[Router-Dialer0] dialer-group 2
[Router-Dialer0] ppp authentication-mode pap
[Router-Dialer0] ppp pap local-user userb password simple userb
[Router-Dialer0] interface serial 0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
[Router-Serial0] dialer bundle-member 1
[Router-Serial0] link-protocol ppp
[Router-Serial0] ppp authentication-mode pap
[Router-Serial0] ppp pap local-user userb password simple usera

```

#### 5 Configure RouterC:

```

[Router] dialer-rule 1 ip permit
[Router] local-user usera password simple usera
[Router] interface dialer 0
[Router-Dialer0] ip address 122.1.1.2 255.255.255.0
[Router-Dialer0] undo dialer enable-circular
[Router-Dialer0] dialer bundle 1
[Router-Dialer1] dialer number 8810049
[Router-Dialer0] dialer user usera
[Router-Dialer0] dialer-group 1
[Router-Dialer0] ppp authentication-mode pap
[Router-Dialer0] ppp pap local-user userc password simple userc
[Router-Dialer0] interface serial 0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
[Router-Serial0] dialer bundle-member 1
[Router-Serial0] link-protocol ppp
[Router-Serial0] ppp authentication-mode pap
[Router-Serial0] ppp pap local-user userc password simple userc

```

**Solution 3:**

Establish a connection via ISDN BRI or PRI interfaces by using Circular DCC, and configure the DCC parameters on the physical interfaces.

**1** Configure RouterA:

```
[Router] dialer-rule 1 ip permit
[Router] interface bri 0
[Router-Bri0] ip address 100.1.1.1 255.255.255.0
[Router-Bri0] dialer enable-circular
[Router-Bri0] dialer-group 1
[Router-Bri0] dialer route ip 100.1.1.2 8810052
[Router-Bri0] dialer route ip 100.1.1.3 8810063
```

**2** Configure RouterB:

```
[Router] dialer-rule 2 ip permit
[Router] interface bri 0
[Router-Bri0] ip address 100.1.1.2 255.255.255.0
[Router-Bri0] dialer enable-circular
[Router-Bri0] dialer-group 2
[Router-Bri0] dialer route ip 100.1.1.1 8810048
```

**3** Configure RouterC:

```
[Router] dialer-rule 1 ip permit
[Router] interface bri 0
[Router-Bri0] ip address 100.1.1.3 255.255.255.0
[Router-Bri0] dialer enable-circular
[Router-Bri0] dialer-group 1
[Router-Bri0] dialer route ip 100.1.1.1 8810048
```

**Solution 4:**

Establish a connection via the ISDN BRI or PRI interfaces by using Resource-Shared DCC, and configure the DCC parameters on the dialer interfaces.

**1** Configure RouterA:

```
[Router] dialer-rule 1 ip permit
[Router] local-user userb password simple userb
[Router] local-user userc password simple userc
[Router] interface dialer 0
[Router-Dialer0] ip address 100.1.1.1 255.255.255.0
[Router-Dialer0] undo dialer enable-circular
[Router-Dialer0] dialer bundle 1
[Router-Dialer0] dialer user userb
[Router-Dialer0] dialer-group 1
[Router-Dialer0] ppp authentication-mode pap
[Router-Dialer0] ppp pap local-user usera password simple usera
[Router-Dialer0] dialer number 8810152
[Router-Dialer0] interface dialer 1
[Router-Dialer1] ip address 122.1.1.1 255.255.255.0
[Router-Dialer1] undo dialer enable-circular
[Router-Dialer1] dialer bundle 2
[Router-Dialer1] dialer user userc
[Router-Dialer1] dialer-group 1
[Router-Dialer1] ppp authentication-mode pap
[Router-Dialer1] ppp pap local-user usera password simple usera
[Router-Dialer1] dialer number 8810163
[Router-Dialer1] interface bri 0
[Router-Bri0] undo dialer enable-circular
```

```
[Router-Bri0] dialer bundle-member 1
[Router-Bri0] dialer bundle-member 2
[Router-Bri0] link-protocol ppp
[Router-Bri0] ppp authentication-mode pap
```

## 2 Configure RouterB:

```
[Router] dialer-rule 2 ip permit
[Router] local-user usera password simple usera
[Router] interface dialer 0
[Router-Dialer0] ip address 100.1.1.2 255.255.255.0
[Router-Dialer0] undo dialer enable-circular
[Router-Dialer0] dialer bundle 1
[Router-Dialer0] dialer number 8810148
[Router-Dialer0] dialer user usera
[Router-Dialer0] dialer-group 2
[Router-Dialer0] ppp authentication-mode pap
[Router-Dialer0] ppp pap local-user userb password simple userb
[Router-Dialer0] interface bri 0
[Router-Bri0] undo dialer enable-circular
[Router-Bri0] dialer bundle-member 1
[Router-Bri0] link-protocol ppp
[Router-Bri0] ppp authentication-mode pap
```

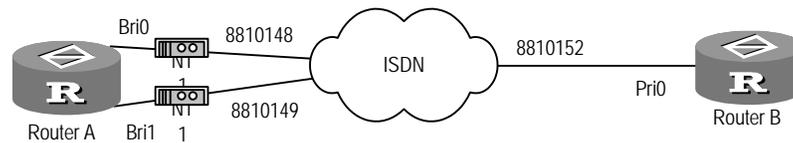
## 3 Configure RouterC:

```
[Router] dialer-rule 1 ip permit
[Router] local-user usera password simple usera
[Router] interface dialer 0
[Router-Dialer0] ip address 122.1.1.2 255.255.255.0
[Router-Dialer0] undo dialer enable-circular
[Router-Dialer0] dialer bundle 1
[Router-Dialer0] dialer number 8810148
[Router-Dialer0] dialer user usera
[Router-Dialer0] dialer-group 1
[Router-Dialer0] ppp authentication-mode pap
[Router-Dialer0] ppp pap local-user userc password simple userc
[Router-Dialer0] interface bri 0
[Router-Bri0] undo dialer enable-circular
[Router-Bri0] dialer bundle-member 1
[Router-Bri0] link-protocol ppp
[Router-Bri0] ppp authentication-mode pap
```

### DCC Application Providing MP Binding

The local router is connected to the remote end via two ISDN BRI interfaces. The traffic threshold must be set 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 Figure 234, the ISDN BRI interfaces on RouterA and the ISDN PRI interface on RouterB are connected through an ISDN network. RouterA must adopt resource-shared DCC to call RouterB, and RouterB adopts circular DCC to call RouterA. The addresses of RouterA and RouterB are 100.1.1.1 and 100.1.1.2, respectively.

**Figure 234** Network for the DCC application providing MP binding**1** Configure RouterA:

```
[Router] dialer-rule 1 ip permit
[Router] local-user userb password simple userb
[Router] flow-interval 3
[Router] interface dialer 0
[Router-Dialer0] ip address 100.1.1.1 255.255.255.0
[Router-Dialer0] undo dialer enable-circular
[Router-Dialer0] dialer bundle 1
[Router-Dialer0] ppp mp
[Router-Dialer0] dialer threshold 50
[Router-Dialer0] dialer user userb
[Router-Dialer0] dialer-group 1
[Router-Dialer0] ppp authentication-mode pap
[Router-Dialer0] ppp pap local-user usera password simple usera
[Router-Dialer0] dialer number 8810152
[Router-Dialer0] interface bri 0
[Router-Bri0] undo dialer enable-circular
[Router-Bri0] dialer bundle-member 1
[Router-Bri0] ppp mp
[Router-Bri0] link-protocol ppp
[Router-Bri0] ppp authentication-mode pap
[Router-Bri0] ppp pap local-user usera password simple usera
[Router-Bri0] interface bri 1
[Router-Bri1] undo dialer enable-circular
[Router-Bri1] dialer bundle-member 1
[Router-Bri1] ppp mp
[Router-Bri1] link-protocol ppp
[Router-Bri1] ppp authentication-mode pap
[Router-Bri1] ppp pap local-user usera password simple usera
```

**2** Configure RouterB:

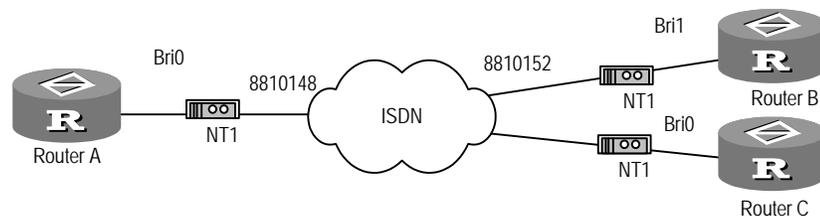
```
[Router] dialer-rule 2 ip permit
[Router] local-user usera password simple usera
[Router] flow-interval 3
[Router] controller e1 0
[Router-E1-0] pri-set
[Router-E1-0] interface serial 0:15
[Router-Serial0:15] link-protocol ppp
[Router-Serial0:15] ppp mp
[Router-Serial0:15] ip address 100.1.1.2 255.255.255.0
[Router-Serial0:15] ppp authentication-mode pap
[Router-Serial0:15] ppp pap local-user userb password simple userb
[Router-Serial0:15] dialer enable-circular
[Router-Serial0:15] dialer-group 2
[Router-Serial0:15] dialer route ip 100.1.1.1 8810148
[Router-Serial0:15] dialer route ip 100.1.1.1 8810149
```

### DCC Application Using ISDN BRI Interface to Dial and Providing Leased Line

To implement circular 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 Figure 235, the B2 channel on the interface Bri0 of RouterA is connected to the B1 channel on the interface Bri0 of RouterC to provide a leased line, whereas the B1 channel is connected to RouterB to implement dialing connection. In the ISDN network, configure the correlation of virtual circuits on the switches respectively corresponding to RouterA and RouterC, so as to ensure both RouterA and RouterC can set up virtual circuit connections to the ISDN network. RouterA adopts Circular 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.

**Figure 235** Network for the DCC application using the ISDN BRI interface to dial and providing a leased line



#### 1 Configure RouterA:

```
[Router] dialer-rule 1 ip permit
[Router] interface bri 0
[Router-Bri0] ip address 100.1.1.1 255.255.255.0
[Router-Bri0] dialer isdn-leased 2
[Router-Bri0] dialer-group 1
[Router-Bri0] dialer route ip 100.1.1.2 8810152
```

#### 2 Configure RouterB:

```
[Router] dialer-rule 2 ip permit
[Router] interface bri 1
[Router-Bri1] ip address 100.1.1.2 255.255.255.0
[Router-Bri1] dialer isdn-leased 1
[Router-Bri1] dialer-group 2
[Router-Bri1] dialer route ip 100.1.1.1 8810148
```

#### 3 Configure RouterC:

```
[Router] dialer-rule 1 ip permit
[Router] interface bri 0
[Router-Bri0] ip address 100.1.1.3 255.255.255.0
[Router-Bri0] dialer-group 1
[Router-Bri0] dialer route ip 100.1.1.1 8810148
```

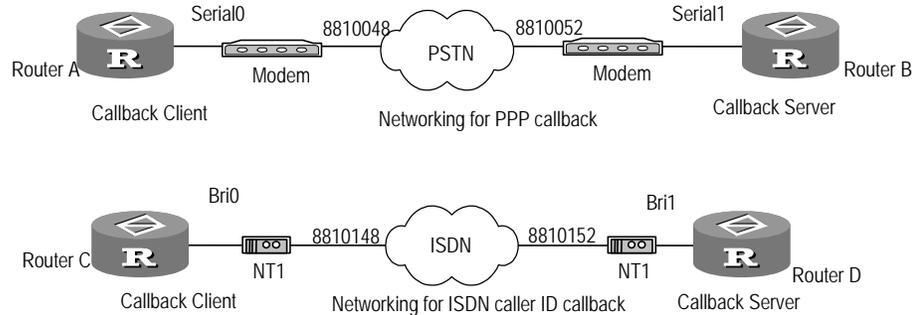
### Router-to-Router Callback for DCC

Two routers implement 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 circular 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.

**Figure 236** Network for the DCC application providing router-to-router callback



### Solution 1:

Use Circular DCC to implement PPP callback. The server determines whether to originate a return call to a client according to the user names configured in the dialer routes.

#### 1 Configure RouterA:

```
[Router] dialer-rule 1 ip permit
[Router] interface serial 0
[Router-Serial0] ip address 100.1.1.1 255.255.255.0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
[Router-Serial0] dialer enable-circular
[Router-Serial0] dialer-group 1
[Router-Serial0] dialer route ip 100.1.1.2 8810052
[Router-Serial0] link-protocol ppp
[Router-Serial0] ppp pap local-user usera password simple usera
[Router-Serial0] ppp callback client
```

#### 2 Configure RouterB:

```
[Router] dialer-rule 2 ip permit
[Router] local-user usera password simple usera
[Router] interface serial 1
[Router-Serial1] ip address 100.1.1.2 255.255.255.0
[Router-Serial1] physical-mode async
[Router-Serial1] modem
[Router-Serial1] dialer enable-circular
[Router-Serial1] dialer-group 2
[Router-Serial1] dialer route ip 100.1.1.1 user usera 8810048
[Router-Serial1] dialer callback-center user
[Router-Serial1] link-protocol ppp
[Router-Serial1] ppp authentication-mode pap
[Router-Serial1] ppp callback server
```

### Solution 2:

Use Circular DCC to implement PPP callback. The server dynamically creates dialer routes and originates return calls to the clients according to the dialer numbers.

#### 1 Configure RouterA:

```
[Router] dialer-rule 1 ip permit
[Router] interface serial 0
```

```
[Router-Serial0] ip address 100.1.1.1 255.255.255.0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
[Router-Serial0] dialer enable-circular
[Router-Serial0] dialer-group 1
[Router-Serial0] dialer route ip 100.1.1.2 8810052
[Router-Serial0] link-protocol ppp
[Router-Serial0] ppp pap local-user usera password simple usera
[Router-Serial0] ppp callback client
```

## 2 Configure RouterB:

```
[Router] dialer-rule 2 ip permit
[Router] local-user usera password simple usera callback-number
8810048
[Router] interface serial 1
[Router-Serial1] ip address 100.1.1.2 255.255.255.0
[Router-Serial1] physical-mode async
[Router-Serial1] modem
[Router-Serial1] dialer enable-circular
[Router-Serial1] dialer-group 2
[Router-Serial1] dialer route ip 100.1.1.1 user usera 8810048
[Router-Serial1] dialer callback-center dial-number
[Router-Serial1] link-protocol ppp
[Router-Serial1] ppp authentication-mode pap
[Router-Serial1] ppp callback server
```

### Solution 3:

Use Circular DCC to implement ISDN caller identification callback.

## 1 Configure RouterA:

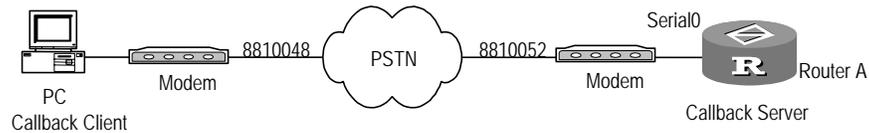
```
[Router] dialer-rule 1 ip permit
[Router] interface bri 0
[Router-Bri0] ip address 100.1.1.1 255.255.255.0
[Router-Bri0] dialer-group 1
[Router-Bri0] dialer route ip 100.1.1.2 user usera 8810152
```

## 2 Configure RouterB:

```
[Router] dialer-rule 2 ip permit
[Router] interface bri 1
[Router-Bri1] ip address 100.1.1.2 255.255.255.0
[Router-Bri1] dialer-group 2
[Router-Bri1] dialer route ip 100.1.1.1 user usera 8810148
[Router-Bri1] dialer call-in 8810148 callback
```

### Router-to-PC Callback for DCC

A router and a PC implement 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. Circular 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.

**Figure 237** Network for the DCC application providing router-to-PC callback

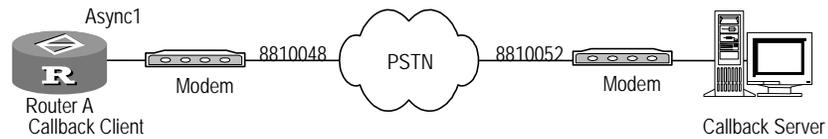
- 1 Configure the PC:
  - a Configure the modem connected to the PC to be in "autoanswer mode".
  - b Select *Start > Programs > Accessories > Communications > Dialup network*.
  - c Click *Set up new connection* in the *Dialup network* window.
  - d Select the *Server type* page in the established new connection, and perform the following operations:
    - Select the option [PPP]
    - Set the [Logon network] option as unchecked
    - Set the [Start software compression] as unchecked
  - e 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:

```
[Router] dialer-rule 1 ip permit
[Router] local-user userpc password simple userpc
[Router] interface serial 0
[Router-Serial0] ip address 100.1.1.1 255.255.255.0
[Router-Serial0] remote address 100.1.1.2
[Router-Serial0] physical-mode async
[Router-Serial0] modem
[Router-Serial0] dialer enable-circular
[Router-Serial0] dialer-group 1
[Router-Serial0] dialer route ip 100.1.1.2 user userpc 8810052
[Router-Serial0] dialer callback-center user
[Router-Serial0] link-protocol ppp
[Router-Serial0] ppp authentication-mode pap
[Router-Serial0] ppp pap local-user Router password simple Router
[Router-Serial0] ppp callback server
```

### NT Server-to-Router Callback for DCC

A router and an NT server implement PPP callback via the serial interfaces across PSTN.

As shown in Figure 238, RouterA and the NT server are interconnected via the modems across PSTN. In this case, circular 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.

**Figure 238** Network for the DCC application providing NT server-to-router callback**1** Configure RouterA:

```
[Router] dialer-rule 1 ip permit
[Router] interface async 0
[Router-Async0] async mode protocol
[Router-Async0] link-protocol ppp
[Router-Async0] ppp callback client
[Router-Async0] ppp pap local-user Router password simple Router
[Router-Async0] ip address ppp-negotiate
[Router-Async0] dialer enable-circular
[Router-Async0] dialer-group 1
[Router-Async0] dialer route ip 100.1.1.254 8810052
```

**2** Configure NT server:

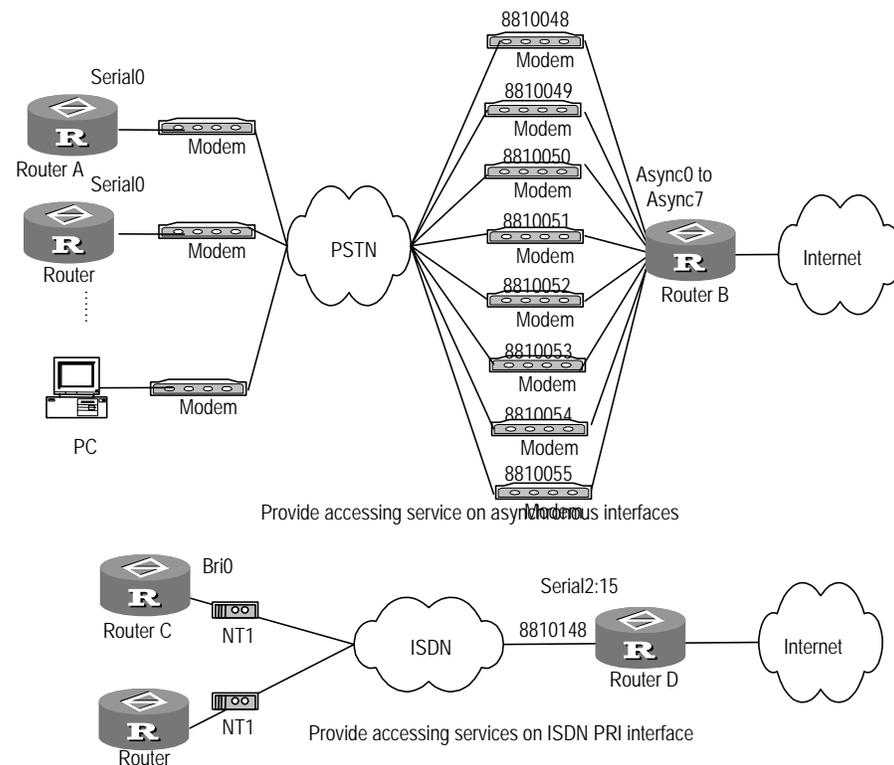
- a** Configure the modem connected to the PC to be in "autoanswer mode", open [Start/Programs/Accessories/Communications/Dialup Network], click [Set up new connection] in the [Dialup Network] window, select the [Server type] page in the established new connection, and perform the following operations:
  - b** 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".
  - c** Then, select the menu bar [Management tools/Server management] to enable remote accessing service.
  - d** 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.

### Dial Number Circular Standby and Internet Access for DCC

In PSTN, the dial number circular standby 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.

**Figure 239** Network for the DCC application providing dial number circular standby and accessing service



#### Solution 1:

Configure dial number circular standby on the dialing parties, adopt Circular 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:

```
[Router] dialer-rule 1 ip permit
[Router] local-user userb password simple passb
[Router] interface serial 0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
```

```
[Router-Serial0] ip address ppp-negotiate
[Router-Serial0] dialer enable-circular
[Router-Serial0] dialer-group 1
[Router-Serial0] dialer route ip 100.1.1.254 8810048
[Router-Serial0] dialer route ip 100.1.1.254 8810049
.....
[Router-Serial0] dialer route ip 100.1.1.254 8810055
[Router-Serial0] link-protocol ppp
[Router-Serial0] ppp pap local-user user1 password simple user1
```

## 2 Configure RouterB:

```
[Router] dialer-rule 2 ip permit
[Router] aaa-enable
[Router] aaa authentication-scheme local-first
[Router] aaa accounting-scheme optional
[Router] local-user user1 password simple pass1
[Router] local-user user2 password simple pass2
.....
[Router] local-user user16 password simple pass16
[Router] ip pool 1 100.1.1.1 100.1.1.16
[Router] interface dialer 0
[Router-Dialer0] ip address 100.1.1.254 255.255.255.0
[Router-Dialer0] remote address pool 1
[Router-Dialer0] dialer enable-circular
[Router-Dialer0] dialer-group 2
[Router-Dialer0] link-protocol ppp
[Router-Dialer0] ppp authentication-mode pap
[Router-Dialer0] ppp pap local-user userc password simple passc
[Router-Dialer0] interface async 1
[Router-Async1] dialer circular-group 0
[Router-Async1] link-protocol ppp
[Router-Async1] ppp authentication-mode pap
[Router-Async1] interface async 2
[Router-Async2] dialer circular-group 0
.....
[Router-Async7] interface async 8
[Router-Async8] dialer circular-group 0
[Router-Async8] link-protocol ppp
[Router-Async8] ppp authentication-mode pap
```

## 3 Configure subscriber PC:

- a Install a modem in a subscriber PC, configure it to be in "autoanswer 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
- b 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

- c 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 circular DCC to set up the connection via the ISDN PRI interface. Configure the DCC parameters on the dialer interface.

#### 1 Configure RouterC:

```
[Router] dialer-rule 1 ip permit
[Router] local-user userb password simple passb
[Router] interface bri 0
[Router-Bri0] ip address ppp-negotiate
[Router-Bri0] dialer-group 1[Quidway-Bri0] dialer enable-circular
[Router-Bri0] dialer route ip 100.1.1.254 8810148
[Router-Bri0] link-protocol ppp
[Router-Bri0] ppp chap user user1
[Router-Bri0] ppp chap password simple pass1
```

#### 2 Configure RouterD:

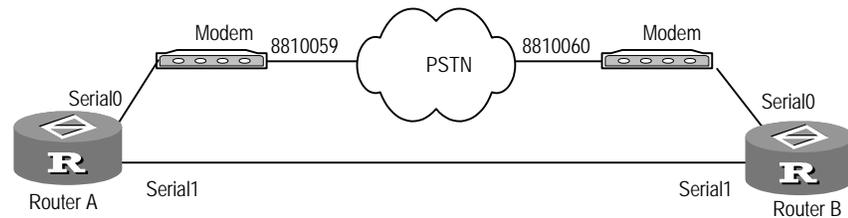
```
[Router] dialer-rule 2 ip permit
[Router] local-user user1 password simple pass1
[Router] local-user user2 password simple pass2
.....
[Router] local-user user16 password simple pass6
[Router] ip pool 1 100.1.1.1 100.1.1.16
[Router] controller e1 2
[Router-E1-2] pri-set
[Router-E1-2] interface serial 2:15
[Router-Serial2:15] ip address 100.1.1.254 255.255.255.0
[Router-Serial2:15] remote address pool 1
[Router-Serial2:15] dialer enable-circular
[Router-Serial2:15] dialer-group 2
[Router-Serial2:15] link-protocol ppp
[Router-Serial2:15] ppp authentication-mode chap
[Router-Serial2:15] ppp chap user userb
[Router-Serial2:15] ppp chap password simple passb
```

### Logical Interface Standby through Dialer route for DCC

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 Figure 240, 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 on RouterA is used as the dialer interface, and Serial1 is connected to RouterB through straightforward DDN. The address of Serial0 on RouterA is 100.1.1.1, and the address of the Serial1 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.

**Figure 240** Network for the DCC application providing logic interface standby through dialer route



### Solution 1:

Adopt circular DCC and use the logic interface configured through the **dialer route** command as the standby interface.

#### 1 Configure RouterA:

```
[Router] dialer-rule 1 ip permit
[Router] interface serial 0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
[Router-Serial0] ip address 100.1.1.1 255.255.255.0
[Router-Serial0] dialer enable-circular
[Router-Serial0] dialer-group 1
[Router-Serial0] dialer route ip 100.1.1.2 8810060 logic-channel 1
[Router-Serial0] interface serial 1
[Router-Serial1] ip address 200.1.1.1 255.255.255.0
[Router-Serial1] link-protocol ppp
[Router-Serial1] standby logic-channel 1
```

#### 2 Configure RouterB:

```
[Router] dialer-rule 2 ip permit
[Router] interface serial 0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
[Router-Serial0] ip address 100.1.1.2 255.255.255.0
[Router-Serial0] dialer enable-circular
[Router-Serial0] dialer-group 2
[Router-Serial0] dialer route ip 100.1.1.1 8810059 logic-channel 1
[Router-Serial0] interface serial 1
[Router-Serial1] ip address 200.1.1.2 255.255.255.0
[Router-Serial1] link-protocol ppp
[Router-Serial1] standby logic-channel 1
```

### Solution 2:

Adopt circular DCC and use the logical interface configured through the **dialer route** command as the main interface.

#### 1 Configure RouterA:

```
[Router] dialer-rule 1 ip permit
[Router] interface serial 0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
[Router-Serial0] ip address 100.1.1.1 255.255.255.0
[Router-Serial0] dialer enable-circular
[Router-Serial0] dialer-group 1
```

```
[Router-Serial0] dialer route ip 100.1.1.2 8810060 logic-channel 1
[Router-Serial0] logic-channel 1
[Router-logic-channel1] standby interface serial 1
[Router-logic-channel1] interface serial 1
[Router-Serial1] ip address 200.1.1.1 255.255.255.0
[Router-Serial1] link-protocol ppp
```

## 2 Configure RouterB:

```
[Router] dialer-rule 2 ip permit
[Router] interface serial 0
[Router-Serial0] physical-mode async
[Router-Serial0] modem
[Router-Serial0] ip address 100.1.1.2 255.255.255.0
[Router-Serial0] dialer enable-circular
[Router-Serial0] dialer-group 2
[Router-Serial0] dialer route ip 100.1.1.1 8810059 logic-channel 1
[Router-Serial0] logic-channel 1
[Router-logic-channel1] standby interface serial 1
[Router-logic-channel1] interface serial 1
[Router-Serial1] ip address 200.1.1.2 255.255.255.0
[Router-Serial1] link-protocol ppp
```

---

## Troubleshooting DCC

### Modem does not dial when the router forwards the data, so the DCC dialup connection cannot be set up.

Do the following:

- 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.

### The remote end cannot be pinged after the modem is connected.

Do the following:

- Check whether the same encapsulation 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` have 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.

**Use the DCC Debugging Information to Locate Problems**

**Enabling DCC debugging**

Execute the following commands in system view for displaying the DCC debugging information:

```
[Router] debugging dialer event
[Router] debugging dialer packet
[Router] info-center enable
```

**Output debugging information for the interconnection failure between DCC and the remote end and diagnosis**

In this section, the debugging information that may be output when DCC cannot reach the remote end will be displayed and explained. The user can solve the problems with the solutions recommended in this section.

**Table 774** DCC Fault Messages

| Message                                     | Fault                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DCC: Receive CALL_DISC_IND                  | <p>The debugging information is probably output because:</p> <p>The physical connection between the local and remote ends is down, phone cable is not securely connected to the router, or the quality of phone line is not good.</p> <p>PPP authentication is not correctly configured, so the PPP authentication is failed.</p> <p>Remote DCC authentication is failed, because <i>name</i> in the commands <b>dialer user</b> and <b>dialer route</b> configured for DCC is inconsistent with <i>name</i> configured for PPP authentication, and the <b>dialer route</b> at the remote end does not contain the local network address.</p> <p>The remote end disconnects the connection because the remote DCC idle-timeout timer has timed out.</p> <p>Solution:</p> <p>If PPP configuration is incorrect or <i>name</i> configurations are inconsistent, implement the configuration as shown in the above example.</p> <p>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.</p> |
| DCC: link negotiation Down on interface *** | <p>The link is probably disconnected because PPP negotiation is failed due to a wrong PPP configuration. To solve the problem, refer to the previous example to make the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| DCC: NAME authentication ERROR, failed      | <p>The debugging information is probably outputted because <i>name</i> configured in the commands <b>dialer user</b> and <b>dialer route</b> is inconsistent with that configured in PPP authentication. The connection is disconnected since the local DCC authentication has been failed. To solve the problem, refer to the previous example to make the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Message                                                                              | Fault                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DCC: peeraddr matching error on interface ***, shutdown link                         | The debugging information is probably outputted because the local dialer route does not contain the remote network address. To solve the problem, 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                      | The debugging information does not indicate any error. DCC normally disconnects the connection, because the local DCC idle-timeout timer has been timed out.                                                                                                                                                                                                             |
| DCC: wait-for-carrier-timeout on a link on interface ***, shutdown!start enable-time | The debugging information is probably outputted because the local router cannot contact the remote end for a long time. It may occur because the remote end is busy or the quality of the phone line is bad.                                                                                                                                                             |
| DCC: The interface has no dialer-group, discard the packet!                          | The debugging information is probably outputted because the <b>dialer-group</b> command has not been configured on the corresponding dialer interface or the physical interface on which DCC is directly enabled. To solve the problem, refer to the previous example to make the configuration.                                                                         |
| DCC: there is not a dialer number on the interface, failed, discard packet           | The debugging information is probably outputted, because neither <b>dialer route</b> nor the <b>dialer number</b> is configured on the corresponding dialer interface or the physical interface on which DCC is enabled directly. To solve the problem, configure the <b>dialer route</b> and the dialer number on the local end for the outbound call at the local end. |
| DCC: Enable-timeout is effective , failed                                            | Rather than indicating an error, the outputted debugging information means that the enable-timeout timer on the corresponding physical interface have not timed out yet. The physical interface can be used for dialing upon the timeout of the timer.                                                                                                                   |

This chapter covers the following topics:

- Modem Function Provided by 3Com Routers
- Configuring a Modem
- Displaying and Debugging a Modem
- Modem Configuration Examples
- Troubleshooting

---

### Modem Function Provided by 3Com Routers

To offer the optimal flexibility, 3Com routers provide the following modem management functions:

- Provide the scripts (modem script) for modem management to enable the user to better control the modems connected to the router. A modem script can be executed by the following two means:
  - Executes a modem script directly through the **script-string** command to initialize the modem or other configurations.
  - Triggers the modem script with particular events, such as router startup, modem dial-in connection, and the **start-chat** command.
- Using 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 through the dumb terminal or modem dialup, to configure and manage the router.
- Directly send AT commands to the modem via the serial interface for managing the modem.
- Interwork with the equipment of other equipment vendors. That is, the asynchronous serial interfaces of the participating parties are working in the flow mode and interconnected through modems.
- Provides rich debugging information for modem monitoring and maintenance.

### Modem Script

3Com routers provide t modem scripts, which are mainly used for:

- Flexibly controlling the modems of different models. For example, using different initialization AT commands able to interoperate with 3Com 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 through the modem, routers can negotiate the protocol to be encapsulated with the physical link and its operating parameters.

### 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 "-".
- The default timeout time waiting for a receive-string is 5 seconds. **TIMEOUT seconds** can be inserted into the script 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, "") have 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 are the delimiters in the string at the same time.

**Table 775** Script Keywords

| Keyword                            | Description                                                                                                                                                                                                                                                                                     |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ABORT</b> <i>receive-string</i> | The string following <b>ABORT</b> will be compared with the strings sent from a modems or remote DTE device for a match. The match mode is full match. Multiple <b>ABORT</b> entries can be configured for a script, and all of them take effect in the whole script execution period.          |
| <b>TIMEOUT</b> seconds             | The digit following <b>TIMEOUT</b> 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 fail. Once being set, the setting will be valid till a new <b>TIMEOUT</b> is set. |

In which, *seconds* defaults to 180 and is in the range of 0 to 180.

**Table 776** Script Escape Characters

| Escape character | Description                                                                                                                                                                                    |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \c               | 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 "newline".                                                                                                                                                            |
| \r               | Represents the character "Enter".                                                                                                                                                              |
| \s               | Represents the character "Space".                                                                                                                                                              |
| \t               | Represents the character "Tab".                                                                                                                                                                |
| \\               | Represents the character "\".                                                                                                                                                                  |
| \T               | Represents telephone number.                                                                                                                                                                   |

## Configuring a Modem

Modem Configuration includes:

- Configure the Modem Dial-in and Dial-out Authorities
- Configure Modem Through the AT Command
- Configure a Modem Script
- Execute a Modem Script Manually
- Specify the Events that Trigger Modem Scripts
- Configure the modem-related operation mode for the asynchronous interface
- Configure the Modem Answer Mode
- Configure Authentication for a Modem Dial-in User

### Configure the Modem Dial-in and Dial-out Authorities

Perform the following configuration in interface (asynchronous serial, AUX or AM interface) view.

**Table 777** Configure the Modem Dial-In and Dial-Out Authorities

| Operation                               | Command           |
|-----------------------------------------|-------------------|
| Enable only modem dial-in               | <b>modem in</b>   |
| Enable only modem dial-out              | <b>modem out</b>  |
| Enable both modem dial-in and dial-out  | <b>modem</b>      |
| Disable both modem dial-in and dial-out | <b>undo modem</b> |

By default, modem dial-in and dial-out are allowed.

**Configure Modem Through the AT Command**

Perform the following configuration in interface (asynchronous serial, AUX or AM interface) view.

**Table 778** Configure a Modem Script

| Operation                              | Command                 |
|----------------------------------------|-------------------------|
| Configure modem through the AT Command | <b>sendat at-string</b> |

A modem can accept the AT commands only when it is in AT command mode. If it is forwarding data, the AT command sent via the **sendat at-string** command is invalid.

**Configure a Modem Script**

Perform the following configuration in system view.

**Table 779** Configure a Modem Script

| Operation               | Command                                         |
|-------------------------|-------------------------------------------------|
| Define a modem script   | <b>script-string script-name script-content</b> |
| Delete the modem script | <b>undo script-string script-name</b>           |

For the format of *script*, refer to the modem script syntax description.

**Execute a Modem Script Manually**

If necessary, the user can execute the modem script through the **start-chat** command for managing the external modem to which the interface is connected.

Perform the following configuration in interface (asynchronous serial, AUX or AM interface) view.

**Table 780** Execute a Modem Script Manually

| Operation                       | Command                       |
|---------------------------------|-------------------------------|
| Manually execute a modem script | <b>start-chat script-name</b> |

**Specify the Events that Trigger Modem Scripts**

Associating modem scripts with events, is to automatically execute the corresponding script after a particular event occurs to the router. In 3Com routers, the following script events are supported:

- An outgoing call is established to a line: The specified script will be executed if a modem outgoing call is established.
- An incoming call is established to a line: The specified script will be executed if a modem incoming call is established.
- DCC dial: Start the dial script when implementing DCC dial.
- Line reset: Execute the specified script when a line is disconnected.
- Power on the system and reboot it: Execute the specified script on the corresponding asynchronous serial interface when the system is powered on and initialized.

For the the events in the previous list, the corresponding scripts can be specified through the **script** command.

Perform the following configuration in interface (asynchronous serial, AUX or AM interface) view.

**Table 781** Specify the Events Triggering the Modem Scripts

| Operation                                                                                               | Command                                          |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Specify the automatically executed modem script when the calling-out connection is set up successfully. | <b>script trigger login <i>script-name</i></b>   |
| Specify the automatically executed modem script when the calling-in connection is set up successfully.  | <b>script trigger connect <i>script-name</i></b> |
| Specify the automatically executed modem script before DCC dialing.                                     | <b>script trigger dial <i>script-name</i></b>    |
| Specify the automatically executed modem script at the time of line reset.                              | <b>script trigger logout <i>script-name</i></b>  |
| Specify the automatically executed modem script at the time of system power-on and restart.             | <b>script trigger init <i>script-name</i></b>    |
| Specify the default modem initialization string for initializing modem.                                 | <b>script init-string <i>init-string</i></b>     |



*The argument following the **script init-string** command is the initialization string rather than the modem script name.*

### Configure the Modem Answer Mode

This configuration depends on whether the external modem to which the asynchronous interface is connected is in auto-answer mode (whether the AA LED on the modem is on). If the modem is in auto-answer mode, the user should execute **modem-autoanswer** before using the dial function. If not, the user should execute **undo modem-autoanswer**. Inconsistency of the configuration and the modem status may cause the abnormal acceptance of some modem incoming calls.

Perform the following configuration in interface (asynchronous serial, AUX or AM interface) view.

**Table 782** Configure the Answer Mode for the Modem

| Operation                                           | Command                       |
|-----------------------------------------------------|-------------------------------|
| Configure the modem to work in auto-answer mode     | <b>modem auto-answer</b>      |
| Configure the modem to work in non-auto answer mode | <b>undo modem auto-answer</b> |

By default, the modem works in non-auto answer mode.

### Configure Authentication for a Modem Dial-in User

The command **modem-login** is configured to authenticate the name and password of the dial-in user. Generally this command is used together with the command of **script trigger connect**, thus many usernames can login at the same interface.

Perform the following configuration in interface (asynchronous serial, AUX or AM interface) view.

**Table 783** Configure Authentication for Modem Dial-In User

| Operation                                       | Command                 |
|-------------------------------------------------|-------------------------|
| Configure authentication for modem dial-in user | <b>modem-login</b>      |
| Delete authentication for modem dial-in user    | <b>undo modem-login</b> |

By default, the authentication for a modem dial-in user is not configured.

## Displaying and Debugging a Modem

Execute the **debugging** command in all views for the debugging.

**Table 784** Display and Debug Modem

| Operation                                          | Command                                                |
|----------------------------------------------------|--------------------------------------------------------|
| Enable debugging of the <b>AT</b> command of modem | <b>debugging modem at [ interface type number ]</b>    |
| Enable modem event debugging                       | <b>debugging modem event [ interface type number ]</b> |

## Modem Configuration Examples

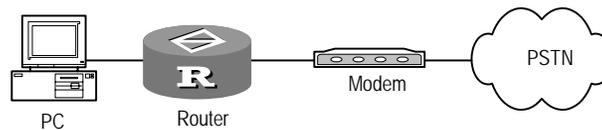
This section provides the following examples:

- Managing a Modem Through a Modem Script
- Power-on Initialization through the Initialization Script
- Use the Script to Dial Directly
- Authentication for Modem Dial-in User

### Managing a Modem Through a Modem Script

#### Configure a Modem adaptation baud rate

On the asynchronous interface connected to the modem, use a standard AT command to configure the modem baud rate, and send the "AT" command to the modem. If "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".

**Figure 241** Network of the configuration for the router to manage the modem

- 1 Configure a modem script.
 

```
[Router] script-string baud "" AT OK AT&W OK
```
- 2 Execute the corresponding script in interface view, supposing the modem is connected to the interface Serial0.
 

```
[Router] interface serial 0
[Router-Serial0] start-chat baud
```

## Restore the ex-factory modem settings

To restore the ex-factory modem settings, use the "AT&F" command.

```
[Router]script-string factory "" AT OK AT&F OK
[Router]interface serial 0
[Router-Serial0]start-chat factory
```

## Configure the modem initialization parameters

Correctly initializing the modem configuration is an important step for the correct connection with the modem. The following contents briefly introduce the conventional AT initialization commands and the works for initialization.

- When the negotiation is being carried out between modems, the modem speed must not be changed. Otherwise, the user should send an AT command to the remote modem so that the modem can be set to the new speed.
- The port speed must not change when a session is negotiated with a remote modem. If the speed of the port on the access server is changed, you must establish a direct Telnet session to the modem and send an AT command so that the modem can be set to the new speed.
- Modems differ in the method they use to lock the EIA/TIA-232 serial interface speed. Refer to the modem documentation to learn how the modem locks the modem speed (check the settings &b, \j, &q, \n, or s-register settings).
- The modem must use the data carrier detect (DCD) to indicate when a connection is established with a remote end. Most modems use the &c1 command to implement the configuration. Refer to the modem documentation for details.
- The modem must disconnect the modem active connections via the data terminal ready (DTR) signals. Most modems use &d2 or &d3 to implement the setting. Refer to the modem documentation for details.
- If the modem is required to access incoming calls, it must be configured with the number of off-hook ringing for incoming calls. The user should not to adopt the ringing auto-answer mode. S0=0 is adopted to make the configuration for most of the modems. For details, please refer to the modem operation manuals provided by the related manufacturers.

Considering the previously listed situations, the following initialization string is designed for typical applications:

```
AT&b1&c1&d2&s0=0
```

The initialization string enables the following functions:

- Locks the speed of the modem to the serial interface speed
- Enables DCD
- Enables disconnection of DTR
- Configures the non-auto answer

```
[Router]script-string init "" AT&b1&c1&d2&s0=0 OK
[Router]interface serial 0
[Router-Serial0]start-chat init
```

### Power-on Initialization through the Initialization Script

Enable the router to initialize the modem to which the asynchronous interface is connected when powering on the router or rebooting it.

```
[Router] script-string init "" AT OK AT&B1&C1&D2&S0=1 OK AT&W OK
[Router] interface async 0
[Router-Async0] modem
[Router-Async0] start-chat init
```

### Use the Script to Dial Directly

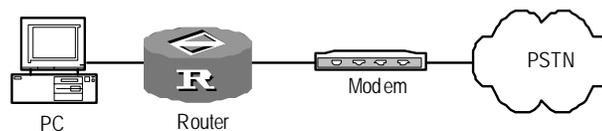
Configure a modem script and direct dial.

```
[Router] script-string dial "" AT OK ATDT8810058 CONNECT
[Router] interface async 0
[Router-Async0] modem
[Router-Async0] start-chat dial
```

### Authentication for Modem Dial-in User

Before logging in network through dialing, multiple users who connect with modem are authenticated on 3Com router based on username and password. Only the authenticated users can logging in network, and those who have failed the authentication are not allowed to log in.

Figure 242 Network of authentication for modem dial-in user



#### 1 Configure a modem script.

```
[Router] script-string welcome "" "Welcome use 3Com router!"
```

#### 2 Configure a modem user, and enable AAA authentication.

```
[Router] local-user testuser password simple testuser service
exec-operator
[Router] aaa-enable
[Router] aaa authentication-scheme login default local
[Router] aaa accounting-scheme optional
```

#### 3 Execute specified script in serial0 interface view.

```
[Router] interface serial 0
[Router-Serial0] modem-login
[Router-Serial0] script trigger connect welcome
[Router-Serial0] undo modem auto-answer
```

## Troubleshooting

**The modem is in abnormal status (such as the dial tone or busy tone remains for a long time).**

Do the following:

- 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, proceed to run the **AT** string, such as “AT&F OK ATE0S0=0&C1&D2 OK AT&W” on the router physical interface connected to the modem.

