



3Com[®] Switch 8800 Family Configuration Guide

Switch 8807
Switch 8810
Switch 8814

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

Copyright © 2007, 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 and the 3Com logo are registered trademarks of 3Com Corporation.

Cisco is a registered trademark of Cisco Systems, Inc.

Funk RADIUS is a registered trademark of Funk Software, Inc.

Aegis is a registered trademark of Aegis Group PLC.

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

IEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc.

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

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

CONTENTS

ABOUT THIS GUIDE

- Conventions 15
- Related Documentation 16

1 PRODUCT OVERVIEW

- Product Overview 17
- Function Features 18

2 COMMAND LINE INTERFACE

- Command Line Interface 21
- Command Line View 21
- Features and Functions of Command Line 29

3 LOGGING IN TO SWITCH

- Setting Up Configuration Environment through the Console Port 33
- Setting up Configuration Environment through Telnet 34
- Setting Up Configuration Environment through Modem Dial-up 37

4 USER INTERFACE CONFIGURATION

- User Interface Overview 39
- User Interface Configuration 40
- Displaying and Debugging User Interface 48

5 MANAGEMENT INTERFACE CONFIGURATION

- Management Interface Overview 49
- Management Interface Configuration 49

6 CONFIGURATION FILE MANAGEMENT

- Configuration File Management 51

7 VLAN CONFIGURATION

- VLAN Overview 55
- Configuring VLAN 55
- Configuring Protocol-Based VLAN 57
- Configuring IP Subnet-Based VLAN 58

Configure the CPU Port in an VLAN 58
Displaying and Debugging a VLAN 59
VLAN Configuration Example 59

8 SUPER VLAN CONFIGURATION

Super VLAN Overview 61
Configuring a Super VLAN 61

9 ISOLATE-USER-VLAN CONFIGURATION

Isolate-user-VLAN Overview 65
Isolate-use-vlan Configuration Task 65
Displaying and Debugging an isolate-user-VLAN 67
Isolate-user-VLAN Configuration Example 68

10 IP ADDRESS CONFIGURATION

Introduction to IP Addresses 71
Configuring IP Address 73
Displaying IP Address 76
IP Address Configuration Example 76
Troubleshooting IP Address Configuration 77

11 IP PERFORMANCE CONFIGURATION

Configuring IP Performance 79
Displaying and Debugging IP Performance 79
Troubleshooting IP Performance 81

12 GARP&GVRP CONFIGURATION

Configuring GARP 83
Configuring GVRP 85

13 ETHERNET PORT CONFIGURATION

Ethernet Port Overview 89
Ethernet Port Configuration 89
Setting the Interval of Performing Statistics on Ports 92
Displaying and Debugging Ethernet Port 98
Ethernet Port Configuration Example 98
Ethernet Port Troubleshooting 99

14 LINK AGGREGATION CONFIGURATION

Overview 101
Link Aggregation Configuration 104
Displaying and Debugging Link Aggregation 108
Link Aggregation Configuration Example 108

15 PORT ISOLATION CONFIGURATION

- Port Isolation Overview 111
- Configuration Tasks 111
- Port Isolation Configuration Example 113

16 MAC ADDRESS TABLE MANAGEMENT

- MAC Address Table Management Overview 115
- MAC Address Table Management Configuration 116
- Maximum MAC Address Number Learned by Ethernet Port and Forwarding Option Configuration 117
- Configuring Max Number of MAC Addresses that can be Learned in a VLAN 118
- Displaying and Debugging MAC Address Tables 119
- Resetting MAC Addresses 119
- MAC Address Table Management Configuration Example 119

17 MSTP REGION-CONFIGURATION

- Introduction to MSTP 121
- Configuring MSTP 132
- Displaying and Debugging MSTP 150
- Typical MSTP Configuration Example 152

18 DIGEST SNOOPING CONFIGURATION

- Introduction to Digest Snooping 155
- Digest Snooping Configuration 155

19 FAST TRANSITION

- Introduction 159
- Configuring Fast transition 160

20 BPDU TUNNEL CONFIGURATION

- BPDU Tunnel Overview 163
- Configuring BPDU Tunnel 163
- BPDU Tunnel Configuration Example 164

21 ACL CONFIGURATION

- ACL Overview 167
- ACL Configuration Tasks 169
- Displaying and Debugging ACL Configurations 176
- ACL Configuration Example 177

22 QoS CONFIGURATION

- QoS Overview 181
- Introduction to QoS Configuration Based on Port Groups 184
- QoS Configuration 188

QoS Configuration Example 202

23 LOGON USER ACL CONTROL CONFIGURATION

Overview 209

Configuring ACL for Telnet/SSH Users 209

Configuring ACL for SNMP Users 212

24 VLAN-ACL CONFIGURATION

VLAN-ACL Overview 215

VLAN-ACL Configuration 215

25 802.1X CONFIGURATION

802.1x Overview 221

802.1x Configuration 223

Displaying and Debugging 802.1x 229

Packet Attack Prevention Configuration 230

802.1x Configuration Example 230

26 AAA AND RADIUS/HWTACACS PROTOCOL CONFIGURATION

AAA and RADIUS/HWTACACS Protocol Overview 235

AAA Configuration 239

Configuring RADIUS Protocol 245

Configuring HWTACACS Protocol 256

Displaying and Debugging AAA and RADIUS Protocol 261

AAA and RADIUS/HWTACACS Protocol Configuration Examples 262

Troubleshooting AAA and RADIUS/HWTACACS 265

27 PORTAL CONFIGURATION

Portal Overview 267

Basic Portal Configuration 270

Portal Authentication-free User and Free IP Address Configuration 276

Portal Rate Limit Function Configuration 278

Portal User Deletion 278

28 IP ROUTING PROTOCOL OVERVIEW

Introduction to IP Route and Routing Table 279

Routing Management Policy 282

29 STATIC ROUTE CONFIGURATION

Introduction to Static Route 285

Configuring Static Route 286

Displaying and Debugging Static Route 287

Typical Static Route Configuration Example 288

Troubleshooting Static Route Faults 289

30 RIP CONFIGURATION

- Introduction to RIP 291
- Configuring RIP 292
- Displaying and Debugging RIP 300
- Typical RIP Configuration Example 300
- Troubleshooting RIP Faults 301

31 OSPF CONFIGURATION

- OSPF Overview 303
- OSPF GR Overview 307
- Configuring OSPF 311
- Displaying and Debugging OSPF 330
- Typical OSPF Configuration Example 331
- Troubleshooting OSPF Faults 336

32 INTEGRATED IS-IS CONFIGURATION

- Introduction to Integrated IS-IS 339
- Configuring Integrated IS-IS 343
- Displaying and Debugging Integrated IS-IS 358
- Typical Integrated IS-IS Configuration Example 359

33 BGP CONFIGURATION

- BGP/MBGP Overview 361
- Configuring BGP 364
- Displaying and Debugging BGP 383
- Typical BGP Configuration Examples 384
- Troubleshooting BGP 390

34 IP ROUTING POLICY CONFIGURATION

- Introduction to IP Routing Policy 393
- Configuring IP Routing Policy 394
- Displaying and Debugging the Routing Policy 401
- Typical IP Routing Policy Configuration Example 401
- Troubleshooting Routing Policy 402

35 ROUTE CAPACITY CONFIGURATION

- Route Capacity Configuration 405

36 RECURSIVE ROUTING CONFIGURATION

- Recursive Routing Configuration 407

37 IP MULTICAST OVERVIEW

- IP Multicast Overview 409

Implementation of IP Multicast 411
RPF Mechanism for IP Multicast Packets 414

38 STATIC MULTICAST MAC ADDRESS CONFIGURATION

Static Multicast MAC Address Overview 417
Configuring a Static Multicast MAC Address 417
Displaying and Maintaining Static Multicast MAC Address Configuration 418

39 IGMP SNOOPING CONFIGURATION

IGMP Snooping Overview 419
IGMP Snooping Configuration 422
Multicast Static Routing Port Configuration 426
Displaying and Maintaining IGMP Snooping 427
IGMP Snooping Configuration Example 427
Troubleshooting IGMP Snooping 428

40 MULTICAST VLAN CONFIGURATION

Multicast VLAN Overview 431
Multicast VLAN Configuration 431
Multicast VLAN Configuration Example 432

41 COMMON MULTICAST CONFIGURATION

Introduction to Common Multicast Configuration 435
Common Multicast Configuration 435
Managed multicast Configuration 437
Configuring Broadcast/Multicast Suppression 439
Displaying and Debugging Common Multicast Configuration 440

42 IGMP CONFIGURATION

IGMP Overview 441
Introduction to IGMP Proxy 442
IGMP Configuration 444
Displaying and Debugging IGMP 453

43 PIM-DM CONFIGURATION

PIM-DM Overview 455
PIM-DM Configuration 456
Displaying and Debugging PIM-DM 459
PIM-DM Configuration Example 460

44 PIM-SM CONFIGURATION

PIM-SM Overview 463
PIM-SM Configuration 465
Displaying and Debugging PIM-SM 469

PIM-SM Configuration Example 469

45 MSDP CONFIGURATION

MSDP Overview 473

MSDP Configuration 476

Displaying and Debugging MSDP 482

MSDP Configuration Examples 483

46 MBGP MULTICAST EXTENSION CONFIGURATION

MBGP Multicast Extension Overview 493

MBGP Multicast Extension Configuration 494

Displaying and Debugging MBGP Configuration 501

MBGP Multicast Extension Configuration Example 501

47 MPLS ARCHITECTURE

MPLS Overview 507

MPLS Basic Concepts 507

MPLS Architecture 510

48 MPLS BASIC CAPABILITY CONFIGURATION

MPLS Basic Capability Overview 515

MPLS Configuration 515

LDP Configuration 517

Displaying and Debugging MPLS Basic Capability 521

Typical MPLS Configuration Example 523

Troubleshooting MPLS Configuration 526

49 BGP/MPLS VPN CONFIGURATION

BGP/MPLS VPN Overview 529

BGP/MPLS VPN Configuration 537

Displaying and Debugging BGP/MPLS VPN 550

Typical BGP/MPLS VPN Configuration Example 552

Troubleshooting BGP/MPLS VPN Configuration 599

50 CARD INTERMIXING FOR MPLS SUPPORT

Overview 601

Restrictions in Intermixing Networking 602

Intermixing Configuration Task 603

Restrictions in Networking of Various MPLS Cards 611

51 MPLS VLL

MPLS L2VPN Overview 613

CCC MPLS L2VPN Configuration 616

Martini MPLS L2VPN Configuration 621

Kompella MPLS L2VPN Configuration	625
Displaying and Debugging MPLS L2VPN	629
Troubleshooting MPLS L2VPN	630

52 VPLS CONFIGURATION

VPLS Overview	633
Basic VPLS Network Architectures	634
VPLS Operational Principle	635
Concepts Related to VPLS	637
VPLS Basic Configuration	638
Displaying and Debugging VPLS	646
VPLS Basic Configuration Example	646
Troubleshooting VPLS	650

53 VRRP CONFIGURATION

Introduction to VRRP	653
Configuring VRRP	654
Displaying and debugging VRRP	659
VRRP Configuration Example	660
Troubleshooting VRRP	664

54 HA CONFIGURATION

Introduction to HA	667
Configuring HA	667
Displaying and Debugging HA Configuration	669
HA Configuration Example	670

55 ARP CONFIGURATION

Introduction to ARP	671
Configuring ARP	672
Displaying and Debugging ARP	675

56 ARP TABLE SIZE CONFIGURATION

Introduction to ARP Table Size Configuration	677
Configuring ARP Table Size Dynamically	678
Displaying ARP Table Size Configuration	678
Configuration Example	679

57 DHCP CONFIGURATION

Some Concepts about DHCP	681
Configuring General DHCP	684
Configuring DHCP Server	686
Configuring DHCP Relay	698
DHCP Option 82 Configuration	702

58 DNS CONFIGURATION

- Introduction to DNS 709
- Configuring Static Domain Name Resolution 710
- Configuring Dynamic Domain Name Resolution 710
- Displaying and Debugging Domain Name Resolution 711
- DNS Configuration Example 711
- Troubleshooting Domain Name Resolution Configuration 712

59 NETSTREAM CONFIGURATION

- Netstream Overview 713
- Netstream Configuration 714
- Netstream Configuration Examples 716

60 NDP CONFIGURATION

- Introduction to NDP 719
- Introduction to NDP Configuration Tasks 719
- NDP Configuration Example 721

61 POE CONFIGURATION

- PoE Overview 723
- PoE Configuration 724
- Comprehensive Configuration Example 726

62 POE PSU SUPERVISION CONFIGURATION

- Introduction to PoE PSU Supervision 729
- AC Input Alarm Thresholds Configuration 729
- DC Output Alarm Thresholds Configuration 730
- Displaying PoE Supervision Information 731
- PoE PSU Supervision Configuration Example 731

63 UDP HELPER CONFIGURATION

- Overview 733
- Configuring UDP Helper 733
- Displaying UDP Helper 735

64 SNMP CONFIGURATION

- SNMP Overview 737
- SNMP Versions and Supported MIB 737
- Configuring SNMP 738
- Displaying and Debugging SNMP 743
- SNMP Configuration Example 743

65 RMON CONFIGURATION

- RMON Overview 747
- Configuring RMON 747
- Displaying and Debugging RMON 750
- RMON Configuration Example 751

66 NTP CONFIGURATION

- Brief Introduction to NTP 753
- NTP Configuration 755
- Displaying and Debugging NTP 760
- NTP Configuration Example 761

67 SSH TERMINAL SERVICE

- SSH Terminal Service 769
- SFTP Service 781

68 FILE SYSTEM MANAGEMENT

- File System Configuration 789

69 DEVICE MANAGEMENT

- Device Management Overview 793
- Device Management Configuration 793
- Displaying and Debugging Device Management 796
- Device Management Configuration Example 796

70 FTP&TFTP CONFIGURATION

- FTP Configuration 801
- TFTP Configuration 806

71 INFORMATION CENTER

- Information Center Function 811

72 SYSTEM MAINTENANCE AND DEBUGGING

- Basic System Configuration 835
- Displaying the Status and Information of the System 836
- System Debugging 836
- Testing Tools for Network Connection 838

73 PROTOCOL PORT SECURITY CONFIGURATION

- Introduction to Protocol Port Security 841

74 PACKET STATISTICS CONFIGURATION

Introduction to Egress Packet Statistics 843

75 ETHERNET PORT LOOPBACK DETECTION

Ethernet Port Loopback Detection Function 845

Configuring the Loopback Detection Function 845

Displaying and Maintaining the Loopback Detection Function 845

76 QINQ CONFIGURATION

QinQ Overview 847

VLAN VPN Configuration 849

VLAN VPN Configuration 849

Traffic Classification-Based Nested VLAN Configuration 850

Adjusting TPID Values for QinQ Packets 853

VLAN-VPN Tunnel Configuration 855

77 NQA CONFIGURATION

Introduction to NQA 861

NQA Configuration 861

Displaying and Maintaining NQA 865

78 PASSWORD CONTROL CONFIGURATION

Introduction to Password Control Configuration 867

79 ACRONYMS

ABOUT THIS GUIDE

This guide describes the 3Com® Switch 8800 and how to install hardware, configure and boot software, and maintain software and hardware. This guide also provides troubleshooting and support information for your switch.

This guide is intended for Qualified Service personnel who are responsible for configuring, using, and managing the switches. It assumes a working knowledge of local area network (LAN) operations and familiarity with communication protocols that are used to interconnect LANs.



Always download the Release Notes for your product from the 3Com World Wide Web site and check for the latest updates to software and product documentation:

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

Conventions

Table 1 lists icon 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 lists text conventions that are used throughout this guide.

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."

Table 2 Text Conventions

Convention	Description
Words in <i>italics</i>	<p>Italics are used to:</p> <ul style="list-style-type: none"> Emphasize a point. Denote a new term at the place where it is defined in the text. Identify menu names, menu commands, and software button names. <p>Examples:</p> <ul style="list-style-type: none"> From the <i>Help</i> menu, select <i>Contents</i>. Click <i>OK</i>.
Words in bold	<p>Boldface type is used to highlight command names. For example, "Use the display user-interface command to..."</p>

Related Documentation

The following manuals offer additional information necessary for managing your Switch 8800:

- *Switch 8800 Command Reference Guide* — Provides detailed descriptions of command line interface (CLI) commands, that you require to manage your Switch 8800.
- *Switch 8800 Configuration Guide*— Describes how to configure your Switch 8800 using the supported protocols and CLI commands.
- *Switch 8800 Release Notes* — Contains the latest information about your product. If information in this guide differs from information in the release notes, use the information in the *Release Notes*.

These documents are available in Adobe Acrobat Reader Portable Document Format (PDF) on the 3Com World Wide Web site:

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

1

PRODUCT OVERVIEW

Product Overview

The 3Com Switch 8800 Family Series Routing Switches (hereinafter referred to as Switch 8800 Family series) are a series of large capacity, modularized L2/L3 switches. They are mainly designed for broadband MAN, backbone, switching core and convergence center of large-sized enterprise network and campus network. They provide diverse services and can be used in constructing stable and high-performance IP network. The series include the following main models:

- Switch 8807 routing switch
- Switch 8810 routing switch
- Switch 8814 routing switch

Switch 8800 Family series use integrated chassis, which can be subdivided into power supply area, module area, backplane and fan area.

For Switch 8807, in the module area, there are seven slots: the top two (slot0, slot1) accommodate fabric modules, which are in 1+1 redundancy; the remaining five accommodate I/O Modules.

For Switch 8810, in the module area, there are 10 slots: the two (slot4, slot5) in the middle accommodate fabric modules, which are in 1+1 redundancy; the remaining 8 accommodate I/O Modules.

For Switch 8814, in the module area, there are 14 slots: the two (slot6, slot7) in the middle accommodate fabric modules, which are in 1+1 redundancy; the remaining 12 accommodate I/O Modules, which can be hybrid. For specific configurations of the hybrid modules, refer to the "BGP/MPLS VPN Configuration" section of the MPLS module.

Switch 8800 Family series support the following services:

- Internet broadband access
- MAN, enterprise/campus networking
- Providing multicast service and multicast routing and supporting multicast audio and video services.

Function Features

Table 1 Function features

Features	Implementation
VLAN	VLAN compliant with IEEE 802.1Q Standard
	Port-based, protocol-based, and IP subnet-based VLAN
	GARP VLAN registration protocol (GVRP)
	Super VLAN
	VLAN isolation
	Guest VLAN
STP protocol	Dynamic VLAN
	spanning tree protocol (STP)/rapid spanning tree protocol (RSTP)/multiple spanning tree protocol (MSTP), compliant with IEEE 802.1D/IEEE 802.1w/IEEE 802.1s Standard
Flow control	IEEE 802.3x flow control (full-duplex)
	Back-pressure-based flow control (half-duplex)
Broadcast storm control	Broadcast storm control
	Multicast control
Multicast	Internet group management protocol snooping (IGMP snooping)
	Internet group management protocol (IGMP v2)
	Protocol-independent multicast-dense mode (PIM-DM)
	Protocol-independent multicast-sparse mode (PIM-SM)
	Multicast source discovery protocol (MSDP)
	Multiprotocol BGP (MBGP)
	Any-RP
	Static route
	Routing information protocol (RIP) v1/v2
	Open shortest path first (OSPF)
IP routing	Border gateway protocol (BGP)
	Intermediate system-to-intermediate system intra-domain routing information exchange protocol (IS-IS)
	Equivalent routes
	Policy-based routing
	IP routing policy
	OSPF/IS-IS/BGP graceful restart (GR)
	Inter-card link aggregation
Link aggregation	LACP
	Dynamic host configuration protocol (DHCP) relay
DHCP	DHCP server
	DHCP Option82 and Option60
Mirroring	Supports the port-based inter-card mirroring and flow-based inter-card mirroring
	Flow mirroring (packets can be duplicated to CPU and other ports)

Table 1 Function features

Features	Implementation
MPLS	<p>L3 multiprotocol label switching (MPLS) VPN (option1/2/3), embedded MPLS VPN, hierarchical PE (HoPE), CE dual homing, MCE, and multi-role host</p> <p>VLL, including Martini, Kompella and CCC modes</p> <p>VPLS</p>
Quality of service (QoS)	<p>Supports different types of traffic classification, including port-based, VLAN-based, COS priority-based, IP address-based, TOS priority-based, DSCP priority-based, TCP/UDP port-based, protocol type-based, and class of service (CoS)-based traffic classification</p> <p>Traffic supervision. The granularity is 8 Kbps</p> <p>Traffic shaping</p> <p>Priority mark/Remark</p> <p>Queue scheduling: supports strict priority queuing (SP), weighted round robin (WRR), and SP+WRR</p> <p>Congestion avoidance algorithms Tail-Drop and WRED</p> <p>Supports up to eight priority queues per port</p> <p>Multi-level user management and password protection</p> <p>Password control</p> <p>802.1X authentication</p> <p>Packet filtering</p>
Security features	<p>Port-based receiving broadcast frame control and supports rate calculation in terms of bytes or packets</p> <p>Guards against attack through anti-virus protocol packets, such as DOS attack</p> <p>AAA/RADIUS/HWTACACS</p> <p>SSH 2.0</p> <p>Firewall Application Module and IPsec Application Module</p> <p>Portal</p> <p>Accounting of education networks</p>
Dedicated service processing	Netstream
QinQ	<p>Port-based VLAN VPN</p> <p>Selective QinQ</p>

Table 1 Function features

Features	Implementation
Management and Maintenance	Command line interface configuration
	Local configuration through the Console port and the AUX port
	Local and remote configuration through Telnet on an Ethernet port
	Remote configuration through modem dialup through the AUX port.
	SNMP management (supports 3Com's network management products, remote monitoring (RMON) MIB group 1, 2, 3 and 9)
	VPN manager (a MPLS VPN network management tool)
	System logs
	Hierarchical alarms
	Output of the debugging information
	Ping and Tracert
Loading and updating	Network Quality Assurance (NQA)
	Supports to load and upgrade software through the XModem protocol
	Supports to load and upgrade software through the file transfer protocol (FTP) and the trivial file transfer protocol (TFTP)
	Simultaneous loading of BootROM and host software

2

COMMAND LINE INTERFACE

Command Line Interface

3Com series switches provide a series of configuration commands and command line interfaces for configuring and managing the switch. The command line interface has the following characteristics:

- Local configuration via the Console port and AUX port.
- Local or remote configuration via Telnet.
- Remote configuration through dialing with modem via the AUX port.
- Hierarchy command protection to avoid the unauthorized users accessing switch.
- Enter a "?" to get immediate online help.
- Provide network testing commands, such as Tracert and Ping, to fast troubleshoot the network.
- Provide various detailed debugging information to help with network troubleshooting.
- Log in and manage other switch directly, using the Telnet command.
- Provide FTP service for the users to upload and download files.
- Provide the function similar to Doskey to execute a history command.
- The command line interpreter searches for target not fully matching the keywords. It is ok for you to key in the whole keyword or part of it, as long as it is unique and not ambiguous.

Command Line View

3Com series switches provide hierarchy protection for the command lines to avoid unauthorized user accessing illegally.

Commands are classified into four levels, namely visit level, monitoring level, configuration level and management level. They are introduced as follows:

- Visit level: Commands of this level involve command of network diagnosis tool (such as **ping** and **tracert**), command of switch between different language environments of user interface (**language-mode**) and the **telnet** command. The operation of saving configuration file is not allowed on this level of commands.
- Monitoring level: Commands of this level, including the **display** command and the **debugging** command, are used to system maintenance, service fault diagnosis, etc. The operation of saving configuration file is not allowed on this level of commands.

- Configuration level: Service configuration commands, including routing command and commands on each network layer, are used to provide direct network service to the user.
- Management level: They are commands that influence basis operation of the system and system support module, which plays a support role on service. Commands of this level involve file system commands, FTP commands, TFTP commands, XModem downloading commands, user management commands, and level setting commands.

At the same time, login users are classified into four levels that correspond to the four command levels respectively. After users of different levels log in, they can only use commands at the levels that are equal to or lower than its own level.

In order to prevent unauthorized users from illegal intrusion, user will be identified when switching from a lower level to a higher level with **super [level]** command. User ID authentication is performed when users at lower level switch to users at higher level. In other words, user password of the higher level is needed (Suppose the user has set the **super password [level level] { simple | cipher } password**.) For the sake of confidentiality, on the screen the user cannot see the password that he entered. Only when correct password is input for three times, can the user switch to the higher level. Otherwise, the original user level will remain unchanged.

Different command views are implemented according to different requirements. They are related to one another. For example, after logging in the switch, you will enter user view, in which you can only use some basic functions such as displaying the running state and statistics information. In user view, key in **system-view** to enter system view, in which you can key in different configuration commands and enter the corresponding views.

The command line provides the following views:

- User view
- System view
- Port view
- VLAN view
- VLAN interface view
- Local-user view
- User interface view
- FTP Client command view
- SFTP Client view
- MST region view
- PIM view
- MSDP view
- IPv4 multicast sub-address family view
- RIP view
- OSPF view

- OSPF area view
- BGP view
- IS-IS view
- Route policy view
- Basic ACL view
- Advanced ACL view
- Layer-2 ACL view
- Conform-level view
- WRED index view
- RADIUS server group view
- ISP domain view
- MPLS view
- VPNv4 sub-address family view
- VPN-instance sub-address family view
- BGP-VPNv4 sub-address family view
- MPLS L2VPN view
- L2VPN address family view
- Route-Policy view
- vpn-instance view
- OSPF protocol view
- Remote-peer view
- VSI-LDP view
- VSI view
- HWTACACS view
- Port group view

The following table describes the function features of different views and the ways to enter or quit. Port numbers are only for examples.

Table 2 Function feature of command view

Command view	Function	Prompt	Command to enter	Command to exit
User view	Show the basic information about operation and statistics	<SW8800>	Enter right after connecting the switch	Use quit to end the disconnection with the switch
System view	Configure system parameters	[SW8800]	Key in system-view in user view	Use quit or return to return to user view

Table 2 Function feature of command view

Command view	Function	Prompt	Command to enter	Command to exit
		[3Com-Ethernet2/1/1]	100M Ethernet port view Key in interface ethernet 2/1/1 in system view	
Port view	Ethernet port view: Configure Ethernet port parameters	[3Com-GigabitEthernet2/1/1]	GigabitEthernet port view Key in interface gigabitethernet 2/1/1 in system view	Use quit to return to system view
		[3Com-GigabitEthernet2/1/1]	10G Ethernet port view Key in interface gigabitethernet 2/1/1 in system view	Use return to return to user view
VLAN view	Configure VLAN parameters	[3Com-Vlan1]	Key in vlan 1 in system view	Use quit to return to system view Use return to return to user view
VLAN interface view	Configure IP interface parameters for a VLAN or a VLAN aggregation	[3Com-Vlan-interface1]	Key in interface vlan-interface 1 in system view	Use quit to return to system view Use return to return to user view
Local-user view	Configure local user parameters	[3Com-luser-user1]	Key in local-user user1 in system view	Use quit to return to system view Use return to return to user view
User interface view	Configure user interface parameters	[3Com-ui0]	Key in user-interface 0 in system view	Use quit to return to system view Use return to return to user view
FTP client command view	Configure FTP Client parameters	[ftp]	Key in ftp in user view	Use quit to return to system view

Table 2 Function feature of command view

Command view	Function	Prompt	Command to enter	Command to exit
SFTP Client view	Configure SFTP Client parameters	<sftp-client>	Key in sftp ip-address in system view	Use quit to return to system view Use return to return to user view
MST region view	Configure MST region parameters	[3Com-mst-region]	Key in stp region-configuration in system view	Use quit to return to system view Use return to return to user view
PIM view	Configure PIM parameters	[3Com-PIM]	Key in pim in system view	Use quit to return to system view Use return to return to user view
MSDP view	Configure MSDP parameters	[3Com-msdp]	Key in msdp in system view	Use quit to return to system view Use return to return to user view
IPv4 multicast sub-address family view	Enter the IPv4 multicast sub-address family view to configure MBGP multicast extension parameters	[3Com-bgp-af-mul]	Key in ipv4-family multicast in BGP view	Use quit to return to BGP view Use return to return to user view
RIP view	Configure RIP parameters	[3Com-rip]	Key in rip in system view	Use quit to return to system view Use return to return to user view
OSPF view	Configure OSPF parameters	[3Com-ospf-1]	Key in ospf in system view	Use quit to return to system view Use return to return to user view
OSPF area view	Configure OSPF area parameters	[3Com-ospf-1-area-0 .0.0.1]	Key in area 1 in OSPF view	Use quit to return to OSPF view Use return to return to user view

Table 2 Function feature of command view

Command view	Function	Prompt	Command to enter	Command to exit
BGP view	Configure BGP parameters	[3Com-bgp]	Key in bgp 100 in system view	Use quit to return to system view Use return to return to user view
IS-IS view	Configure IS-IS parameters	[3Com-isis]	Key in isis in system view	Use quit to return to system view Use return to return to user view
Route policy view	Configure route policy parameters	[3Com-route-policy]	Key in route-policy policy1 permit node 10 in system view	Use quit to return to system view Use return to return to user view
Basic ACL view	Define the rule of basic ACL	[3Com-acl-basic-2000]	Key in acl number 2000 in system view	Use quit to return to system view Use return to return to user view
Advanced ACL view	Define the rule of advanced ACL	[3Com-acl-adv-3000]	Key in acl number 3000 in system view	Use quit to return to system view Use return to return to user view
Layer-2 ACL view	Define the rule of layer-2 ACL	[3Com-acl-link-4000]	Key in acl number 4000 in system view	Use quit to return to system view Use return to return to user view
Conform-level view	Configure the "DSCP + Conform-level Service group" mapping table and "EXP + Conform-level->service parameters" mapping table and "Local-precedence + Conform-level 802.1p priority" mapping table	[3Com-conform-level-0]	Key in qos conform-level 0 in system view	Use quit to return to system view Use return to return to user view

Table 2 Function feature of command view

Command view	Function	Prompt	Command to enter	Command to exit
WRED index view	Configure WRED parameters	[3Com-wred-0]	Key in wred 0 in system view	Use quit to return to system view Use return to return to user view
RADIUS server group view	Configure radius parameters	[3Com-radius-1]	Key in radius scheme 1 in system view	Use quit to return to system view Use return to return to user view
ISP domain view	Configure ISP domain parameters	[3Com-isp-3Com163.net]	Key in domain 3Com163.net in system view	Use to return to system view Use return to return to user view
MPLS view	Configure MPLS parameters	[3Com-mpls]	Key in mpls in system view	Use quit to return to system view Use return to return to user view
VPNv4 sub-address family view	Configure VPNv4 address family parameters	[3Com-bgp-af-vpn]	Key in ipv4-family vpnv4 in BGP view	Use quit to return to system view Use return to return to user view
VPN-instance sub-address family view	Configure VPN instance sub-address family parameters	[3Com-bgp-af-vpn-in-stance]	Key in ipv4-family vpn-instance vpna in BGP/RIP view	Use quit to return to system view Use return to return to user view
BGP-VPNv4 sub-address family view	Configure BGP-VPNv4 sub-address family parameters	[3Com-bgp-af-vpn]	Key in ipv4-family vpn-instance in BGP/RIP view	Use quit to return to system view Use return to return to user view
MPLS L2VPN view	Configure MPLS L2VPN service parameters	[3Com-mpls-l2vpn-v-pna]	Key in mpls l2vpn vpna encapsulation Ethernet in system view	Use quit to return to system view Use return to return to user view
L2VPN address family view	Configure L2VPN service parameters	[3Com-bgp-af-l2vpn]	Key in l2vpn-family in BGP view	Use quit to return to system view Use return to return to user view

Table 2 Function feature of command view

Command view	Function	Prompt	Command to enter	Command to exit
Route-Policy view	Configure Route-Policy service parameters	[3Com-route-policy]	Key in route-policy <i>route-policy-name</i> { permit deny } node <i>node-number</i> in system view	Use quit to return to system view Use return to return to user view
vpn-instance view	Configure vpn-instance parameters	[3Com-vpn-vpn-instance_blue]	Key in ip vpn-instance vpn-instance_vpn <i>vpn</i> in system view	Use quit to return to system view Use return to return to user view
OSPF protocol view	Configure OSPF protocol parameters	[3Com-ospf-100]	Key in ospf <i>process-id</i> [router-id <i>router-id-number</i>] [vpn-instance <i>vpn-instance-name</i>] in system view	Use quit to return to system view Use return to return to user view
Remote-peer view	Configure MPLS peer group parameters	[3Com-mpls-remote 1]	Key in mpls remote 1	Use quit to return to system view Use return to return to user view
VSI-LDP view	Configure some VPLS features	[8500-vsi-3Com-ldp]	Key in vsi 3Com in system view Key in pwsignal ldp in vsi view	Use quit to return to vsi view Use return to return to user view
VSI view	Specify VPLS mode	[8500-vsi-3Com]	Key in vsi 3Com in system view	Use quit to return to system view Use return to return to user view
HWTACACS view	Configure HWTACACS protocol parameters	[8500-hwtacacs-3Com]	Key in hwtacacs scheme 3Com in system view	Use quit to return to system view Use return to return to user view
Port group view	Combine the ports with the same configuration, omitting repeated configuration procedure	[8500-port-group X]	Key in port-group X in system view	Use quit to return to system view Use return to return to user view

Features and Functions of Command Line

Online Help of Command Line

The command line interface provides the following online help modes.

- Full help
- Partial help

You can get the help information through these online help commands, which are described as follows.

- 1 Input "?" in any view to get all the commands in it and corresponding descriptions.

```
<SW8800> ?
User view commands:
 language-mode Specify the language environment
 ping           Ping function
 quit          Exit from current command view
 super         Privilege current user a specified priority level
 telnet        Establish one TELNET connection
 tracert       Trace route function
```

- 2 Input a command with a "?" separated by a space. If this position is for keywords, all the keywords and the corresponding brief descriptions will be listed.

```
<SW8800> language-mode ?
 chinese Chinese environment
 english English environment
```

- 3 Input a command with a "?" separated by a space. If this position is for parameters, all the parameters and their brief descriptions will be listed.

```
[SW8800] garp timer leaveall ?
 INTEGER<65-32765> Value of timer in centiseconds
                   (LeaveAllTime > (LeaveTime [On all ports]))
                   Time must be multiple of 5 centiseconds
[SW8800] garp timer leaveall 300 ?
 <cr>
```

<cr> indicates no parameter in this position. The next command line repeats the command, you can press <Enter> to execute it directly.

- 4 Input a character string with a "?", then all the commands with this character string as their initials will be listed.

```
<SW8800> p?
 ping  pwd
```

- 5 Input a command with a character string and "?", then all the key words with this character string as their initials in the command will be listed.

```
<SW8800> display ver?
 version
```

- 6 Input the first letters of a keyword of a command and press <Tab> key. If no other keywords are headed by this letters, then this unique keyword will be displayed automatically.

- 7 To switch to the Chinese display for the above information, perform the language-mode command.

Displaying Characteristics of Command Line

Command line interface provides the following display characteristics:

- For users’ convenience, the instruction and help information can be displayed in both English and Chinese.
- For the information to be displayed exceeding one screen, pausing function is provided. In this case, users can have three choices, as shown in the table below.

Table 3 Functions of displaying

Key or Command	Function
Press <Ctrl+C> when the display pauses	Stop displaying and executing command.
Enter a space when the display pauses	Continue to display the next screen of information.
Press <Enter> when the display pauses	Continue to display the next line of information.

History Command of Command Line

Command line interface provides the function similar to that of DosKey. The commands entered by users can be automatically saved by the command line interface and you can invoke and execute them at any time later. History command buffer is defaulted as 10. The operations are shown in the table below.

Table 4 Retrieve history command

Operation	Key	Result
Display history command	display history-command	Display history command by user inputting
Retrieve the previous history command	Up cursor key <,Üè> or <Ctrl+P>	Retrieve the previous history command, if there is any.
Retrieve the next history command	Down cursor key <,Üi> or <Ctrl+N>	Retrieve the next history command, if there is any.



Cursor keys can be used to retrieve the history commands in Windows 3.X Terminal and Telnet. However, in Windows 9X HyperTerminal, the cursor keys ,Üè and ,Üi do not work, because Windows 9X HyperTerminal defines the two keys differently. In this case, use the combination keys <Ctrl+P> and <Ctrl+N> instead for the same purpose.

Common Command Line Error Messages

All the input commands by users can be correctly executed, if they have passed the grammar check. Otherwise, error messages will be reported to users. The common error messages are listed in the following table.

Table 5 Common command line error messages

Error messages	Causes
Unrecognized command	Cannot find the command.
	Cannot find the keyword.
	Wrong parameter type.
	The value of the parameter exceeds the range.

Table 5 Common command line error messages

Error messages	Causes
Incomplete command	The input command is incomplete.
Too many parameters	Enter too many parameters.
Ambiguous command	The parameters entered are not specific.

Editing Characteristics of Command Line

Command line interface provides the basic command editing function and supports to edit multiple lines. A command cannot longer than 256 characters. See the table below.

Table 6 Editing functions

Key	Function
Common keys	Insert from the cursor position and the cursor moves to the right, if the edition buffer still has free space.
Backspace	Delete the character preceding the cursor and the cursor moves backward.
Leftwards cursor key <,Üê> or <Ctrl+B>	Move the cursor a character backward
Rightwards cursor key <,Üí> or <Ctrl+F>	Move the cursor a character forward
Up cursor key <,Üë> or <Ctrl+P>	Retrieve the history command.
Down cursor key <,Üì> or <Ctrl+N>	
<Tab>	Press <Tab> after typing the incomplete key word and the system will execute the partial help: If the key word matching the typed one is unique, the system will replace the typed one with the complete key word and display it in a new line; if there is not a matched key word or the matched key word is not unique, the system will do no modification but display the originally typed word in a new line.

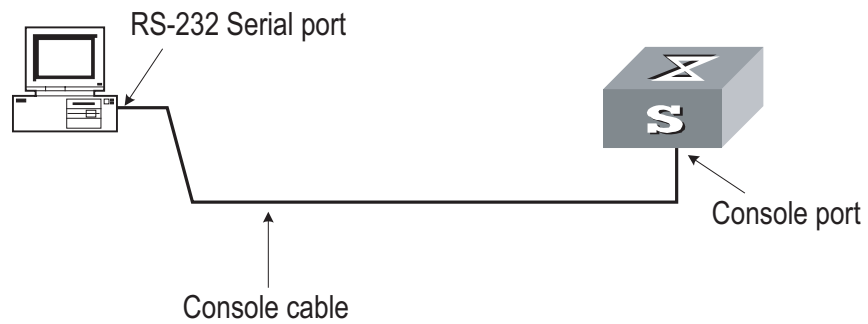
3

LOGGING IN TO SWITCH

Setting Up Configuration Environment through the Console Port

Step 1: As shown in the figure below, to set up the local configuration environment, connect the serial port of a PC (or a terminal) to the Console port of the switch with the Console cable.

Figure 1 Set up the local configuration environment through the Console port



Step 2: Run a terminal emulator (such as Terminal of Windows 3X or HyperTerminal of Windows 9X) on the computer. Set the terminal communication parameters as follows: Set "Bits per second" to "9600", "Data bits" to "8", "Parity" to "none", "Stop bits" to "1", and "Flow control" to "none", and select the "VT100" as the terminal type.

Figure 2 Set up new connection

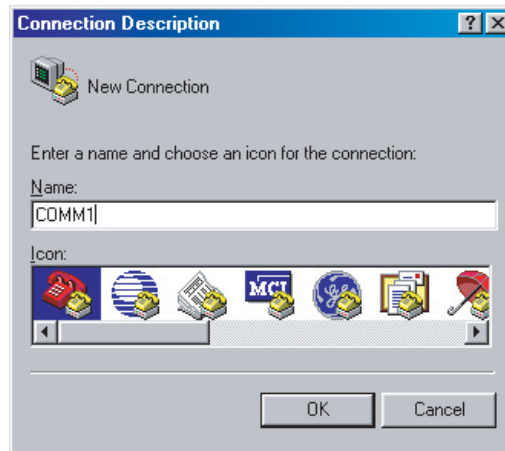
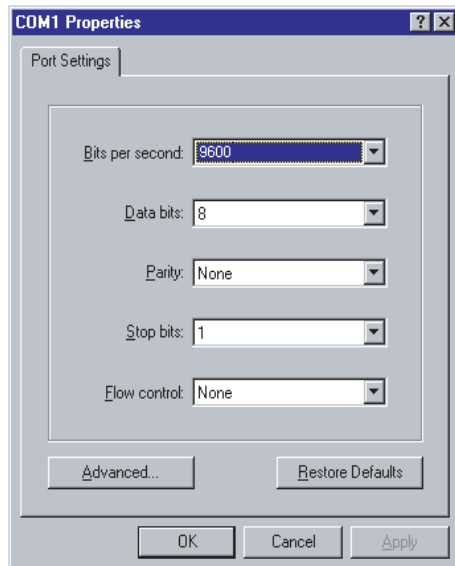


Figure 3 Configure the port for connection



Figure 4 Set communication parameters



Step 3: The switch is powered on. Display self-test information of the switch and prompt you to press Enter to show the command line prompt such as <SW8800>.

Step 4: Input a command to configure the switch or view the operation state. Input a "?" for help. For details of specific commands, refer to the following chapters.

Setting up Configuration Environment through Telnet

Connecting a PC to the Switch through Telnet

After you have correctly configured IP address of a VLAN interface for a switch via Console port (using **ip address** command in VLAN interface view), and added the port (that connects to a terminal) to this VLAN (using **port** command in VLAN view), you can telnet this switch and configure it.

Step 1: Before logging into the switch through telnet, you need to configure the Telnet user name and password on the switch through the console port.

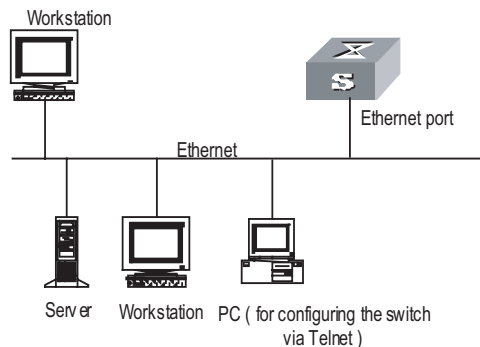


By default, the password is required for authenticating the Telnet user to log in to the switch. If a user logs in via the Telnet without password, he will see the prompt "Login password has not been set !".

```
<SW8800> system-view
Enter system view , return user view with Ctrl+Z.
[SW8800] user-interface vty 0
[3Com-ui-vty0] set authentication password simple xxxx (xxxx is the
login password of Telnet user)
```

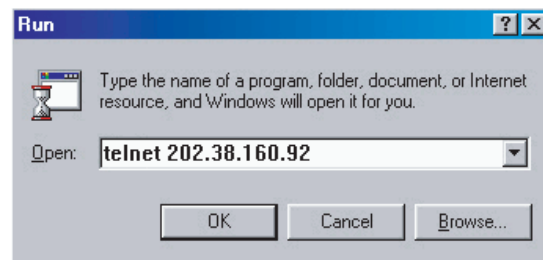
Step 2: To set up the configuration environment, connect the Ethernet port of the PC to that of the switch via the LAN, as shown in Figure 5.

Figure 5 Set up configuration environment through telnet



Step 3: Run Telnet on the PC and input the IP address of the VLAN connected to the PC port, as shown in Figure 6.

Figure 6 Run Telnet



Step 4: The terminal displays "Login authentication!" and prompts the user to input the logon password. After you input the correct password, it displays the command line prompt (such as <SW8800>). If the prompt "All user interfaces are used, please try later! The connection was closed by the remote host!" appears, it indicates that the maximum number of Telnet users that can be accessed to the switch is reached at this moment. In this case, please reconnect later. At most 5 Telnet users are allowed to log on to the 3Com series switches simultaneously.

Step 5: Use the corresponding commands to configure the switch or to monitor the running state. Enter "?" to get the immediate help. For details of specific commands, refer to the following chapters.



- When configuring the switch via Telnet, do not modify the IP address of it unless necessary, for the modification might cut the Telnet connection.
- By default, when a Telnet user passes the password authentication to log on to the switch, he can access the commands at Level 0.

Accessing a Switch through another Switch via Telnet

After a user has logged in to a switch, he or she can configure another switch through the switch via Telnet. The local switch serves as Telnet client and the peer switch serves as Telnet server. If the ports connecting these two switches are in a same local network, their IP addresses must be configured in the same network segment. Otherwise, the two switches must establish a route that can reach each other.

As shown in the figure below, after you telnet to a switch, you can run **telnet** command to log in and configure another switch.

Figure 7 Provide Telnet Client service



Step 1: Configure the Telnet user name and password on the Telnet Server through the console port.



By default, the password is required for authenticating the Telnet user to log in to the switch. If a user logs in via the Telnet without password, he will see the prompt "Login password has not been set !".

```
<SW8800> system-view
System View: return to User View with Ctrl+Z
[SW8800] user-interface vty 0
[3Com-ui-vty0] set authentication password simple xxxx (xxxx is the
login password of Telnet user)
```

Step 2: The user logs in the Telnet Client (switch). For the login process, refer to the section describing "Connecting a PC to the Switch through Telnet".

Step 3: Perform the following operations on the Telnet Client:

```
<SW8800> telnet xxxx (xxxx can be the hostname or IP address of the Telnet Server
. If it is the hostname, you need to use the ip host command to specify.)
```

Step 4: Enter the preset login password and you will see the prompt such <SW8800>. If the prompt "All user interfaces are used, please try later! The connection was closed by the remote host!" appears, it indicates that the maximum number of Telnet users that can be accessed to the switch is reached at this moment. In this case, please connect later.

Step 5: Use the corresponding commands to configure the switch or view its running state. Enter "?" to get the immediate help. For details of specific commands, refer to the following chapters.

Setting Up Configuration Environment through Modem Dial-up

Step 1: The modem user is authenticated via the Console port of the switch before he or she logs in to the switch through a dial-up Modem.



By default, the password is required for authenticating the Modem user to log in to the switch. If a user logs in via the Modem without password, he or she will see the prompt "Login password has not been set !".

```
<SW8800> system-view
System View: return to User View with Ctrl+Z..
[SW8800] user-interface aux 0
[3Com-ui-aux0] set authentication password simple xxxx (xxxx is the
login password of the Modem user.)
```

Step 2: As shown in the figure below, to set up the remote configuration environment, connect the Modems to a PC (or a terminal) serial port and the switch AUX port respectively.

Figure 8 Set up remote configuration environment

Step 3: Dial for connection to the switch, using the terminal emulator and Modem on the remote end. The number dialed shall be the telephone number of the Modem connected to the switch. See the two figures below.

Figure 9 Set the dialed number

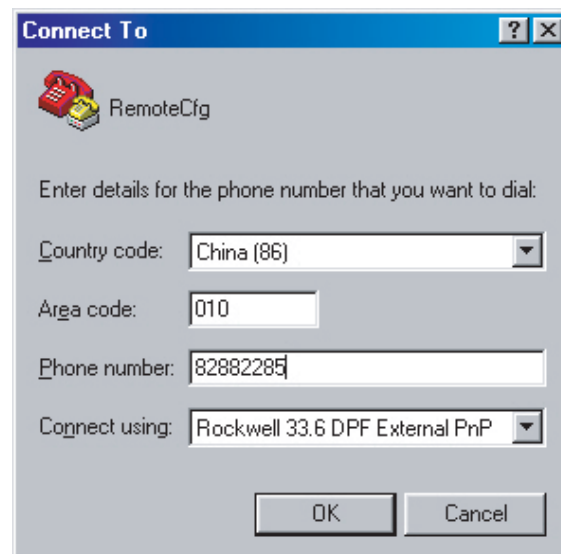
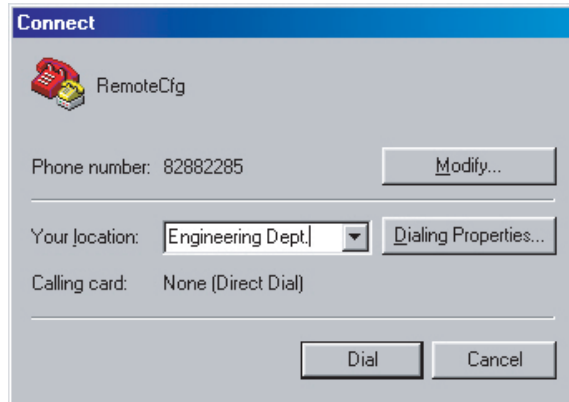


Figure 10 Dial on the remote PC

Step 4: Enter the preset login password on the remote terminal emulator and wait for the prompt such as <SW8800>. Then you can configure and manage the switch. Enter "?" to get the immediate help. For details of specific commands, refer to the following chapters.



By default, when a Modem user logs in, he can access the commands at Level 0.

4

USER INTERFACE CONFIGURATION

User Interface Overview

To facilitate system management, the switches support user interface based configuration for the configuration and management of port attributes. Presently, the Switch 8800 Family series switches support the following user interface based configuration methods:

- Local configuration via the Console port and AUX port
- Local and remote configuration through Telnet on Ethernet port
- Remote configuration through dialing with modem via the AUX port.

According to the above-mentioned configuration methods, there are three types of user interfaces:

- Console user interface

Console user interface is used to log in to the switch via the Console port. A switch can only have one Console user interface.

- AUX user interface

AUX user interface is used to log in to the switch locally or remotely with a modem via the AUX port. A switch can only have one AUX user interface. The local configuration for it is similar to that for the Console user interface.

- VTY user interface

VTY user interface is used to telnet the switch. A switch can have up to five VTY user interface.

User interface is numbered in the following two ways: absolute number and relative number.

Absolute number

The user interfaces of the Switch 8800 Family routing switch include three types, which are sequenced as follows: console interface (CON), auxiliary interface (AUX) and virtual interface (VTY). A switch has one CON, one AUX and multiple VTYS. The first absolute number is designated as 0; the second one is designated as 1; and so on. This method can specify a unique user interface or a group of interfaces.

It follows the rules below.

- Console user interface is numbered as the first interface designated as user interface 0.

- AUX user interface is numbered as the second interface designated as user interface 1.
- VTY is numbered after AUX user interface. The absolute number of the first VTY is incremented by 1 than the AUX user interface number.

Relative number

The relative number is in the format of "user interface type" + "number". The "number" refers to the internal number for each user interface type. This method can only specify one interface or one group of interfaces for a user interface type instead of different user interface types.

It follows the rules below:

- Number of Console user interface: console 0.
- Number of AUX user interface: AUX 0.
- Number of VTY: The first VTY interface is designated as VTY 0; the second one is designated as VTY 1, and so on.

User Interface Configuration

The following sections describe the user interface configuration tasks.

- "Entering User Interface View"
- "Define the Login Header"
- "Configuring Asynchronous Port Attributes"
- "Configuring Terminal Attributes"
- "Managing Users"
- "Configuring Modem Attributes"
- "Configuring Redirection"

Entering User Interface View

The following command is used for entering a user interface view. You can enter a single user interface view or multi user interface view to configure one or more user interfaces respectively.

Perform the following configuration in system view.

Table 7 Enter user interface view

Operation	Command
Enter a single user interface view or multi user interface views	user-interface [<i>type</i>] <i>first-number</i> [<i>last-number</i>]

Define the Login Header

The following command is used for configuring the displayed header when user login.

When the users log in to the switch, if a connection is activated, the **login** header will be displayed. After the user successfully logs in the switch, the **shell** header will be displayed.

Perform the following configuration in system view.

Table 8 Configure the login header.

Operation	Command
Configure the login header	header [shell incoming login] <i>text</i>
Remove the login header configured	undo header [shell incoming login]

Note that if you press <Enter> after typing any of the three keywords **shell**, **login** and **incoming** in the command, then what you type after the word header is the contents of the login information, instead of identifying header type.

Configuring Asynchronous Port Attributes

The following commands can be used for configuring the attributes of the asynchronous port in asynchronous interactive mode, including speed, flow control, parity, stop bit and data bit.

Perform the following configurations in user interface (Console and AUX user interface only) view.

Configuring the transmission speed

Table 9 Configure the transmission speed

Operation	Command
Configure the transmission speed	speed <i>speed-value</i>
Restore the default transmission speed	undo speed

By default, the transmission speed on an asynchronous port is 9600bps.

Configuring flow control

Table 10 Configure flow control

Operation	Command
Configure the flow control	flow-control { hardware none software }
Restore the default flow control mode	undo flow-control

By default, the flow control on an asynchronous port is none, that is, no flow control will be performed.

Configuring parity

Table 11 Configure parity

Operation	Command
Configure parity mode	parity { even mark none odd space }
Restore the default parity mode	undo parity

By default, the parity on an asynchronous port is none, that is, no parity bit.

Configuring the stop bit

Table 12 Configure the stop bit

Operation	Command
Configure the stop bit	stopbits { 1 1.5 2 }
Restore the default stop bit	undo stopbits

By default, an asynchronous port supports 1 stop bit.

Note that setting 1.5 stop bits is not available on Switch 8800 Family series at present.

Configuring the data bit

Table 13 Configure the data bit

Operation	Command
Configure the data bit	databits { 7 8 }
Restore the default data bit	undo databits

By default, an asynchronous port supports 8 data bits.

Configuring Terminal Attributes

The following commands can be used for configuring the terminal attributes, including enabling/disabling terminal service, disconnection upon timeout, lockable user interface, configuring terminal screen length and history command buffer size.

Perform the following configuration in user interface view. Perform **lock** command in user view.

Enabling/disabling terminal service

After the terminal service is disabled on a user interface, you cannot log in to the switch through the user interface. However, the user logged in through the user interface before disabling the terminal service can continue his operation. After such user logs out, he cannot log in again. In this case, a user can log in to the switch through the user interface only when the terminal service is enabled again.

Table 14 Enable/disable terminal service

Operation	Command
Enable terminal service	shell
Disable terminal service	undo shell

By default, terminal service is enabled on all the user interfaces.

Note the following points:

- For the sake of security, the **undo shell** command can only be used on the user interfaces other than Console user interface.
- You cannot use this command on the user interface via which you log in.
- You will be asked to confirm before using **undo shell** on any legal user interface.

Configuring idle-timeout

Table 15 Configure idle-timeout

Operation	Command
Configure idle-timeout	idle-timeout <i>minutes</i> [<i>seconds</i>]
Restore the default idle-timeout	undo idle-timeout

By default, `idle-timeout` is enabled and set to 10 minutes on all the user interfaces. That is, the user interface will be disconnected automatically after 10 minutes without any operation.

`idle-timeout 0` means disabling `idle-timeout`.

Locking user interface

This configuration is to lock the current user interface and prompt the user to enter the password. This makes it impossible for others to operate in the interface after the user leaves.

Table 16 Lock user interface

Operation	Command
Lock user interface	lock

Setting the screen length

If a command displays more than one screen of information, you can use the following command to set how many lines to be displayed in a screen, so that the information can be separated in different screens and you can view it more conveniently.

Table 17 Set the screen length

Operation	Command
Set the screen length	screen-length <i>screen-length</i>
Restore the default screen length	undo screen-length

Note that the number of lines that can be displayed in each screen remains the same when **screen-length** is set to 1 or 2.

By default, 24 lines (including the multi-screen identifier lines) are displayed in one screen when the multi-screen display function is enabled .

Use **screen-length 0** to disable the multi-screen display function.

Setting the history command buffer size

Table 18 Set the history command buffer size

Operation	Command
Set the history command buffer size	history-command max-size <i>value</i>
Restore the default history command buffer size	undo history-command max-size

By default, the size of the history command buffer is 10, that is, 10 history commands can be saved.

Managing Users

The management of users includes the setting of user logon authentication method, level of command which a user can use after logging on, level of command which a user can use after logging on from the specifically user interface, and command level.

Configuring the authentication method

The following command is used for configuring the user login authentication method to deny the access of an unauthorized user.

Perform the following configuration in user interface view.

Table 19 Configure the authentication method

Operation	Command
Configure the authentication method	authentication-mode { password scheme [command-authorization] none }

By default, terminal authentication is not required for local users log in via the Console port. However, password authentication is required for local users and remote Modem users to log in via the AUX port, and for Telnet users and the VTY users to log in through Ethernet port.



If the Console port is configured for local password authentication, the user can directly log in to the system even without a password configured; if other user interfaces, such as the AUX port and VTY interface, are configured for local password authentication, users cannot log in to the system without a password.

1 Perform local password authentication to the user interface

Using **authentication-mode password** command, you can perform local password authentication. That is, you need use the command below to configure a login password in order to login successfully.

Perform the following configuration in user interface view.

Table 20 Configure the local authentication password

Operation	Command
Configure the local authentication password	set authentication password { cipher simple } <i>password</i>
Remove the local authentication password	undo set authentication password

Configure for password authentication when a user logs in through a VTY 0 user interface and set the password to 3Com.

```
[SW8800] user-interface vty 0
[3Com-ui-vty0] authentication-mode password
[3Com-ui-vty0] set authentication password simple 3Com
```

2 Perform local or remote authentication of username and password to the user interface

Using **authentication-mode scheme** [**command-authorization**] command, you can perform local or remote authentication of username and password. The type of the authentication depends on your configuration. For detailed information, see "Security" section.

In the following example, local username and password authentication are configured.

Perform username and password authentication when a user logs in through VTY 0 user interface and set the username and password to zbr and 3Com respectively.

```
[3Com-ui-vty0] authentication-mode scheme
[3Com-ui-vty0] quit
[SW8800] local-user zbr
[3Com-luser-zbr] password simple 3Com
[3Com-luser-zbr] service-type telnet
```

3 No authentication

```
[3Com-ui-vty0] authentication-mode none
```



By default, password is required to be set for authenticating local users and remote Modem users log in via the AUX port, and Telnet users log in through Ethernet port. If no password has been set, the following prompt will be displayed "Login password has not been set !."

If the **authentication-mode none** command is used, the local and Modem users via the AUX port and Telnet users will not be required to input password.

Setting the command level used after a user logging in

The following command is used for setting the command level used after a user logging in.

Perform the following configuration in local-user view.

Table 21 Set the command level used after a user logging in

Operation	Command
Set command level used after a user logging in	service-type telnet [level level]
Restore the default command level used after a user logging in	undo service-type telnet

By default, the specified logon user can access the commands at Level 2.

Setting the command level used after a user logs in from a user interface

You can use the following command to set the command level after a user logs in from a specific user interface, so that a user is able to execute the commands at such command level.

Perform the following configuration in user interface view.

Table 22 Set the command level used after a user logging in from a user interface

Operation	Command
Set command level used after a user logging in from a user interface	user privilege level level
Restore the default command level used after a user logging in from a user interface	undo user privilege level

By default, you can access the commands at Level 3 after logging in through the Console user interface, and the commands at Level 0 after logging in through the AUX or VTY user interface.



When a user logs in the switch, the command level that it can access depends on two points. One is the command level that the user itself can access, the other is the set command level of this user interface. If the two levels are different, the former will be taken. For example, the command level of VTY 0 user interface is 1, however, you have the right to access commands of level 3; if you log in from VTY 0 user interface, you can access commands of level 3 and lower.

Setting the command priority

The following command is used for setting the priority of a specified command in a certain view. The command levels include visit, monitoring, configuration, and management, which are identified with 0 through 3 respectively. An administrator assigns authorities as per user requirements.

Perform the following configuration in system view.

Table 23 Set the command priority

Operation	Command
Set the command priority in a specified view.	command-privilege level <i>level</i> view <i>view</i> <i>command</i>
Restore the default command level in a specified view.	Undo command-privilege view <i>view</i> <i>command</i>

Setting input protocol for a user terminal

You can use the following command to set input protocol for a user terminal. The input protocol type can be TELNET, SSH or all.

Perform the following configuration in user interface view.

Table 24 Set input protocol for a user terminal

Operation	Command
Set input protocol for a user terminal	protocol inbound { all telnet ssh }

By default, the input protocol type for a user terminal is all.

Configuring Modem Attributes

When logging in the switch via the Modem, you can use the following commands to configure these parameters.

Perform the following configuration in AUX user interface view.

Table 25 Configure Modem attributes

Operation	Command
Set the interval since the system receives the RING until CD_UP	modem timer answer <i>seconds</i>
Restore the default interval since the system receives the RING until CD_UP	undo modem timer answer
Configure auto answer	modem auto-answer
Configure manual answer	undo modem auto-answer
Configure to allow call-in	modem call-in
Configure to bar call-in	undo modem call-in

Table 25 Configure Modem attributes

Operation	Command
Configure to permit call-in and call-out.	modem both
Configure to disable call-in and call-out	undo modem both

Configuring Redirection **Send command**

The following command can be used for sending messages between user interfaces.

Perform the following configuration in user view.

Table 26 Configure to send messages between different user interfaces.

Operation	Command
Configure to send messages between different user interfaces.	send { all number type number }

Auto-execute command

The following command is used to automatically run a command after you log in. After a command is configured to be run automatically, it will be automatically executed when you log in again.

This command is usually used to automatically execute **telnet** command on the terminal, which will connect the user to a designated device automatically.

Perform the following configuration in user interface view.

Table 27 Configure to automatically run the command

Operation	Command
Configure to automatically run the command	auto-execute command text
Configure not to automatically run the command	undo auto-execute command

Note the following points:

- After executing this command, the user interface can no longer be used to carry out the routine configurations for the local system. Use this command with caution.
- Make sure that you will be able to log in to the system in some other way and cancel the configuration, before you use the **auto-execute command** command and save the configuration.

Telnet 10.110.100.1 after the user logs in through VTY0 automatically.

```
[3Com-ui-vty0] auto-execute command telnet 10.110.100.1
```

When a user logs on via VTY 0, the system will run **telnet 10.110.100.1** automatically.

Displaying and Debugging User Interface

After the above configuration, execute **display** command in any view to display the running of the user interface configuration, and to verify the effect of the configuration.

Execute **free** command in user view to release the user interface connection.

Table 28 Display and debug user interface

Operation	Command
Release a specified user interface connection	free user-interface [<i>type</i>] <i>number</i>
Display the user application information of the user interface	display users [all]
Display the physical attributes and some configurations of the user interface	display user-interface [<i>type number</i> <i>number</i>] [summary]
Query history commands selectively	display history-command [<i>Command-Number</i>] [{ begin include exclude } <i>Match-string</i>]

5

MANAGEMENT INTERFACE CONFIGURATION

Management Interface Overview

Switch 8800 Family series provides a 10/100Base-TX management interface on the Fabric. The management interface can connect a background PC for software loading and system debugging, or a remote network management station for remote system management.

Management Interface Configuration

The following sections describe management interface configuration tasks.

- Configuring interface IP address
- Enabling/disabling the interface
- Setting interface description
- Displaying current system information
- Test network connectivity (**ping**, **tracert**)

See the Port and System Management parts of this manual for details.



CAUTION: *Only the management interface configured with an IP address can run normally.*

6

CONFIGURATION FILE MANAGEMENT

Configuration File Management

Configuration File Management Overview

The management module of configuration file provides a user-friendly operation interface. It saves the configuration of the switch in the text format of command line to record the whole configuration process. Thus you can view the configuration information conveniently.

The format of configuration file includes:

- It is saved in the command format.
- Only the non-default constants will be saved
- The organization of commands is based on command views. The commands in the same command mode are sorted in one section. The sections are separated with a blank line or a comment line (A comment line begins with exclamation mark "#").
- Generally, the sections in the file are arranged in the following order: system configuration, Ethernet port configuration, VLAN interface configuration, routing protocol configuration and so on.
- It ends with "end".

The following sections describe configuration file management tasks.

- "Displaying the Current-Configuration and Saved-Configuration of Switch"
- "Modifying and Saving the Current-Configuration"
- "Erasing Configuration Files from Flash Memory"
- "Configuring the Name of the Configuration File Used for the Next Startup."

Displaying the Current-Configuration and Saved-Configuration of Switch

When the switch is being powered on, the system will read the configuration files from Flash Memory for the initialization of the switch. (Such configuration files are called saved-configuration files). If there is no configuration file in Flash Memory, the system will begin the initialization with the default parameters. Relative to the saved-configuration, the configuration in effect during the operating process of the system is called current-configuration. You can use the following commands to display the current-configuration and saved-configuration information of the switch.

Perform the following configuration in any view.

Table 29 Display the configurations of the switch

Operation	Command
Display the saved-configuration information of the switch	display saved-configuration
Display the current-configuration information of the Ethernet switch	display current-configuration [controller interface <i>interface-type interface-number</i> configuration [<i>configuration</i>]] [{ begin exclude include } <i>regular-expression</i>]
Display the running configuration of the current view	display this



The configuration files are displayed in their corresponding saving formats.

Modifying and Saving the Current-Configuration

You can modify the current configuration of the switch through the CLI. Use the **save** command to save the current-configuration in the Flash Memory, and the configurations will become the saved-configuration when the system is powered on for the next time.

Perform the following configuration in user view.

Table 30 Save the current-configuration

Operation	Command
Save the current-configuration	save [<i>file-name</i>]

Even if the problems like reboot and power-off occur during , the configuration file can be still saved to Flash.

Erasing Configuration Files from Flash Memory

The **reset saved-configuration** command can be used to erase configuration files from Flash Memory. The system will use the default configuration parameters for initialization when the switch is powered on for the next time.

Perform the following configuration in user view.

Table 31 Erase configuration files from Flash Memory

Operation	Command
Erase configuration files from Flash Memory	reset saved-configuration

You may erase the configuration files from the Flash in the following cases:

- After being upgraded, the software does not match with the configuration files.
- The configuration files in flash are damaged. (A common case is that a wrong configuration file has been downloaded.)

Configuring the Name of the Configuration File Used for the Next Startup.

Perform the following configuration in user view.

Table 32 Configure the name of the configuration file used for the next startup

Operation	Command
Configure the name of the configuration file used for the next startup	startup saved-configuration <i>cfgfile</i>

cfgfile is the name of the configuration file and its extension name can be ".cfg". The file is stored in the root directory of the storage devices.

After the above configuration, execute **display** command in any view to display the running of the configuration files, and to verify the effect of the configuration.

Table 33 Display the information of the file used at startup

Operation	Command
Display the information of the file used at startup	display startup

7

VLAN CONFIGURATION

VLAN Overview

Virtual local area network (VLAN) groups the devices in a LAN logically, not physically, into segments to form virtual workgroups. IEEE issued the IEEE 802.1Q in 1999 to standardize the VLAN implementations.

The VLAN technology allows network administrators to logically divide a physical LAN into different broadcast domains or the so-called virtual LANs. Every VLAN contains a group of workstations with the same demands. The workstations, physically separated, are not necessarily on the same physical LAN segment.

You can establish VLANs of the following types on switches:

- Port-based
- IP multicast-based (A multicast group can be a VLAN.)
- Network layer-based (A VLAN can be established by the network layer addresses or protocols of the hosts.)

With the VLAN technology, the broadcast and unicast traffic within a VLAN will not be forwarded to other VLANs. This is helpful to control network traffic, save device investment, simplify network management and enhance security.

Configuring VLAN

The following sections describe VLAN configuration tasks:

- “Creating/Deleting a VLAN”
- “Specifying a Description Character String for a VLAN or VLAN interface”
- “Naming the Current VLAN”
- “Shutting down/Bringing up a VLAN Interface”
- “Configuring Port-Based VLAN”

Creating/Deleting a VLAN

You can use the following commands to create/delete a VLAN. If the VLAN to be created exists, the system will enter the VLAN view directly. Otherwise, the system will create the VLAN first, and then enter the VLAN view.

Perform the following configuration in system view.

Table 34 Create/Delete a VLAN or VLANs

Operation	Command
Create a VLAN and enter the VLAN view	vlan <i>vlan-id</i>
Create VLANs in batch	vlan <i>vlan-id-list</i>
Delete an VLAN or VLANs	undo vlan { <i>vlan-id</i> [to <i>vlan-id</i>] all }

**CAUTION:**

- VLAN 1 is the system-default VLAN and cannot be removed.
- VLANs with their ports being VLAN VPN-enabled cannot be removed.
- Guest VLANs cannot be deleted.
- Protocol-enabled VLANs cannot be deleted.

Specifying a Description Character String for a VLAN or VLAN interface

You can use the following commands to specify a description character string for a VLAN or VLAN interface.

Perform the following configuration in VLAN view or VLAN interface view.

Table 35 Specify a description character string for a VLAN or VLAN interface

Operation	Command
Specify a description character string for a VLAN or VLAN interface	description <i>string</i>
Restore the default description of the current VLAN or VLAN interface	undo description

By default, the description character string of a VLAN is the VLAN ID of the VLAN, such as VLAN 0001. The description character string of a VLAN interface is the VLAN interface name, such as Vlan-interface1 Interface.

Naming the Current VLAN

You can use the following command to name the current VLAN.

Perform the following configuration in VLAN view.

Table 36 Name the current VLAN

Operation	Command
Name the current VLAN	name
Restore the default name of the current VLAN	undo name

By default, the name of the current VLAN is its VLAN ID.

Shutting down/Bringing up a VLAN Interface

You can use the following commands to shut down/bring up a VLAN interface.

Perform the following configuration in VLAN interface view.

Table 37 Shut down/bring up a VLAN interface

Operation	Command
Shut down a VLAN interface	shutdown
Bring up a VLAN interface	undo shutdown

Shutting down or bringing up a VLAN interface has no effect on the status of any Ethernet port in this VLAN.

By default, when all the Ethernet ports in a VLAN are in the Down state, this VLAN interface is also Down. When there are one or more Ethernet ports in the Up state, this VLAN interface is also Up.

Configuring Port-Based VLAN

You can use the following commands to specify Ethernet ports for a VLAN.

Perform the following configuration in VLAN view.

Table 38 Specify Ethernet ports for a VLAN

Operation	Command
Add Ethernet ports to a VLAN	port <i>interface-list</i>
Remove Ethernet ports from a VLAN	undo port <i>interface-list</i>

By default, the system adds all the ports to a default VLAN whose ID is 1.

Note that you can add/remove the trunk and Hybrid ports to/from a VLAN by the **port/undo port** commands in Ethernet port view, but not in VLAN view.

Configuring Protocol-Based VLAN

The following sections describe the protocol-based VLAN configuration tasks:

- “Creating/Deleting a VLAN Protocol Type”
- “Associating/Dissociating a Port with/from a Protocol-Based VLAN”

Creating/Deleting a VLAN Protocol Type

You can use the following commands to create/delete a VLAN protocol type.

Perform the following configuration in VLAN view.

Table 39 Create/Delete a VLAN protocol type

Operation	Command
Create a VLAN protocol type	protocol-vlan [<i>protocol-index</i>] { at ipx { ethernetii llc raw snap } } mode { ethernetii etype <i>etype-id</i> llc dsap <i>dsap-id</i> ssap <i>ssap-id</i> snap etype <i>etype-id</i> }
Delete an existing VLAN protocol type	undo protocol-vlan { <i>protocol-index</i> [to <i>protocol-end</i>] all }

Associating/Dissociating a Port with/from a Protocol-Based VLAN

Perform the following configuration in Ethernet port view.

Table 40 Associate/Dissociate a port with/from a protocol-based VLAN

Operation	Command
Associate a port with a protocol-based VLAN	port hybrid protocol-vlan vlan <i>vlan-id</i> { <i>vlan-protocol-list</i> all }
Remove a port from a protocol-based VLAN	undo port hybrid protocol-vlan vlan { <i>vlan-id</i> { <i>vlan-protocol-list</i> all } all }



- The port to be associated with a protocol-based VLAN must be of Hybrid type and in this VLAN.
- The same protocol can be configured in the different VLANs, but cannot be configured repeatedly in the same VLAN.
- A port cannot be associated with different VLANs with the same protocols configured.

- You cannot delete a protocol-based VLAN that has ports associated with.
- You cannot delete a protocol-based VLAN on a port while the port is associated with the VLAN.

Configuring IP Subnet-Based VLAN

The following sections describe the IP subnet-based VLAN configuration tasks:

- Associating/dissociating a specified port with/from an IP subnet-based VLAN
- Configuring an IP subnet-based VLAN

Associating/Dissociating a Specified Port with/from an IP Subnet-Based VLAN

Use the following commands to associate/dissociate a specified port with/from an IP subnet-based VLAN.

Perform the following configuration in Ethernet port view.

Table 41 Associate/dissociate a port with/from an IP subnet-based VLAN

Operation	Command
Associate a specified port with an IP subnet-based VLAN	port hybrid ip-vlan vlan <i>vlan-id</i>
Remove a specified port from an IP subnet-based VLAN	undo port hybrid ip-vlan vlan <i>vlan-id</i>

Configuring/deleting an IP Subnet-Based VLAN

Perform the following configuration in VLAN view.

Table 42 Configure/delete an IP subnet-based VLAN

Operation	Command
Create an IP subnet-based VLAN	vlan-type ip-subnet ip <i>ip-address</i> { [<i>net-mask</i> <i>net-mask-length</i>] }
Delete an IP subnet-based VLAN	undo vlan-type ip-subnet { <i>index-begin</i> [to <i>index-end</i>] all }

Configure the CPU Port in an VLAN

The CPU is a special port in the Switch 8800 Family series routing switches. By default, because the CPU port is in a VLAN, when common broadcast packets and unknown multicast packets are broadcast within a VLAN, these packets will also be broadcast to the CPU. To prevent waste of CPU resources, you can move the CPU port out of the VLAN, so that common broadcast packets and unknown multicast packets will not be handed to the CPU for processing.

You can use the following command to move the CPU port out of the VLAN.

Perform the following configuration in VLAN view.

Table 43 Move the CPU port out of/into the VLAN

Operation	Command
Move the CPU port out of the VLAN	trap-to-cpu disable
Move the CPU port into the VLAN	undo trap-to-cpu disable

By default, the CPU port is in the VLAN.

You can also move the CPU ports out of/into all the VLANs at a time.

Perform the following configuration in system view.

Table 44 Move the CPU port out of/into the specified VLANs

Operation	Command
Move the CPU port out of the specified VLANs	trap-to-cpu disable vlan { <i>vlan-list</i> all }
Move the CPU port into the specified VLANs	undo trap-to-cpu disable vlan { <i>vlan-list</i> all }

Displaying and Debugging a VLAN

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

Table 45 Display and Debug a VLAN

Operation	Command
Display the related information about the VLAN interface	display interface vlan-interface [<i>vlan-id</i>]
Display the related information about the VLAN	display vlan [<i>vlan-id to vlan-id</i> all static dynamic]
Display the protocol information and protocol index configured on the specified VLAN	display protocol-vlan vlan { <i>vlan-list</i> all }
Display the protocol information and protocol index configured on the specified port	display protocol-vlan interface { <i>interface-list</i> all }
Display information about CPU port in a VLAN	display trap-to-cpu

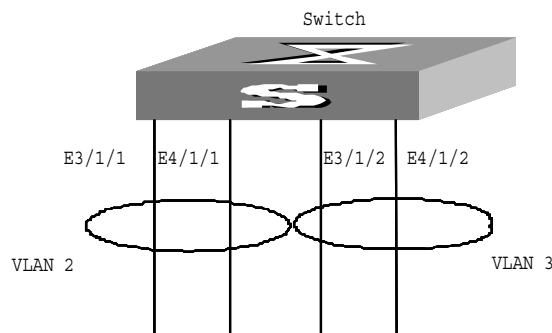
VLAN Configuration Example

Network requirements

- Create VLAN 2 and VLAN 3.
- Add Ethernet3/1/1 and Ethernet4/1/1 to VLAN 2.
- Add Ethernet3/1/2 and Ethernet4/1/2 to VLAN 3.

Network diagram

Figure 11 Network diagram for VLAN configuration



Configuration procedure

Create VLAN 2 and enter its view.

```
[SW8800] vlan 2
```

Add Ethernet3/1/1 and Ethernet4/1/1 to VLAN 2.

```
[3Com-vlan2] port ethernet3/1/1 ethernet4/1/1
```

Create VLAN 3 and enters its view.

```
[3Com-vlan2] vlan 3
```

Add Ethernet3/1/2 and Ethernet4/1/2 to VLAN 3.

```
[3Com-vlan3] port ethernet3/1/2 ethernet4/1/2
```

8

SUPER VLAN CONFIGURATION

Super VLAN Overview

Super VLAN is also called VLAN aggregation. The following is the fundamental principle: A super VLAN contains multiple sub VLANs. A super VLAN can be configured with an IP address of the virtual port, while a sub VLAN cannot be configured with the IP address of the virtual port. Each sub VLAN is a broadcast domain. Different sub VLANs are isolated at Layer 2. When users in a sub VLAN need to communicate with each other, they use the IP address of the virtual interface of the super VLAN as the IP address of the gateway. The IP address is shared by multiple VLANs. Therefore IP addresses are saved. If different sub VLANs want to communicate with one another at Layer 3, or a sub VLAN communicates with other networks, you can enable ARP proxy. The address resolution protocol (ARP) proxy can forward and process ARP request and response packets so that the isolated sub VLANs can communicate with each other at Layer 3. By default, ARP proxy is disabled in a sub VLAN.

Configuring a Super VLAN

Super VLAN configuration includes:

- Configure a VLAN to be a super VLAN
- Configure sub VLANs
- Establish mappings between the super VLAN and the sub VLANs
- Enable ARP proxy for the sub VLANs

Configuration Tasks



- You can configure multiple super VLANs for a switch. The configured VLAN port and IP address configurations are the same as common VLAN configurations.
- A sub VLAN configuration is the same as a common VLAN configuration. The following table describes the specific commands to configure a sub VLAN. For detailed information, refer to “VLAN Configuration”.

You can configure a super VLAN as follows:

Table 46 Configure a super VLAN

Operation	Command	Description
Enter system view	system-view	-
Enter VLAN view	vlan <i>vlan-id</i>	Required

Table 46 Configure a super VLAN

Operation	Command	Description
Set the VLAN type to super VLAN	supervlan	Required. The VLAN-ID is the configured VLAN ID in the range 1 to 4094.
Exit from Super VLAN view	quit	-
Create a sub VLAN and enter sub VLAN view	vlan <i>vlan-id</i>	Required
Add Ethernet ports to sub a VLAN	port <i>interface-list</i>	Optional
Exit from Sub VLAN view	quit	-
Enter Super VLAN view	vlan <i>vlan-id</i>	-
Configure the mapping relation between super VLAN and sub VLANs	subvlan <i>sub-vlan-list</i>	Required.
Enable ARP proxy for the sub VLAN	arp proxy enable	Optional. This command is necessary for multiple sub VLANs to communicate with one another.
Display configuration information	display super vlan [<i>supervlan-id</i>]	Optional. You can execute the display super vlan command in any view.

**CAUTION:**

- A Super VLAN cannot contain ports.
- After you set the VLAN type to super VLAN, the ARP proxy is automatically enabled on the VLAN port, and you do not need to configure the proxy.
- When a super VLAN exists, the ARP proxy should be enabled on the corresponding VLAN port.
- The default VLAN cannot be set to a super VLAN.
- You can add multiple ports (non-uplink port) to each sub VLAN.
- You cannot configure a virtual port for a sub VLAN.
- If the **undo subvlan** command does not include *vlan-id*, the mapping relationship between all sub VLANs and specified super VLANs is removed; if the **undo subvlan** command includes *vlan-id*, the mapping relationship between the specified sub VLANs and specified super VLANs is removed.
- In Super VLAN configuration, do not enable multicast VLAN and IGMP-snooping.
- Super VLAN does not support VRRP.

Super VLAN Configuration Example

Network requirements

Create Super VLAN 10.

Create sub VLANs VLAN 2, VLAN 3 and VLAN 5.

- VLAN 2 contains ports 1 and 2;
- VLAN 3 contains ports 3 and 4;
- VLAN 5 contains ports 5 and 6.

These sub VLANs are isolated at Layer 2. It is required that these sub VLANs communicate with one another at Layer 3.

Network diagram

Omitted

Configuration procedure

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan 10
[3Com-vlan10] supervlan
[3Com-vlan10] vlan 2
[3Com-vlan2] port ethernet3/1/1 ethernet3/1/2
[3Com-vlan2] arp proxy enable
[3Com-vlan2] vlan 3
[3Com-vlan3] port Ethernet3/1/3 ethernet3/1/4
[3Com-vlan3] arp proxy enable
[3Com-vlan3] vlan 5
[3Com-vlan5] port ethernet3/1/5 ethernet3/1/6
[3Com-vlan5] arp proxy enable
[3Com-vlan5] vlan 10
[3Com-vlan10] subvlan 2 3 5
[3Com-vlan10] interface vlan 10
[3Com-Vlan-interface10] ip address 10.110.1.1 255.255.255.0
```


9

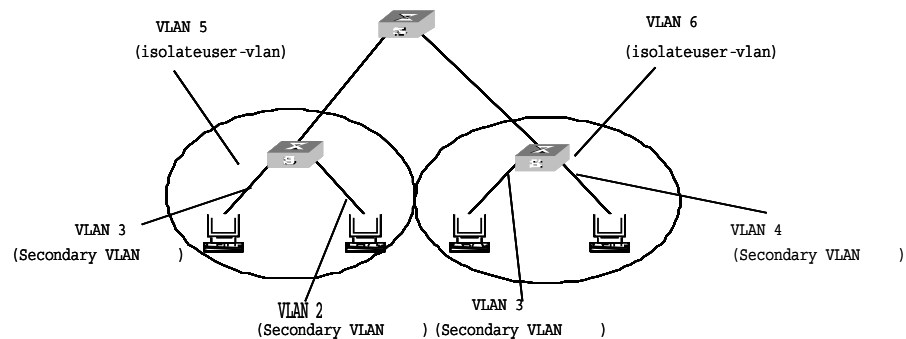
ISOLATE-USER-VLAN CONFIGURATION

Isolate-user-VLAN Overview

Isolate-user-VLAN can save the VLAN resource in a network. It adopts the two-level VLAN architecture. One level is isolate-user-VLAN level, and the other is Secondary VLAN level, as shown in Figure 12.

- An isolate-user-VLAN corresponds to multiple Secondary VLANs. It contains all the ports and upstream ports of the corresponding Secondary VLANs. In this way, a switch that is of upper level only needs recognizing the isolate-user-VLANs of the downstream switch instead of the Secondary VLANs, thereby streamlining the configuration and saving the VLAN source.
- You can use isolate-user-VLAN to implement the isolation of the Layer-2 packets by assigning a Secondary VLAN for each user, with each of the Secondary VLANs containing the ports and the upstream ports connected to the user. You can configure the ports connected to different users to be of the same Secondary VLAN to enable these users to communicate with each other on Layer 2.

Figure 12 Isolate-user-VLANs and Secondary VLANs



Isolate-use-vlan Configuration Task

Configuration Tasks

Table 47 Isolate-user-VLAN configuration tasks

Configuration tasks	Description	Detailed configuration
Configure an isolate-user-VLAN	Required	Refer to section "Product Overview"
Configure Secondary VLAN	Required	Refer to section "Configuring a Secondary VLAN"
Configure the mapping relationship between isolate-user-VLANs and Secondary VLANs	Required	Refer to section "Mapping an isolate-user-vlan to Secondary VLANs"

Configuring an isolate-user-VLAN

Table 48 Configure an isolate-user-VLAN

Operation	Command	Description
Enter system view	system-view	-
Create a VLAN	vlan <i>vlan-id</i>	Required
Configure the VLAN as an isolate-user-VLAN	isolate-user-vlan enable	Required You cannot configure VLAN 1 as an isolate-user-VLAN Optional
Add ports to the isolate-user-VLAN	port <i>interface-list</i>	Optional An isolate-user-VLAN can contain multiple ports, including upstream ports connecting to other switches. However the contained ports can only be access or hybrid ports, not trunk ports.

Configuring a Secondary VLAN

Table 49 Configure a Secondary VLAN

Operation	Command	Description
Enter system view	system-view	-
Create a VLAN as a Secondary VLAN	vlan <i>vlan-id</i>	Required You cannot configure VLAN 1 as a Secondary VLAN. Optional
Add ports to the Secondary VLAN	port <i>interface-list</i>	You can add multiple ports (not uplink ports) to a Secondary VLAN.



- An isolate-user-VLAN can correspond to up to 64 Secondary VLANs.
- You can configure up to 32 isolate-user-VLANs for a system.
- You can configure up to 1,024 Secondary VLANs for a system.
- You cannot configure the same MAC address in a Secondary VLAN corresponding to an isolate-user-VLAN.
- If a VLAN is an isolate-user-VLAN or a Secondary VLAN, you cannot configure vlan-interface; a VLAN configured with vlan-interface cannot be configured as an isolate-user-VLAN or a Secondary VLAN.

Mapping an isolate-user-vlan to Secondary VLANs


Table 50 Map an isolate-user-VLAN to secondary VLANs

Operation	Command	Description
Enter system view	system-view	-
Map an isolate-user-VLAN to secondary VLANs	isolate-user-vlan <i>isolate-user-vlan-num</i> secondary <i>secondary-vlan-numlist</i>	Required

Note the following when mapping an isolate-user-vlan to Secondary VLANs

- 1 If the isolate-user-VLAN contains ports
 - For hybrid ports, if the default port VLAN ID is the same as the isolate-user-VLAN ID, and the port joins the isolate-user-VLAN in the Untagged mode, all the hybrid ports meeting the requirements will join the Secondary VLAN in the Untagged mode simultaneously. For those not meeting the requirements, no other processing will be made.
 - For an access port, the system will set the port as a hybrid port and set the default port VLAN ID and isolate-user-VLAN ID to be the same. Moreover, the port joins the isolate-user-VLAN and Secondary VLAN in the Untagged mode.
- 2 If the Secondary VLAN contains ports
 - For a hybrid port, if the default port VLAN ID is the same as the Secondary VLAN ID, and the port joins the Secondary VLAN in the Untagged mode, all the hybrid ports meeting the requirements will join the isolate-user-VLAN in the Untagged mode simultaneously. For those not meeting the requirements, no other processing will be made.
 - For an access port, the system will set the port as a hybrid port and set the default port VLAN ID and Secondary VLAN ID to be the same. Moreover, the port joins the isolate-user-VLAN and Secondary VLAN in the Untagged mode.

Note the following after mapping an isolate-user-VLAN to a Secondary VLAN

- Trunk ports and access ports cannot join an isolate-user-VLAN or Secondary VLAN.
 - Hybrid ports can join or exit from an isolate-user-VLAN and Secondary VLAN.
-  You cannot directly set an isolate-user-VLAN or Secondary VLAN as other type of VLAN than common VLAN, such as multicast VLAN, Super/Sub VLAN, Guest VLAN or VLAN running L2VPN services.
- When you set a common VLAN as an isolate-user-VLAN or Secondary VLAN, the VLAN cannot contain trunk ports.

Displaying and Debugging an isolate-user-VLAN

After the above configuration, execute **display** command in any view to display the running of the isolate-user-VLAN configuration, and to verify the effect of the configuration.

Table 51 Display and debug isolate-user-VLAN

Operation	Command
Display the mapping relationship between the isolate-user-vlan and Secondary VLAN	display isolate-user-vlan [<i>isolate-user-vlan-num</i>]

Isolate-user-VLAN Configuration Example

Network requirements

Switch A is connected to Switch B and Switch C in the downstream.

1 On Switch B

VLAN 5 is an isolate-user-VLAN, including an upstream port (Ethernet2/1/1 port) and two Secondary VLANs, VLAN2 and VLAN3. VLAN 2 includes Ethernet2/1/2 port and VLAN 3 includes Ethernet2/1/3 port.

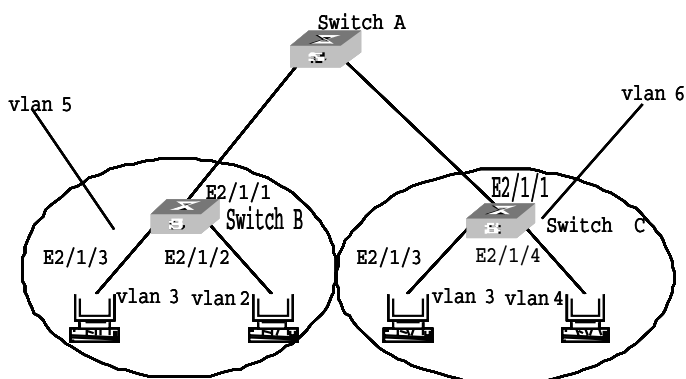
2 On Switch C

VLAN 6 is an isolate-user-VLAN including an upstream port (Ethernet2/1/1 port) and two Secondary VLANs: VLAN3 and VLAN4. VLAN3 includes Ethernet2/1/3 port and VLAN4 includes Ethernet2/1/4 port.

Seen from the Switch A, either Switch B or Switch C carries one VLAN, VLAN 5 and VLAN 6 respectively.

Network diagram

Figure 13 Network diagram for isolate-user-VLAN



Configuration procedure

Only the configurations on the Switch B and Switch C are listed below.

1 Configuration on Switch B

Configure an isolate-user-VLAN.

```
<SW8800>system-view
[SW8800] vlan 5
[3Com-vlan5] isolate-user-vlan enable
[3Com-vlan5] port ethernet2/1/1
```

Configure Secondary VLANs.

```
[3Com-vlan5] vlan 3
[3Com-vlan3] port ethernet2/1/3
[3Com-vlan3] vlan 2
[3Com-vlan2] port ethernet2/1/2
```

Configure the mapping relationship between the isolate-user-VLAN and the Secondary VLANs.

```
[3Com-vlan2] quit  
[SW8800] isolate-user-vlan 5 secondary 2 to 3
```

2 Configuration on Switch C

Configure an isolate-user-VLAN.

```
<SW8800>system-view  
[SW8800] vlan 6  
[3Com-vlan6] isolate-user-vlan enable  
[3Com-vlan6] port ethernet2/1/1
```

Configure Secondary VLANs.

```
[3Com-vlan6] vlan 3  
[3Com-vlan3] port ethernet2/1/3  
[3Com-vlan3] vlan 4  
[3Com-vlan4] port ethernet2/1/4
```

Configure the mapping relationship between the isolate-user-VLAN and the Secondary VLANs.

```
[3Com-vlan4] quit  
[SW8800] isolate-user-vlan 6 secondary 3 to 4
```


10

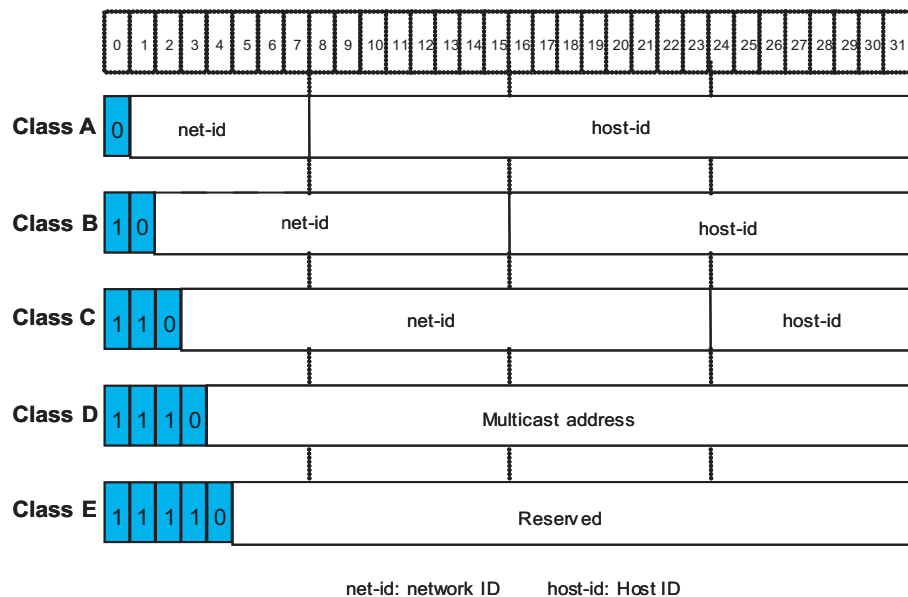
IP ADDRESS CONFIGURATION

Introduction to IP Addresses

IP Address Classification and Representation

An IP address is a 32-bit address allocated to a device that accesses the Internet. It consists of two fields: net-id field and host-id field. IP addresses are allocated by Network Information Center (NIC) of American Defense Data Network (DDN). To manage IP addresses conveniently, IP addresses are classified into five types. See the following figure.

Figure 14 Five classes of IP addresses



Here, Class A, Class B and Class C addresses are unicast addresses, while Class D addresses are multicast ones and class E addresses are reserved for special applications in future. The first three types are commonly used.

The IP address is in dotted decimal format. Each IP address contains four integers in dotted decimal notation. Each integer corresponds to one byte, for example, 10.110.50.101.

When using IP addresses, note that some of them are reserved for special uses, and are seldom used. The IP addresses you can use are listed in the following table.

Table 52 IP address classes and ranges

Network class	Address range	IP network range available	Note
A	0.0.0.0 to 127.255.255.255	1.0.0.0 to 126.0.0.0	<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, that is, broadcast to all hosts on the network.</p> <p>IP address 0.0.0.0 is used for the host that is not put into use after starting up.</p> <p>The IP address with network ID being 0 indicates the current network and its network can be cited by the router without knowing its network number.</p> <p>The IP addresses with the format of 127.X.Y.Z are reserved for self-loop test and the packets sent to these addresses are not output to the line. The packets are processed internally and regarded as input packets.</p>
B	128.0.0.0 to 191.255.255.255	128.0.0.0 to 191.254.0.0	<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, that is, broadcast to all hosts on the network.</p>
C	192.0.0.0 to 223.255.255.255	192.0.0.0 to 223.255.254.0	<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, that is, broadcast to all hosts on the network.</p>
D	224.0.0.0 to 239.255.255.255	None	<p>Addresses of class D are multicast addresses, among which:</p> <ul style="list-style-type: none"> ■ IP address 224.0.0.0 is reserved and will not be allocated. Those from 224.0.0.1 to 224.0.0.255 are reserved for routing protocols and other protocols that are used to discover and maintain routes. ■ Those from 239.0.0.0 to 239.255.255.255 are used for local multicast management. ■ Those from 224.0.0.255 to 238.255.255.255 are for users.
E	240.0.0.0 to 255.255.255.254	None	The addresses are reserved for future use.
Other addresses	255.255.255.255	255.255.255.255	255.255.255.255 is used as a Local Area Network (LAN) broadcast address.

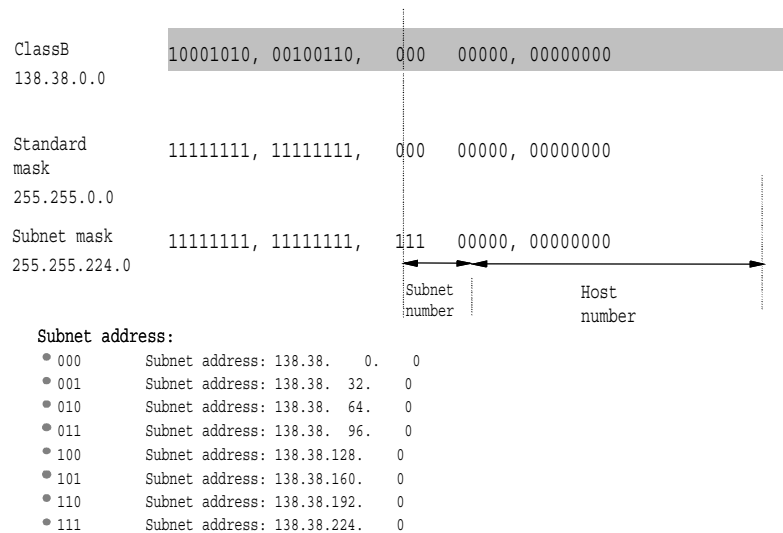
Subnet and Mask

Nowadays, with rapid development of the Internet, IP (V4) addresses are depleting very in a few years. The traditional IP address allocation method wastes IP addresses greatly. In order to make full use of the available IP addresses, the concept of mask and subnet is proposed.

A mask is a 32-bit number corresponding to an IP address. The number consists of 1s and 0s. Principally, these 1s and 0s can be combined randomly. However, the first consecutive bits are set to 1s when you design a mask. The mask divides the IP address into two parts: subnet address and host address. The part of IP address that corresponds to the bits 1s in the mask indicates the subnet address and the other part of IP address indicate the host address. If there is no subnet division, then its subnet 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 subnet mask are 255.0.0.0, 255.255.0.0 and 255.255.255.0 respectively.

The mask can be used to divide a Class A network containing more than 16,000,000 hosts or a Class B network containing more than 60,000 hosts into multiple small networks. Each small network is called a subnet. For example, for the Class B network address 138.38.0.0, the mask 255.255.224.0 can be used to divide the network into eight subnets: 138.38.0.0, 138.38.32.0, 138.38.64.0, 138.38.96.0, 138.38.128.0, 138.38.160.0, 138.38.192.0 and 138.38.224.0 (Refer to the following figure). Each subnet can contain more than 8000 hosts.

Figure 15 Subnet division of an IP address



Configuring IP Address

The following sections describe IP address configuration tasks:

- "Configuring the Hostname and Host IP Address"
- "Configuring the IP Address of the VLAN Interface"
- "IP Address Protection Configuration"
- "Configuring Whether the Switch Sends Unreachable Packets"

Configuring the Hostname and Host IP Address

Using this command, you can associate a host name with an IP address. After that, when using an application like telnet, you can use the host name instead of the IP address that is hard to memorize, and the system automatically translates the host name to the IP address.

Perform the following configuration in system view.

Table 53 Configure the host name and the corresponding IP address

Operation	Command
Configure the host name and the corresponding IP address	ip host <i>hostname ip-address</i>
Cancel the host name and the corresponding IP address	undo ip host <i>hostname [ip-address]</i>

By default, there is no host name associated to any host IP address.

Configuring the IP Address of the VLAN Interface

You can configure an IP address for every VLAN interface of the switch. Generally, it is enough to configure one IP address for an interface. You can also configure 21 IP addresses for an interface at most, so that it can be connected to several subnets. Among these IP addresses, one is the primary IP address and all others are secondary.

Perform the following configuration in VLAN interface view.

Table 54 Configure an IP address for a VLAN interface

Operation	Command
Configure an IP address for a VLAN interface	ip address <i>ip-address { mask mask-length } [sub]</i>
Delete an IP address of a VLAN interface	undo ip address <i>ip-address { mask mask-length } [sub]</i>



*When you use the **ip address** command to configure IP addresses of VLAN interfaces, the system will prompt if you continue if the IP address you configure is in different network segment from the existing IP address. If you do continue, the IP address of the VLAN interface will be modified. In addition, if the ARP entries (including dynamic ARP entries and static ARP entries) in the original network segment match the new network segment, they will not be removed; otherwise, the ARP entries in the original network segment will be removed.*

By default, the IP address of a VLAN interface is null.

IP Address Protection Configuration

How IP address protection works

The IP address protection functions can be used for bindings between IP addresses and MAC addresses to ensure that only users using the IP addresses corresponding to the specified MAC addresses can access the Internet while users using other IP addresses cannot. This function works once configured on the switch, without configurations on the server or client.

The IP address protection function needs to work together with the MAC address auto filling function to complete bindings between IP addresses and MAC addresses. When the MAC address auto filling function is enabled, you can configure a static ARP entry that has only an IP address and the MAC address auto filling function can automatically fill the ARP entry with the learned MAC address.

After the IP address protection function is enabled on a VLAN interface, the current interface will no longer dynamically learn ARP mapping entries, and existing dynamic ARP mapping entries will be removed. At the same time, the switch will enable the MAC address auto filling function, so that the user can

configure static ARP entries that have only IP addresses. The switch will automatically fill the MAC address in the ARP mapping entries so that only users configured with static ARP entries can have access to the network.

IP address protection configuration

The tasks of IP address protection configuration include:

- Configuring auto-fill ARP address
- Enabling IP address protection

Table 55 Configure IP address protection

Operation	Command	Description
Enter system view	system-view	-
Configure auto-fill ARP address	arp static <i>ip-address</i>	Optional
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	-
Enable IP address protection	ip-protect enable	By default, the IP address protection function is disabled on VLAN interface
View the IP address protection status of the current VLAN interface	display this	You can carry out the display this command in any view



CAUTION:

- The MAC address auto filling function is enabled only when the IP address protection function is enabled on the interface.
- Once after the initial auto filling of ARP address, the user-configured static ARP entry becomes a normal static ARP entry and cannot be filled again.

Configuring Whether the Switch Sends Unreachable Packets

When receiving an IP packet whose TTL is 1, the switch sends an unreachable packet to the sending end. However, if an attacker continuously sends IP packets whose TTLs are less than or equal to 1 to the switch, the switch keeps sending unreachable packets to the attacker. In this case, the switch CPU is under attack.

When receiving an IP packet whose TTL is less than or equal to 1, the switch sends the ICMP packet "time exceeded" to the network management system instead of sending an unreachable packet to the sending end, thus avoiding attack on the CPU.

Table 56 Configure whether the switch sends unreachable packets

Operation	Command	Description
Enter system view	system-view	-
Configure that the switch sends the ICMP message "time exceeded" to the network management system when the switch receives an IP packet whose TTL is less than or equal to 1	ip icmp-time-exceed enable	By default, the switch sends the ICMP message "time exceeded" to the network management system

Table 56 Configure whether the switch sends unreachable packets

Operation	Command	Description
Configure that the switch sends an unreachable packet to the sending end when the switch receives an IP packet whose TTL is less than or equal to 1	undo ip icmp-time-exceed enable	-

Displaying IP Address

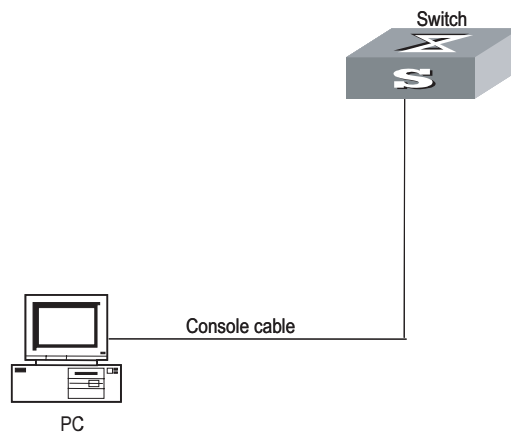
After the above configuration, execute the **display** command in any view to display the IP addresses configured on interfaces of the network device, and to verify the effect of the configuration.

Table 57 Display and debug IP address

Operation	Command
Display all hosts on the network and the corresponding IP addresses	display ip host
Display the configurations of a VLAN interface	display ip interface vlan-interface <i>vlan-id</i>

IP Address Configuration Example**Network requirements**

Configure the IP address as 129.2.2.1 and subnet mask as 255.255.255.0 for the VLAN interface 1 of the switch.

Network diagram**Figure 16** Network diagram for IP address configuration**Configuration procedure**

Enter VLAN interface 1.

```
[SW8800] interface vlan-interface 1
```

Configure the IP address for VLAN interface 1.

```
[3Com-Vlan-interface1] ip address 129.2.2.1 255.255.255.0
```

**Troubleshooting IP
Address Configuration**

Fault 1: The switch cannot ping through a certain host in the LAN.

Troubleshooting can be performed as follows:

- 1** Check the configuration of the switch. Use the **display arp** command to view the ARP entry table that the switch maintains.
- 2** Check which VLAN includes the port of the switch used to connect to the host. Check whether the VLAN has been configured with a VLAN interface. Then check whether the IP address of the VLAN interface and that of the host are on the same network segment.
- 3** If the configuration is correct, enable the ARP debugging on the switch, and check whether the switch can correctly send and receive ARP packets. If it can only send ARP packets but cannot receive them, errors may occur on the Ethernet physical layer.

11

IP PERFORMANCE CONFIGURATION

Configuring IP Performance

IP performance configuration includes:

- “Configuring TCP Attributes”

Configuring TCP Attributes

TCP attributes that can be configured include:

- synwait timer: When sending the syn packets, TCP starts the synwait timer. If response packets are not received before synwait timeout, the TCP connection is terminated. The timeout of synwait timer ranges from 2 to 600 seconds and it is 75 seconds by default.
- finwait timer: When the TCP connection state turns from FIN_WAIT_1 to FIN_WAIT_2, finwait timer is started. If FIN packets are not received before finwait timer timeout, the TCP connection is terminated. The timeout of finwait timer ranges from 76 to 3600 seconds and it is 675 seconds by default.
- The receiving/sending buffer size of the connection-oriented socket is in the range from 1 to 32 KB and is 8 KB by default.

Perform the following configuration in System view.

Table 58 Configure TCP attributes

Operation	Command
Configure timeout time for the synwait timer in TCP	tcp timer syn-timeout <i>time-value</i>
Restore the default timeout time of the synwait timer	undo tcp timer syn-timeout
Configure timeout time for the FIN_WAIT_2 timer in TCP	tcp timer fin-timeout <i>time-value</i>
Restore the default timeout time of the FIN_WAIT_2 timer	undo tcp timer fin-timeout
Configure the socket receiving/sending buffer size of TCP	tcp window <i>window-size</i>
Restore the socket receiving/sending buffer size of TCP to default value	undo tcp window

Displaying and Debugging IP Performance

After the above configuration, execute the **display** command in any view to display the running of the IP performance configuration, and to verify the effect of the configuration.

Table 59 Display IP performance

Operation	Command
Display TCP connection state	display tcp status

Table 59 Display IP performance

Operation	Command
Display TCP connection statistics data	display tcp statistics
Display UDP statistics information	display udp statistics
Display IP statistics information	display ip statistics
Display ICMP statistics information	display icmp statistics
Display the current socket information of the system	display ip socket [socktype <i>sock-type</i>] [<i>task-id</i> <i>socket-id</i>]
Display the summary of the Forwarding Information Base (FIB)	display fib
Display the FIB entries matching the destination IP address (range)	display fib [<i>ip-address1</i> { <i>mask1</i> <i>mask-length1</i> } [<i>ip-address2</i> { <i>mask2</i> <i>mask-length2</i> } longer] longer]
Display the FIB entries matching a specific ACL	display fib acl { <i>number</i> <i>name</i> }
Display the FIB entries which are output from the buffer according to regular expression and related to the specific character string	display fib { begin include exclude } <i>text</i> }
Display the FIB entries matching the specific prefix list	display fib ip-prefix <i>listname</i>
Display the total number of FIB entries	display fib statistics

Execute the **reset** command in user view to clear IP, TCP and UDP statistics information. Execute the **debugging** command to debug IP performance.

Table 60 Debug IP performance

Operation	Command
Reset IP statistics information	reset ip statistics
Reset TCP statistics information	reset tcp statistics
Reset UDP statistics information	reset udp statistics
Enable the debugging of IP packets	debugging ip packet [acl <i>acl-number</i>]
Disable the debugging of IP packets	undo debugging ip packet
Enable the debugging of ICMP packets	debugging ip icmp
Disable the debugging of ICMP packets	undo debugging ip icmp
Enable the debugging of UDP connections	debugging udp packet [<i>task-id</i> <i>socket-id</i>]
Disable the debugging of UDP connections	undo debugging udp packet [<i>task-id</i> <i>socket-id</i>]
Enable the debugging of TCP connections	debugging tcp packet [<i>task-id</i> <i>socket-id</i>]
Disable the debugging of TCP connections	undo debugging tcp packet [<i>task-id</i> <i>socket-id</i>]
Enable the debugging of TCP events	debugging tcp event [<i>task-id</i> <i>socket-id</i>]
Disable the debugging of TCP events	undo debugging tcp event [<i>task-id</i> <i>socket-id</i>]
Enable the debugging of the MD5 authentication	debugging tcp md5
Disable the debugging of the MD5 authentication	undo debugging md5

Troubleshooting IP Performance

Fault: IP layer protocol works normally but TCP and UDP cannot work normally.

Troubleshoot: In the event of such a fault, you can enable the corresponding debugging information output to view the debugging information.

- Use the **display** command to view the running information of IP performance and make sure that the PCs used by the user is running normally.
- Use the **terminal debugging** command to output the debugging information to the console.
- Use the **debugging udp packet** command to enable the UDP debugging to trace the UDP packet.

The following are the UDP packet formats:

```
UDP output packet:
Source IP address:202.38.160.1
Source port:1024
Destination IP Address 202.38.160.1
Destination port: 4296
task = ROUT(15)
socketid = 6,
src = 192.168.1.1:520,
dst = 255.255.255.255:520,
datalen = 24
```

- Use the **debugging tcp packet** command to enable the TCP debugging to trace the TCP packets.

Operations include:

```
<SW8800> terminal debugging
<SW8800> debugging tcp packet
```

Then the TCP packets received or sent can be checked in real time. Specific packet formats include:

```
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
task = ROUT(15)
socketid = 5
state = Established
src = 172.16.1.2
Source port:1025
dst = 172.16.1.1
Destination port: 4296
seq = 1921836502
ack = 4192768493
```

```
flag = ACK  
window = 16079
```

12

GARP&GVRP CONFIGURATION

Configuring GARP

GARP Overview Generic attribute registration protocol (GARP) offers a mechanism that is used by the members in the same switching network to distribute, propagate and register such information as VLAN and multicast addresses.

GARP does not exist in a switch as an entity. A GARP participant is called GARP application. The main GARP applications at present are GVRP (GARP VLAN registration protocol) and GMRP. For details, refer to section "Configuring GVRP" "Configuring GVRP" and section "Configuring Multicast". When a GARP participant is on a port of the switch, this port corresponds to a GARP participant.

The GARP mechanism enables the configuration information on one GARP member to be propagated rapidly across the whole switching network. A GARP member can be a terminal workstation or a bridge. The GARP member can notify other members to register or remove its attribute information by sending declarations or withdrawing declarations. It can also register or remove the attribute information of other GARP members according to the received declarations/withdrawn declarations.

GARP members exchange information by sending messages. There are mainly three types of GARP messages, Join, Leave, and LeaveAll. When a GARP participant wants to register its attribute information with other switches, it sends the Join message outward. When it wants to remove some attribute information from other switches, it sends the Leave message. The LeaveAll timer is started simultaneously when each GARP participant is enabled and the LeaveAll message is sent upon expiration. The Join and Leave messages cooperate to ensure the logout and the re-registration of a message. The message exchange enables all the to-be-registered attribute information to be propagated to all the switches across the same switching network.

The destination MAC addresses of the packets of the GARP participants are specific multicast MAC addresses. A GARP-supporting switch classifies the packets received from the GARP participants and processes them with corresponding GARP applications (GVRP or GMRP).

GARP and GMRP are described in details in the IEEE 802.1P standard (which has been added to the IEEE802.1D standard). 3Com series switches fully support the GARP compliant with the IEEE standards.

The following section describes the GARP configuration task:

- "Setting the GARP Timer"



- The value of GARP timer will be used in all the GARP applications, including GVRP and GMRP, running in one switched network.
- In one switched network, the GARP timers on all the switching devices should be set to the same value. Otherwise, GARP application cannot work normally.

Setting the GARP Timer

GARP timers include Hold timer, Join timer, Leave timer and LeaveAll timer.

The GARP participant sends the Join Message regularly when Join timer times out so that other GARP participants can register its attribute values.

When the GARP participant wants to remove some attribute values, it sends the Leave Message. The GARP participant that receives the message starts the Leave timer. If the Join Message is not received again before the Leave timer expires, the GARP attribute values are removed.

LeaveAll timer is started as soon as the GARP participant is enabled. The LeaveAll message is sent upon timeout so that other GARP participants remove all the attribute values of this participant. Then, LeaveAll timer is restarted and a new cycle begins.

When the switch receives some GARP registration information, it does not send the Join Message immediately. Instead, it enables a Hold timer and sends the Join Message upon timeout of the Hold timer. In this way, all the VLAN registration information received within the time specified by the Hold timer can be sent in one frame so as to save the bandwidth resources.

Configure Hold timer, Join timer and Leave timer in Ethernet port view. Configure LeaveAll timer in system view.

Table 61 Set the GARP timer

Operation	Command
Set GARP Hold timer, Join timer and Leave timer	garp timer { hold join leave } timer_value
Set GARP LeaveAll timer	garp timer leaveall timer_value
Restore the default settings of GARP Hold timer, Join timer and Leave timer	undo garp timer { hold join leave }
Restore the default settings of GARP LeaveAll timer	undo garp timer leaveall

By default, Hold timer is 10 centiseconds, Join timer is 20 centiseconds, Leave timer is 60 centiseconds, and LeaveAll timer is 1000 centiseconds.

Note that, the value of Join timer should be no less than the doubled value of Hold timer, and the value of Leave timer should be greater than the doubled value of Join timer and smaller than the Leaveall timer value. Besides, you must set the value of the Join timer in terms of 5 centiseconds. Otherwise, the system will prompt message of error.

The value range of a timer varies with the values of other timers. So if the value of a timer you want to set is not within the available value range, you can change the value range by changing the values of other related timers.

- The lower limit of Hold timer is 10 centiseconds. You can change its upper limit by changing the value of Join timer.
- You can change the lower limit and upper limit of Join timer by changing the value of Hold timer and Leave timer respectively.
- You can change the lower limit and upper limit of Leave timer by changing the value of Join timer and LeaveAll timer respectively.
- The upper limit of LeaveAll timer is 32765 centiseconds. You can change its lower limit by changing the value of Leave timer.

Displaying and Debugging GARP

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

Execute the **reset** command in user view to reset the configuration of GARP. Execute the **debugging** command in user view to debug the configuration of GARP.

Table 62 Display and debug GARP

Operation	Command
Display GARP statistics information	display garp statistics [interface <i>interface-list</i>]
Display GARP timer	display garp timer [interface <i>interface-list</i>]
Clear GARP statistics information	reset garp statistics [interface <i>interface-list</i>]
Enable GARP event debugging	debugging garp event
Disable GARP event debugging	undo debugging garp event

Configuring GVRP

GVRP Overview

GARP VLAN Registration Protocol (GVRP) is a GARP application. Based on GARP operating mechanism, GVRP provides maintenance of the dynamic VLAN registration information in the switch and propagates the information to other switches. All the GVRP-supporting switches can receive VLAN registration information from other switches and dynamically update the local VLAN registration information including the active members and through which port those members can be reached. All the GVRP-supporting switches can propagate their local VLAN registration information to other switches so that the VLAN information can be consistent on all GVRP-supporting devices in one switching network. The VLAN registration information propagated by GVRP includes both the local static registration information configured manually and the dynamic registration information from other switches.

GVRP is described in details in the IEEE 802.1Q standard. 3Com series switches fully support the GARP compliant with the IEEE standards.

Main GVRP configuration includes:

- “Enabling/Disabling Global GVRP”
- “Enabling/Disabling Port GVRP”
- “Setting the GVRP Registration Type”

In the above-mentioned configuration tasks, GVRP should be enabled globally before it is enabled on the port. Configuration of GVRP registration type can only take effect after the port GVRP is enabled. Besides, GVRP must be configured on the Trunk port.



- When you configure an aggregation group, the GVRP feature configured on the master port is unchanged, but that on the slave port is disabled.
- When you add a port to an existing aggregation group, the GVRP feature on the port is disabled.
- When the master port leaves an aggregation group, the GVRP feature on both the group and port is unchanged; when a slave port leaves an aggregation group, the GVRP feature on the port is disabled.
- When you configure GVRP feature on any port in an aggregation group, the configuration is mapped to the master port of the group.
- When you query the GVRP feature configured on any port in an aggregation group, the returned result is about the master port of the group.

Enabling/Disabling Global GVRP

You can use the following command to enable/disable global GVRP.

Perform the following configurations in system view.

Table 63 Enable/disable global GVRP

Operation	Command
Enable global GVRP	gvrp
Disable global GVRP	undo gvrp

By default, global GVRP is disabled.

Enabling/Disabling Port GVRP

You can use the following command to enable/disable the GVRP on a port.

Perform the following configurations in Ethernet port view.

Table 64 Enable/disable port GVRP

Operation	Command
Enable port GVRP	gvrp
Disable port GVRP	undo gvrp

GVRP should be enabled globally before it is enabled on the port. The GVRP can only be enabled/disabled on Trunk ports.

By default, port GVRP is disabled.

Setting the GVRP Registration Type

The GVRP registration types include **normal**, **fixed** and **forbidden** (refer to IEEE 802.1Q).

- When an Ethernet port is set to be in **normal** registration mode, the dynamic and manual creation, registration and deregistration of VLAN are allowed on this port.

- When a Trunk port is set as **fixed**, the port is not allowed to dynamically register/deregister a VLAN, it only propagates information about static VLANs that are manually configured instead of that of dynamic VLANs. That is, a Trunk port that is of fixed type only permits manually configured VLANs even you configure it to permit all VLANs.
- When an Ethernet port is set to be in **forbidden** registration mode, all the VLANs except VLAN1 will be deregistered and no other VLANs can be created and registered on this port.

Perform the following configuration in Ethernet port view.

Table 65 Set the GVRP registration type

Operation	Command
Set GVRP registration type	gvrp registration { normal fixed forbidden }
Restore the default GVRP registration type	undo gvrp registration

By default, GVRP registration type is **normal**.

Displaying and Debugging GVRP

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

Execute the **debugging** command in user view to debug the configuration of GVRP.

Table 66 Display and debug GVRP

Operation	Command
Display GVRP statistics information	display gvrp statistics [interface interface-list]
Display GVRP global status information	display gvrp status
Enable GVRP packet or event debugging	debugging gvrp { packet event }
Disable GVRP packet or event debugging	undo debugging gvrp { packet event }

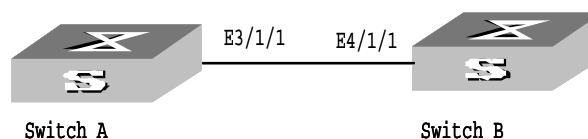
GVRP Configuration Example

Network requirements

To dynamically register and update VLAN information among switches, GVRP needs to be enabled on the switches.

Network diagram

Figure 17 GVRP configuration example



Configuration procedure

Configure Switch A:

```
# Enable GVRP globally.
```

```
[SW8800] gvrp
```

```
# Set Ethernet3/1/1 as a Trunk port and allows all the VLANs to pass through.
```

```
[SW8800] interface ethernet3/1/1  
[3Com-Ethernet3/1/1] port link-type trunk  
[3Com-Ethernet3/1/1] port trunk permit vlan all
```

```
# Enable GVRP on the Trunk port.
```

```
[3Com-Ethernet3/1/1] gvrp
```

```
Configure Switch B:
```

```
# Enable GVRP globally.
```

```
[SW8800] gvrp
```

```
# Set Ethernet4/1/1 as a Trunk port and allows all the VLANs to pass through.
```

```
[SW8800] interface ethernet4/1/1  
[3Com-Ethernet4/1/1] port link-type trunk  
[3Com-Ethernet4/1/1] port trunk permit vlan all
```

```
# Enable GVRP on the Trunk port.
```

```
[3Com-Ethernet4/1/1] gvrp
```


13

ETHERNET PORT CONFIGURATION

Ethernet Port Overview

Switch 8800 Family series can provide conventional Ethernet ports, fast Ethernet ports, 1000 Mbps Ethernet ports and 10 Gbps Ethernet ports. The configurations of these Ethernet ports are basically the same, which will be described in the following sections.

Ethernet Port Configuration

The following sections describe Ethernet port configuration tasks:

- “Entering Ethernet Port View”
- “Enabling/Disabling an Ethernet Port”
- “Setting Ethernet Port Description”
- “Setting the Duplex Attribute of the Ethernet Port”
- “Setting Speed on the Ethernet Port”
- “Setting the Cable Type for the Ethernet Port”
- “Enabling/Disabling Flow Control for the Ethernet Port”
- “Setting the Interval of Performing Statistics on Ports”
- “Enabling/Disabling Jumbo Frames’ Passing a Card”
- “Setting Broadcast/Multicast Suppression on Ethernet Port”
- “Setting the Ethernet Port Mode”
- “Setting the Link Type for the Ethernet Port”
- “Adding the Ethernet Port to Specified VLANs”
- “Setting the Default VLAN ID for the Ethernet Port”
- “Setting the VLAN VPN Feature on a Port”
- “Copying Port Configurations to Other Ports”
- “Setting Port Hold Time”
- “Setting the Ethernet Port in Loopback Mode”

Entering Ethernet Port View

Before configuring the Ethernet port, enter Ethernet port view first.

Perform the following configuration in system view.

Table 67 Entering Ethernet port view

Operation	Command
Enter Ethernet port view	interface <i>interface-type interface-number</i>

Enabling/Disabling an Ethernet Port

After configuring the related parameters and protocol of the port, you can use **undo shutdown** command to enable the port. If you do not want a port to forward data any more, use **shutdown** command to disable it.

Perform the following configuration in Ethernet port view.

Table 68 Enabling/disabling an Ethernet port

Operation	Command
Disable an Ethernet port	shutdown
Enable an Ethernet port	undo shutdown

By default, the port is enabled.

Setting Ethernet Port Description

To distinguish the Ethernet ports, you can use the following command to make some necessary descriptions.

Perform the following configuration in Ethernet port view.

Table 69 Setting Ethernet port description

Operation	Command
Set an Ethernet port description	description <i>text</i>
Delete the Ethernet port description	undo description

By default, an Ethernet port has no description.

Setting the Duplex Attribute of the Ethernet Port

To configure a port to send and receive data packets at the same time, set it to full-duplex. To configure a port to either send or receive data packets at a time, set it to half-duplex. If the port has been set to auto-negotiation mode, the local and peer ports will automatically negotiate about the duplex mode.

Perform the following configuration in Ethernet port view.

Table 70 Setting the duplex attribute for the Ethernet port

Operation	Command
Set duplex attribute for Ethernet port	duplex { auto full half }
Restore the default duplex attribute of Ethernet port	undo duplex

Note that, 10/100 Mbps electrical Ethernet port can operate in full-duplex, half-duplex or auto-negotiation mode. The 10/100/1000 Mbps electrical Ethernet port can operate in full duplex, half duplex or auto-negotiation mode. When the port operates at 1000 Mbps or in auto mode, the duplex mode can be set to **full** (full duplex) or **auto** (auto-negotiation). The optical 100/1000 Mbps and 10 Gbps Ethernet ports work in full duplex mode without user intervention.

The port defaults the **auto** (auto-negotiation) mode.

Setting Speed on the Ethernet Port

You can use the following command to set the speed on the Ethernet port. If the speed is set to auto-negotiation mode, the local and peer ports will automatically negotiate about the port speed.

Perform the following configuration in Ethernet port view.

Table 71 Setting speed on the Ethernet port

Operation	Command
Set Ethernet port speed	speed { 10 100 1000 10000 auto }
Restore the default speed on Ethernet port	undo speed

The optional parameters of this command are determined by the port types and duplex modes. For example, the 10/100/1000 electrical ports support three optional parameters including 10 Mbps, 100 Mbps, and 1000 Mbps. You can select proper port speed as you require. But when the duplex mode is changed into half duplex mode, the port speed can be set to 1000 Mbps or **auto**.

Note that, the 10/100 Mbps electrical Ethernet port can operate at 10 Mbps, 100 Mbps and in auto mode. You can set it accordingly. The 10/100/1000Mbps electrical Ethernet port can operate at 10 Mbps, 100 Mbps, or 1000 Mbps as per different requirements. However in half duplex mode, the port cannot operate at 1000 Mbps or in auto mode. The 100 Mbps optical Ethernet port supports 100 Mbps; the 1000 Mbps optical Ethernet port supports 1000 Mbps; the 10 Gbps optical Ethernet port supports 10 Gbps without user intervention.

By default, the speed of the port is in **auto** mode.

Setting the Cable Type for the Ethernet Port

The Ethernet port supports the straight-through and cross-over network cables. The following command can be used for configuring the cable type.

Perform the following configuration in Ethernet port view.

Table 72 Setting the type of the cable connected to the Ethernet port

Operation	Command
Set the type of the cable connected to the Ethernet port	mdi { across auto normal }
Restore the default type of the cable connected to the Ethernet port	undo mdi

Note that, the settings only take effect on 10/100 Mbps and 10/100/1000 Mbps electrical ports.

By default, the cable type is **auto** (auto-recognized). That is, the system can automatically recognize the type of cable connecting to the port.

Enabling/Disabling Flow Control for the Ethernet Port

After enabling flow control in both the local and the peer switch, if congestion occurs in the local switch, the switch will inform its peer to pause packet sending. Once the peer switch receives this message, it will pause packet sending, and vice versa. In this way, packet loss is reduced effectively. The flow control function of the Ethernet port can be enabled or disabled through the following command.

Perform the following configuration in Ethernet port view.

Table 73 Enabling/disabling flow control for the Ethernet port

Operation	Command
Enable Ethernet port flow control	flow-control
Disable Ethernet port flow control	undo flow-control

By default, Ethernet port flow control is disabled.

Setting the Interval of Performing Statistics on Ports

Use the following configuration tasks to set the interval of performing statistics on ports. The switch performs the statistics about the average speed during the interval.

Perform the following configuration in Ethernet port view to set the interval of performing statistics on ports.

Table 74 Set the interval of performing statistics on ports

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	Interface <i>interface-type</i> <i>interface-number</i>	Optional; The <i>interface-type</i> argument is the Ethernet port type
Enter PoS port view	Interface <i>interface-type</i> <i>interface-number</i>	Optional; The <i>interface-type</i> argument is the PoS port type
Set the interval of performing statistics on ports	flow-interval <i>interval</i>	Required; The interval of performing statistics on ports is 300 seconds by default

Enabling/Disabling Jumbo Frames' Passing a Card

During large throughput data switching, like file transmission, a card may encounter jumbo frames larger than the standard Ethernet frame length. The following command can be used to enable jumbo frames to pass a card or disable them from passing a card.

Perform the following configuration in system view.

Table 75 Enabling/disabling jumbo frames' passing a card

Operation	Command
Enable Jumbo frames to pass the card on a specified slot, and set the maximum length of Jumbo frames allowed to pass the card	jumboframe enable [<i>jumboframe-value</i>] slot <i>slot-num</i>
Disable Jumbo frames from passing the card on a specified slot	jumboframe disable slot <i>slot-num</i>

By default, jumbo frames are allowed to pass cards.



The system supports discrete values of Jumbo frame lengths ranging from 1536 to 10240. However, effective Jumbo frame values fall into several sections: the

effective Jumbo frame value for the 1536-1552 section is 1552, that for the 1553-9022 section is 9022, that for the 9023-9192 section is 9192, and that for the 9193-10240 section is 10240.

Setting Broadcast/Multicast Suppression on Ethernet Port

To prevent port congestion resulting from broadcast/multicast packet flooding, the switch supports broadcast/multicast suppression. You can enable broadcast/multicast suppression by setting the speed percentage or bandwidth values..

Perform the following configuration in Ethernet port view.

Table 76 Setting broadcast/multicast suppression on Ethernet port

Operation	Command
Configure broadcast suppression ration Ethernet port	broadcast-suppression { <i>ratio</i> bandwidth bandwidth }
Restore the default setting of broadcast suppression on Ethernet port	undo broadcast-suppression
Configure multicast suppression ration Ethernet port	multicast-suppression { <i>ratio</i> bandwidth bandwidth }
Restore the default setting of multicast suppression on Ethernet port	undo multicast-suppression



CAUTION:

- You cannot enable both broadcast suppression and multicast suppression simultaneously on the same card. Namely, once you have enabled broadcast suppression on some ports of a card, you cannot enable multicast suppression on the other ports of the card, and vice versa.
- If multicast suppression is enabled, broadcast packets are also suppressed at the same time, while broadcast suppression does not work on multicast suppression.
- No distinction is made between known multicast and unknown multicast for multicast suppression.

By default, the broadcast suppression ratio is 50%, while the multicast suppression ratio is 100%.

Setting the Ethernet Port Mode

Most ports adopt the LAN mode for general data exchange. The port must work in WAN mode, however, if it needs special frame format for data transfer (such as in fiber transmission). You can configure network mode available on the port using the **port-mode** command.

Perform the following configuration in Ethernet port view.

Table 77 Setting the Ethernet port mode

Operation	Command
Set the Ethernet port mode	port-mode { wan lan }
Restore the default Ethernet port mode	undo port-mode

By default, Ethernet ports works in LAN mode. 10GE Ethernet ports support WAN mode.

Setting the Link Type for the Ethernet Port

Ethernet port can operate in three different link types, access, hybrid, and trunk types. The access port carries one VLAN only, used for connecting to the user's computer. The trunk port can belong to more than one VLAN and receive/send the packets on multiple VLANs, used for connection between the switches. The hybrid port can also carry more than one VLAN and receive/send the packets on multiple VLANs, used for connecting both the switches and user's computers. The difference between the hybrid port and the trunk port is that the hybrid port allows the packets from multiple VLANs to be sent without tags, but the trunk port only allows the packets from the default VLAN to be sent without tags.

Perform the following configuration in Ethernet port view.

Table 78 Setting the link type for the Ethernet port

Operation	Command
Configure the port as access port	port link-type access
Configure the port as hybrid port	port link-type hybrid
Configure the port as trunk port	port link-type trunk
Restore the default link type, that is, the access port	undo port link-type

You can configure three types of ports concurrently on the same switch, but you cannot switch between trunk port and hybrid port. You must turn it first into access port and then set it as other type. For example, you cannot configure a trunk port directly as hybrid port, but first set it as access port and then as hybrid port.

By default, the port is access port.

Adding the Ethernet Port to Specified VLANs

The following commands are used for adding an Ethernet port to a specified VLAN. The access port can only be added to one VLAN, while the hybrid and trunk ports can be added to multiple VLANs.

Perform the following configuration in Ethernet port view.

Table 79 Adding the Ethernet port to specified VLANs

Operation	Command
Add the current access port to a specified VLAN	port access vlan <i>vlan-id</i>
Add the current hybrid port to specified VLANs	port hybrid vlan <i>vlan-id-list</i> { tagged untagged }
Add the current trunk port to specified VLANs	port trunk permit vlan { <i>vlan-id-list</i> all }
Remove the current access port from to a specified VLAN	undo port access vlan
Remove the current hybrid port from to specified VLANs	undo port hybrid vlan <i>vlan-id-list</i>
Remove the current trunk port from specified VLANs	undo port trunk permit vlan { <i>vlan-id-list</i> all }

Note that the access port shall be added to an existing VLAN other than VLAN 1. The VLAN to which Hybrid port is added must have been existed.

After adding the Ethernet port to specified VLANs, the local port can forward packets of these VLANs. The hybrid and trunk ports can be added to multiple VLANs, thereby implementing the VLAN intercommunication between peers. For the hybrid port, you can configure to tag some VLAN packets, based on which the packets can be processed differently.

Setting the Default VLAN ID for the Ethernet Port

Since the access port can only be included in one VLAN only, its default VLAN is the one to which it belongs. The hybrid port and the trunk port can be included in several VLANs, it is necessary to configure the default VLAN ID. If the default VLAN ID has been configured, the packets without VLAN Tag will be forwarded to the port that belongs to the default VLAN. When sending the packets with VLAN Tag, if the VLAN ID of the packet is identical to the default VLAN ID of the port, the system will remove VLAN Tag before sending this packet.

Perform the following configuration in Ethernet port view.

Table 80 Setting the default VLAN ID for the Ethernet port

Operation	Command
Set the default VLAN ID for the hybrid port	port hybrid pvid vlan <i>vlan-id</i>
Set the default VLAN ID for the trunk port	port trunk pvid vlan <i>vlan-id</i>
Restore the default VLAN ID of the hybrid port to the default value	undo port hybrid pvid
Restore the default VLAN ID of the trunk port to the default value	undo port trunk pvid

Note that: to guarantee the proper packet transmission, the default VLAN ID of local hybrid port or Trunk port should be identical with that of the hybrid port or Trunk port on the peer switch.

By default, the VLAN of hybrid port and trunk port is VLAN 1 and that of the access port is the VLAN to which it belongs

Setting the VLAN VPN Feature on a Port

A VLAN Tag consists of only 12 bits (defined by IEEE802.1Q), so Ethernet Switches can support up to 4k VLANs. In networking, especially in MAN (metropolitan area network), a large numbers of VLANs are required to segment users. In this case, 4k VLANs are not enough.

The port VLAN VPN feature of the switch can provide duplex VLAN Tags to a packet, namely, mark the packet with another VLAN Tag besides the original one, thus to provide 4k x 4k VLANs to meet user's demands for VLANs. At the same time, the port VLAN VPN feature provides the following functions: using the original VLAN Tag to differentiate users and services, and using the new VLAN Tag to load service and VPN users. These make VLAN configuration simple and practicable. Through VLAN VPN configuration, Ethernet Switches can meet the requirement in MAN.

If VLAN VPN is enabled on a port, every packet received on the port (no matter whether the packet carries a VLAN Tag or not) will be given a new Tag that specifies the default VLAN of this port. Thus, if the port receives a packet that

already carries a VLAN Tag, the packet will get two Tags; if the port receives an untagged packet, the packet will be given a default VLAN Tag of the port.

Perform the following configuration in Ethernet port view.

Table 81 Setting the port VLAN VPN feature

Operation	Command
Enable the port VLAN VPN feature	vlan-vpn enable
Disable the port VLAN VPN feature	undo vlan-vpn

Note that if any of GVRP, STP, and 802.1x has been enabled on a port, the VLAN VPN feature cannot be enabled on the port.

By default, the port VLAN VPN feature is disabled.

Copying Port Configurations to Other Ports

To keep the configurations of other ports consistent with a specified port, you can use **copy configuration** command to copy the configurations of that specified port to other ports. Such configurations may involve: STP setting, QoS setting, LACP setting, and port setting. The detailed table is as follows:

Table 82 Configurations that can be copied

Attribute	Detailed Setting
STP setting	Enable/disable STP
	Port priority
	Path cost
	Link attributes(point-to-point or not)
	Port mCheck
	Max transmission speed
	Enable/disable root protection
	Enable/disable loop protection
	Edge or non-edge port
	Reset ARP or not
QoS setting	Define/apply flow template
	Traffic reshaping
	Traffic redirection
	Packet filtering
	Priority re-assignment
	Traffic statistics
Port setting	Traffic mirroring
	Rate limiting
	Permitted VLAN ID
	Default VLAN ID
	Add ports to VLAN
	Default 802.1p priority
	Port speed, duplex mode
	Port link type

Table 82 Configurations that can be copied

Attribute	Detailed Setting
LACP	Enable/disable LACP on the port



- Using copy configuration command will clear protocol VLAN attributes of the destination port, but it can not copy protocol VLAN attributes of source port to the destination port.
- Using the **copy configuration** command, you can only copy the configurations of Ethernet ports, Gigabit Ethernet ports and aggregation groups.

Perform the following configuration in system view

Table 83 Copying port configurations to other ports

Operation	Command
Copy port configurations to other ports	copy configuration source { <i>interface-type interface-number</i> aggregation-group <i>agg-id</i> } destination { <i>interface-list</i> [aggregation-group <i>agg-id</i>] }

Note that if the copy source is an aggregation group, the Active port with the smallest number will be taken as the source; if the copy destination is an aggregation group, the configurations of all ports in the group will be updated to the configurations of the source. You cannot specify a dynamic aggregation group as the destination port of the **copy** command.

Setting Port Hold Time

If the Down/Up operation is implemented on ports too frequently, the switch may fail. Therefore, you can configure port hold time to prohibit frequent change of the port status.

Perform the following configuration in system view.

Table 84 Setting the port hold time

Operation	Command
Set the port hold time	link-status hold <i>hold-time</i>
Restore the default value	undo link-status hold

By default, the port hold time is set to 3 seconds.

Setting the Ethernet Port in Loopback Mode

Perform the following configuration in Ethernet port view.

Table 85 Setting the Ethernet port in loopback mode

Operation	Command
Set the Ethernet port in loopback mode	loopback { external internal }
Remove loopback configuration on the port	undo loopback

By default, the Ethernet port is set in loopback mode. At present, the Ethernet ports of the Switch 8800 Family series switches do not support the **external** loopback mode.

Displaying and Debugging Ethernet Port

After the above configuration, execute **display** command in any view to display the running of the Ethernet port configuration, and to verify the effect of the configuration.

Execute **reset** command in user view to clear the statistics information of the port.

Table 86 Displaying and debugging Ethernet port

Operation	Command
Display all the information of the port	display interface <i>interface-type</i> <i>interface-type interface-number</i> [<i>packets</i>]
Display hybrid port or trunk port	display port { hybrid trunk }
Display the statistics information of the port	display counters [<i>rate</i>] { inbound outbound } interface [<i>interface-type</i>]
Clear the statistics information of the port	reset counters interface [<i>interface_type</i> <i>interface-type interface-number</i>]
View Jumbo frame configuration on all cards	display jumboframe configuration



- The Switch 8800 Family series do not support the **Loopback External** mode.
- When 802.1x is enabled on a port, the statistics information of the port cannot be cleared.
- By default, the **display counters** command displays the traffic statistic information of all ports in service.
- The supported Jumbo frame length ranges, as well as the default values, may vary from card to card.

Ethernet Port Configuration Example

Network requirements

Switch A is connected to Switch B through Trunk port GigabitEthernet2/1/1. Configure the Trunk port with default VLAN ID, so that: when receiving the packets without VLAN Tag, the port can forward them to the member ports belonging to the default VLAN; when it sending the packets with VLAN Tag and the packet VLAN ID is the default VLAN ID, the Trunk port remove the packet VLAN Tag and forward the packet.

Network diagram

Figure 18 Network diagram for Ethernet port configuration



Configuration procedure

The following configurations are used for Switch A. Please configure Switch B in the similar way.

Enter the Ethernet port view of GigabitEthernet2/1/1.

```
[SW8800] interface gigabitethernet2/1/1

# Set the GigabitEthernet2/1/1 as a trunk port and allows VLANs 2, 6 through 50,
and 100 to pass.

[3Com-GigabitEthernet2/1/1] port link-type trunk
[3Com-GigabitEthernet2/1/1] port trunk permit vlan 2 6 to 50 100

# Create the VLAN 100.

[SW8800] vlan 100

# Configure the default VLAN ID of GigabitEthernet2/1/1 as 100.

[3Com-GigabitEthernet2/1/1] port trunk pvid vlan 100
```

Ethernet Port Troubleshooting

Symptom 1: Default VLAN ID configuration fails.

Solution: Take the following steps:

- Execute the **display interface** or **display port** command to check if the port is a trunk port or a hybrid port. If it is neither of them, configure it as a trunk or hybrid port.
- Then configure the default VLAN ID.

Symptom 2: The port is in down status.

Solution: Please check

- If the cable connection is correct and if the optical fiber cable is inversely connected.
- If the **shutdown** command is used on the port.
- If the right optical module is inserted.

14

LINK AGGREGATION CONFIGURATION

Overview

Introduction to Link Aggregation

Link aggregation means aggregating several ports together to implement the outgoing/incoming payload balance among the member ports and enhance the connection reliability. Link aggregation may be manual aggregation, dynamic LACP aggregation or static LACP aggregation. For the member ports in an aggregation group, their basic configurations must be the same. That is, if one is a trunk port, others must also be; when it turns into access port, then others must change to access port.

Basic configuration includes STP setting, QoS setting, VLAN setting, and port setting. The STP setting includes STP enabling/disabling, link attribute (point-to-point or not), STP priority, path cost, max transmission speed, loop protection, root protection, edge port or not. The QoS setting includes traffic limiting, priority marking, default 802.1p priority, bandwidth assurance, congestion avoidance, traffic redirection, and traffic statistics. The VLAN setting includes permitted VLAN types, default VLAN ID. The port setting includes port link type.

One Switch 8800 Family series routing switch can support up to 920 aggregation groups. IDs 1 through 31 indicate manual or static aggregation groups. IDs 32 through 64 are reserved. IDs 65 through 192 are routed trunks; IDs 193 through 920 indicate dynamic aggregation groups. The systems with MPLS VPN cards only support seven load balancing aggregation groups; those without MPLS VPN cards support 31 load balancing aggregation groups. The systems with FE modules using EX chips only supports seven load balancing aggregation groups.



At present, Switch 8800 Family series also support trans-module aggregation. The trans-module aggregation is the same as the intra-module aggregation.

Introduction to LACP

Link aggregation control protocol (LACP) based on the IEEE802.3ad standard can be used in dynamic link aggregation. An LACP-enabled port sends link aggregation control protocol data units (LACPDUs) to tell the peer about its system priority, system MAC address, port priority, port number and operation key. After receiving the information from the sender, the receiver compares it with the locally saved information about other ports, chooses member ports for the aggregation group and reaches agreement about if a port can join or leave a dynamic aggregation group.

During port aggregation, LACP generates a configuration mix according to the port configuration (rate, duplex, basic configuration, management key), which is called an operation key. The management key of an LACP-enabled dynamic aggregation port is 0 by default. The management key of an LACP-enabled static

aggregation port is the same as the aggregation group ID. In a dynamic aggregation group, the member ports must have the same operation key. In manual and static aggregation groups, the active ports have the same operation key.

Aggregation Types Port aggregation can be divided into manual aggregation, dynamic LACP aggregation and static LACP aggregation.

Manual aggregation and static LACP aggregation

Both manual aggregation and static LACP aggregation are configured manually, and cannot be added or removed automatically by the system. A manual or static LACP aggregation group must contain a member port at least. In the case of one port in an aggregation group, the unique method for you to remove the port from the aggregation group is to delete the aggregation group. By default, the system disables the LACP for the manual aggregation port. You are prohibited to enable the LACP for the manual aggregation port. By default, the system enables the LACP for the static aggregation port. When a static aggregation group is removed, the member ports will form one or more dynamic LACP aggregation groups with LACP enabled. You are prohibited to disable the LACP for the static aggregation port.

In manual and static aggregation groups, ports can be in active or inactive state. The port in active state can transmit and receive user service packets, but the port in inactive state cannot. The active port with the minimum port number serves as the master port, while others as slave ports.

In a manual aggregation group, the system sets the ports to active or inactive state based on these rules:

- Based on the descending order of priority levels from full duplex/high speed, to full duplex/low-speed, to half duplex/high speed and till half duplex/low speed, the system sets the port with the highest priority to active state, and others to inactive state.
- The system sets to inactive state the ports which cannot aggregate with the master port, due to hardware limit (such as trans-module aggregation is forbidden).
- The system sets to inactive state the ports with basic configurations different from the active port.

In a static aggregation group, the system sets the ports to active or inactive state based on these rules:

- Based on the descending order of priority levels from full duplex/high speed, to full duplex/low-speed, to half duplex/high speed and till half duplex/low speed, the system sets the port with the highest priority to active state, and others to inactive state.
- The system sets to inactive state the active port connecting to the different peer devices, or the port connecting to the same peer device but locating in the different aggregation group.

- The system sets to inactive state the ports which cannot be aggregated with the port, due to hardware limit (for example, trans-module aggregation is forbidden).
- The system sets to inactive state the ports with basic configurations different from the active port.

Since only a defined number of ports can be added in an aggregation group, then if the active ports in an aggregation group exceed the maximum threshold for that group, the system shall set some ports with smaller port numbers (in ascending order) as active ports and others as inactive ports. Both active and inactive ports can transmit and receive LACP protocol, but the inactive ports cannot forward user service packets.

Dynamic LACP aggregation

The system can create/delete automatically dynamic LACP aggregations, and you cannot add/delete member ports into/from dynamic LACP aggregation. The system can also aggregate one port, which is called single port aggregation. The dynamic LACP aggregation LACP is in enabled state. The system can only aggregate the ports with the same speed, duplex attribute, device connection, basic configuration.

Since only a defined number of ports can be added in an aggregation group, then if the current member ports in an aggregation group exceed the maximum threshold for that group, the system shall set some ports with smaller device ID (system priority + system MAC address) and smaller port ID (port priority + port number) as active ports, and others as inactive ports. If the maximum threshold is not exceeded, all member ports are active ports. Both active and inactive ports can transmit and receive LACP protocol, but the inactive ports cannot forward user service packets. In an aggregation group, the active port with the minimum port number serves as the master port, while others as slave ports. When comparing device ID, the system compare system priority first, and then system MAC address in the case of the same system priority. The smaller device ID is regarded as higher priority. When comparing port ID, the system compares port priority first, and then port number in the case of the same port priority. The smaller port ID is regarded as higher priority. If the device ID changes to higher priority, the active and inactive state of the member ports in an aggregation group depends on the device port ID. You can also set system and port priority to define active and inactive ports.

Load Sharing Types of Load sharing

In terms of load balancing, link aggregation may be load balancing aggregation and non-load balancing aggregation. The 8500 series allocate IP packet load sharing according to destination and source IP addresses. The switches allocate non-IP packet load sharing according to source and destination MAC addresses. You can check protocol types in determining if to use IP or MAC addresses. The packet with 0800 ETYP Ethernet field is IP packet. In general, the system only provides limited resources. The system will always allocate hardware aggregation resources to the load balancing aggregation groups with higher priority levels. When the load sharing aggregation resources are used up for existing aggregation groups, newly-created aggregation groups will be non-load sharing ones. The priority levels (in descending order) for allocating load sharing aggregation resources are as follows:

- Aggregation groups of special ports with hardware aggregation resources included, such as non-limited-speed 10GE ports
- Aggregation groups that probably reach the maximum potential rate after the resources are allocated to them
- Aggregation groups with the minimum master port numbers if they reach the equal rate with other groups after the resources are allocated to them
- Manual aggregation has a higher priority level than static aggregation, and static aggregation has a higher priority level than dynamic aggregation
- Under the same conditions, an aggregation group that has occupied resources has a higher priority level than an aggregation group waiting for occupied

When aggregation groups of higher priority levels appear, the aggregation groups of lower priority levels release their hardware resources. For single-port aggregation groups, if they can transmit and receive packets normally without occupying hardware resources, they shall not occupy the resources.

Port state

In a aggregation group, its ports may be in active or inactive state and only the active ports can transmit and receive user service packets, but not inactive ports. The active port with the minimum port number serves as the master port, while others as slave ports.

In a aggregation group, the system sets the ports to active or inactive state based on these rules:

- Based on the descending order of priority levels from full duplex/high speed, to full duplex/low-speed, to half duplex/high speed and till half duplex/low speed, the system sets the port with the highest priority to active state, and others to inactive state.
- The system sets to inactive state the ports which cannot aggregate with the master port, due to hardware limit.
- The system sets to inactive state the ports with basic configurations different from the master port.

Since only a defined number of ports can be supported in an aggregation group, then if the active ports in an aggregation group exceed the port quantity threshold for that group, the system shall set some ports with smaller port numbers (in ascending order) as active ports and others as inactive ports. The active ports can transmit and receive user service packets, but not inactive ports.

A load sharing aggregation group may contain several active ports, but a non-load sharing aggregation group can only have one active port, while others as inactive ports.

Link Aggregation Configuration

The following sections describe link aggregation tasks:

- “Enabling/Disabling LACP at Port”
- “Creating/Deleting an Aggregation Group”
- “Adding/Deleting an Ethernet Port into/from an Aggregation Group”

- “Configuring/Deleting Aggregation Group Description”
- “Configuring System Priority”
- “Configuring Port Priority”



- The active state and inactive state correspond to selected and standby respectively.
- When configuring an aggregation group, the status of GVRP feature configured on the master port is reserved, but that on the slave port is disabled.
- When adding a port to an existing aggregation group, the GVRP feature on the port is disabled.
- When the master port leaves an aggregation group, the status of GVRP feature on both the group and port is reserved; when a slave port leaves an aggregation group, the GVRP feature on the port is disabled.
- When configuring GVRP feature on any port in an aggregation group, the configuration is mapped to the master port of the group.
- When querying the GVRP feature configured on any port in an aggregation group, the returned result is about the master port of the group.

For details, refer to the "VLAN&QinQ" part of this manual

Enabling/Disabling LACP at Port

You should first enable LACP at the ports before performing dynamic aggregation, so that both parties can agree on adding/deleting the ports into/from a dynamic LACP aggregation group.

Perform the following configuration in Ethernet port view.

Table 87 Enabling/disabling LACP on a port

Operation	Command
Enable LACP on a the port	lACP enable
Disable LACP on a the port	undo lACP enable

By default, LACP is not enabled at the port.

Note that:

- You cannot enable LACP at the mirroring port, the port with static MAC address configured, and the port with static ARP configured, port with 802.1x enabled.
- You are inhibited to enable LACP at the port in a manual aggregation group.
- You can add a port with LACP disabled to a static LACP aggregation group, and then the LACP will be enabled automatically.

Creating/Deleting an Aggregation Group

You can use the following command to create/delete an aggregation group (for manual aggregation and static link aggregation). When you delete an aggregation group, all its member ports are disaggregated.

Perform the following configuration in system view.

Table 88 Creating/deleting an aggregation group

Operation	Command
Create an aggregation group	link-aggregation group <i>agg-id</i> mode { manual static }
Delete an aggregation group	undo link-aggregation group <i>agg-id</i>

During creating an aggregation group, if it already exists in the system but contains no member port, it changes to the new type. When you change a static LACP aggregation group to a manual one, LACP shall be disabled at the member ports automatically.



Port aggregation includes manual aggregation, static aggregation and dynamic aggregation.

- In the manual aggregation mode, ports working at different rates can be aggregated. Manual aggregation can be load balancing aggregation if the aggregation resource is available. In this case, if the traffic rate shared by a low-rate port exceeds the maximum rate of the port, packets may be lost.
- In the static aggregation mode, ports working at different rates can also be aggregated. However, the selected/standby state of statically aggregated ports is determined by the transmission rate. Only the ports with the maximum rate and in full-duplex mode can be selected to forward traffic, while other standby ports do not forward traffic.

Adding/Deleting an Ethernet Port into/from an Aggregation Group

You can add/delete ports into/from an aggregation group.

Perform the following configuration in the corresponding view.

Table 89 Adding/deleting an Ethernet port into/from an aggregation group

Operation	Command
Add an Ethernet port into the aggregation group (Ethernet port view)	port link-aggregation group <i>agg-id</i>
Delete an Ethernet port from the aggregation port (Ethernet port view)	undo port link-aggregation group
Aggregate Ethernet ports (system view)	link-aggregation <i>interface-name1</i> to <i>interface-name2</i> [both]

Note that:

- You cannot add a mirrored port, a port configured with a static MAC address, a port with 802.1x enabled, or a VPN port into an aggregation group.
- You must delete the aggregation group, instead of the port, if the aggregation group contains only one port.
- When master port enables VLAN VPN, aggregation is permitted in the system. Because the link type of slave port will always keep same as that of master port. When both master port and slave have VLAN VPN disabled, aggregation is permitted in the system, it is average aggregation. After the port enabling VLAN VPN, aggregation is not permitted in the system, at the same time, the system will tell users that the slave port in the aggregation group conflict with the master port on VLAN VPN.

- When a port is added into an aggregation group, the original ARP information of the port will be lost.

Configuring/Deleting Aggregation Group Description

You can use the following command to create/delete aggregation group description (for manual aggregation and static link aggregation).

Perform the following configuration in system view.

Table 90 Configuring/deleting aggregation group description

Operation	Command
Set an aggregation group description	link-aggregation group <i>agg-id</i> description <i>aname</i>
Delete the aggregation group description	undo link-aggregation group <i>agg-id</i> description

By default, an aggregation group has no description.



You cannot configure the description for a dynamic aggregation group.

Configuring System Priority

The LACP refers to system IDs in determining if the member ports are active and inactive for a dynamic LACP aggregation group. The system ID consists of two-byte system priority and six-byte system MAC, that is, system ID = system priority + system MAC. In comparing system IDs, the system first compares system priority values; if they are equal, then it compares system MAC addresses. The smaller system ID is considered prior.

Changing system priority may affect the priority levels of member ports, and further their active or inactive state.

Perform the following configuration in system view.

Table 91 Configuring system priority

Operation	Command
Configure system priority	lacp system-priority <i>system-priority-value</i>
Restore the default system priority	undo lacp system-priority

By default, system priority is 32,768.

Configuring Port Priority

The LACP compares system IDs first and then port IDs (if system IDs are the same) in determining if the member ports are active or inactive ones for a dynamic LACP aggregation group. If the ports in an aggregation group exceed the port quantity threshold for that group, the system shall set some ports with smaller port IDs as active ports and others as inactive ports. The port ID consists of two-byte port priority and two-byte port number, that is, port ID = port priority + port number. The system first compares port priority values and then port numbers and the small port ID is considered prior.

Perform the following configuration in Ethernet port view.

Table 92 Configuring port priority

Operation	Command
Configure port priority	lACP port-priority <i>port-priority-value</i>
Restore the default port priority	undo lACP port-priority

By default, port priority is 32,768.

Displaying and Debugging Link Aggregation

After the above configuration, execute the **display** command in any view to display the running of the link aggregation configuration, and to verify the effect of the configuration.

In user view, execute the **reset** command to clear statistics on the LACP-enabled port, and the **debugging** command to enable LACP debugging.

Table 93 Displaying and debugging link aggregation

Operation	Command
Display summary information of all aggregation groups	display link-aggregation summary
Display detailed information of a specific aggregation group	display link-aggregation verbose [<i>agg-id</i>]
Display the local device ID	display lACP system-id
Display detailed link aggregation information at the port	display link-aggregation interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>]
Clear LACP statistics on the port	reset lACP statistics [interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>]]
Disable/enable LACP state debugging	[undo] debugging lACP state [interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>]] { actor-churn mux partner-churn ptx rx }* all }
Disable/enable LACP packet debugging	[undo] debugging lACP packet [interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>]]
Disable/enable link aggregation error debugging	[undo] debugging link-aggregation error
Disable/enable link aggregation event debugging	[undo] debugging link-aggregation event

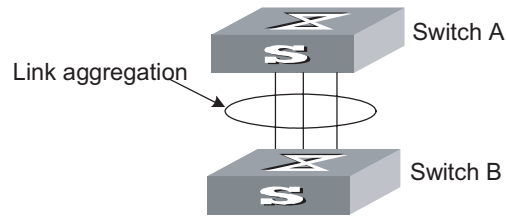
Link Aggregation Configuration Example

Network requirements

Switch A connects switch B with three aggregation ports, numbered as Ethernet2/1/1 to Ethernet2/1/3, so that incoming/outgoing load can be balanced among the member ports.

Network diagram

Figure 19 Network diagram for link aggregation configuration



Configuration procedure

The following only lists the configuration for switch A, and that on switch B is similar.

1 Manual aggregation

Create aggregation group 1.

```
[SW8800] link-aggregation group 1 mode manual
```

Add Ethernet ports Ethernet2/1/1 to Ethernet2/1/3 into aggregation group 1.

```
[SW8800] interface ethernet2/1/1
[3Com-Ethernet2/1/1] port link-aggregation group 1
[3Com-Ethernet2/1/1] interface ethernet2/1/2
[3Com-Ethernet2/1/2] port link-aggregation group 1
[3Com-Ethernet2/1/2] interface ethernet2/1/3
[3Com-Ethernet2/1/3] port link-aggregation group 1
# When the aggregation group numbers are continuous, you can directly
aggregate multiple ports into a group. The group number is allocated by the
system.
[SW8800] link-aggregation ethernet2/1/1 to ethernet2/1/3 both
```

2 Static LACP aggregation

Create aggregation group 1.

```
[SW8800] link-aggregation group 1 mode static
```

Add Ethernet ports Ethernet2/1/1 to Ethernet2/1/3 into aggregation group 1.

```
[SW8800] interface ethernet2/1/1
[3Com-Ethernet2/1/1] port link-aggregation group 1
[3Com-Ethernet2/1/1] interface ethernet2/1/2
[3Com-Ethernet2/1/2] port link-aggregation group 1
[3Com-Ethernet2/1/2] interface ethernet2/1/3
[3Com-Ethernet2/1/3] port link-aggregation group 1
```

3 Dynamic LACP aggregation

Enable LACP on Ethernet ports Ethernet2/1/1 to Ethernet2/1/3.

```
[SW8800] interface ethernet2/1/1
[3Com-Ethernet2/1/1] lacp enable
[3Com-Ethernet2/1/1] interface ethernet2/1/2
[3Com-Ethernet2/1/2] lacp enable
```

```
[3Com-Ethernet2/1/2] interface ethernet2/1/3  
[3Com-Ethernet2/1/3] lacp enable
```

You must set basic configuration, rate and duplex attribute consistent at both ends to aggregate successfully the LACP-enabled ports into a dynamic aggregation group and achieve load sharing.

15

PORT ISOLATION CONFIGURATION

Port Isolation Overview

Using the port isolation feature, you can place different user ports into the same VLAN. As these users cannot communicate with each other, network security improved, a flexible networking scheme is provided, and VLAN resources are conserved.

Configuration Tasks

Table 94 Configuration tasks

Configuration tasks	Description	Detailed configuration
Configure an isolated group	Required	Refer to section "Configuring an Isolated Group"
Configure an upstream port for an isolated group	Required	Refer to section "Configuring an Uplink Port in the Isolated Group"
Configure isolated ports for an isolated group	Required	Refer to section "Configuring Isolated Ports for an Isolated Group"



Layer 3 interfaces should not be configured on VLANs containing isolated ports, otherwise, Layer 3 packets maybe fail to forward.

Configuring an Isolated Group

Table 95 Configuring an isolated group

Operation	Command	Description
Enter system view	system-view	-
Configure an isolated group	port-isolate group <i>isolate-group-id</i>	Required Ports in the isolated group can only communicate with the upstream ports. The isolated ports and the upstream ports must be in the same VLAN.
Query isolation information	display port-isolate group [<i>isolate-group-id</i>] [verbose]	You can carry out this command in any view

Configuring an Uplink Port in the Isolated Group

Table 96 Configuring an uplink port in the isolated group

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	Required

Table 96 Configuring an uplink port in the isolated group

Operation	Command	Description
		Required
Configure the upstream port in the isolated group	port-isolate uplink-port group <i>isolate-group-id</i>	<ul style="list-style-type: none"> You can configure the uplink port for the isolated group only after you create the isolated group The upstream port can only be an Ethernet port You can configure only one upstream port for one isolated group. And the uplink port can be an aggregation group, but not a static or dynamic aggregation group
Query isolation information	display port-isolate group [<i>isolate-group-id</i>] [verbose]	You can carry out this command in any view

Configuring Isolated Ports for an Isolated Group

Table 97 Configuring isolated ports for the isolated group

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	Required
		Required
Configure isolated ports for the isolated group	port-isolate group <i>isolate-group-id</i>	<ul style="list-style-type: none"> You can configure isolated ports for the isolated group only after you create the isolated group. The isolated port can only be configured as an Ethernet port One port can join only one isolated port One port can be either an isolated port or an uplink port, but not both an isolated port and an uplink port in the same isolated group If the isolated port is a member of an aggregation group, other ports in the aggregation group will also join the isolated group
Query isolation information	display port-isolate group [<i>isolate-group-id</i>] [verbose]	You can carry out this command in any view

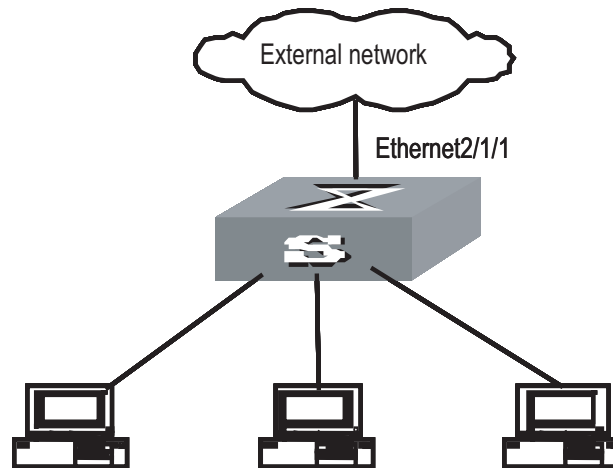
Port Isolation Configuration Example

Network requirements

Users in a community connect to a switch. The switch communicates with the external network through port Ethernet2/1/1. These users are in VLAN 1 and cannot communicate with each other.

Network diagram

Figure 20 Network diagram for port isolation



Configuration procedure

Create isolated group 1.

```
<SW8800>system-view
[SW8800] port-isolate group 1
```

Configure port Ethernet2/1/2 as an isolated port in isolated group 1.

```
[SW8800] interface Ethernet2/1/2
[SW8800-Ethernet2/1/2] port-isolate group 1
```

Configure port Ethernet2/1/1 as an upstream port in isolated group 1.

```
[SW8800] interface Ethernet2/1/1
[SW8800-Ethernet2/1/1] port-isolate uplink-port group 1
```


16

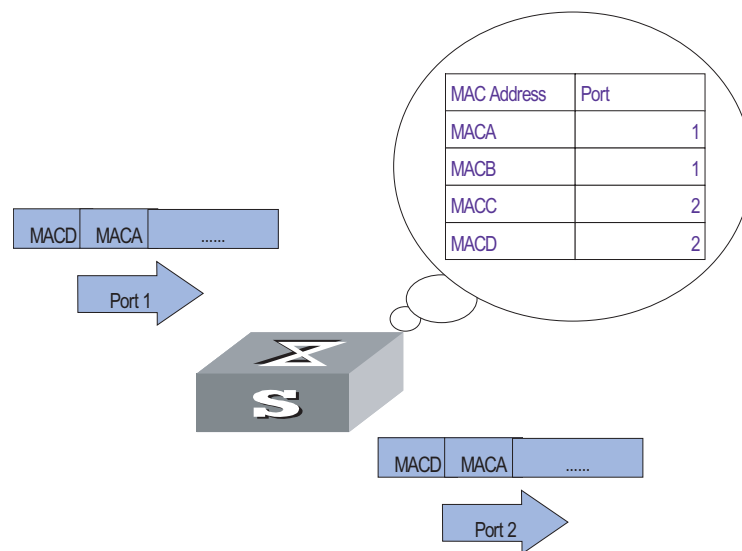
MAC ADDRESS TABLE MANAGEMENT

MAC Address Table Management Overview

A switch maintains a MAC address table for fast forwarding packets. A table entry includes the MAC address of a device and the port ID of the switch connected to the device. The dynamic entries (not configured manually) are learned by the switch. The switch learns a MAC address in the following way: after receiving a data frame from a port (assumed as port A), the switch analyzes its source MAC address (assumed as MAC_SOURCE) and considers that the packets destined at MAC_SOURCE can be forwarded through the port A. If the MAC address table contains the MAC_SOURCE, the switch will update the corresponding entry; otherwise, it will add the new MAC address (and the corresponding forwarding port) as a new entry to the table.

The system forwards the packets whose destination addresses can be found in the MAC address table directly through the hardware and broadcasts those packets whose addresses are not contained in the table. The network device will respond after receiving a broadcast packet and the response contains the MAC address of the device, which will then be learned and added into the MAC address table by the switch. The consequent packets destined the same MAC address can be forwarded directly thereafter.

Figure 21 The switch forwards packets with MAC address table



The switch also provides the function of MAC address aging. If the switch receives no packet for a period of time, it will delete the related entry from the MAC address table. However, this function takes no effect on the static MAC addresses.

You can configure (add or modify) the MAC address entries manually according to the actual networking environment. The entries can be static ones or dynamic ones.

MAC Address Table Management Configuration

The following sections describe the MAC address table management configuration tasks.

- “Setting MAC Address Table Entries”
- “Setting MAC Address Aging Time”
- “Maximum MAC Address Number Learned by Ethernet Port and Forwarding Option Configuration”
- “Configuring Max Number of MAC Addresses that can be Learned in a VLAN”

Setting MAC Address Table Entries

Administrators can manually add, modify, or delete the entries in MAC address table according to the actual needs. They can also delete all the (unicast) MAC address table entries related to a specified port or delete a specified type of entries, such as dynamic entries or static entries.

You can use the following commands to add, modify, or delete the entries in MAC address table.

Perform the following configuration in system view.

Table 98 Set MAC address table entries

Operation	Command
Add/Modify an address entry	mac-address { static dynamic } <i>mac-addr</i> interface <i>interface-type interface-number</i> vlan <i>vlan-id</i>
Delete an address entry	undo mac-address [static dynamic] [<i>mac-addr</i> [interface <i>interface-type interface-number</i>] vlan <i>vlan-id</i>] interface <i>interface-type interface-number</i> vlan <i>vlan-id</i>]

Setting MAC Address Aging Time

The setting of an appropriate aging time can effectively implement the function of MAC address aging. Too long or too short aging time set by subscribers will cause the problem that the switch broadcasts a great amount of data packets without MAC addresses, which will affect the switch operation performance.

If aging time is set too long, the switch will store a great number of out-of-date MAC address tables. This will consume MAC address table resources and the switch will not be able to update MAC address table according to the network change.

If aging time is set too short, the switch may delete valid MAC address table.

You can use the following commands to set the MAC address aging time for the system.

Perform the following configuration in system view.

Table 99 Set the MAC address aging time for the system

Operation	Command
Set the dynamic MAC address aging time	mac-address timer { aging age no-aging }
Restore the default MAC address aging time	undo mac-address timer aging

In addition, this command takes effect on all the ports. However the address aging only functions on the dynamic addresses (the learned or configured as age entries by the user).

By default, the *aging-time* is 300 seconds. With the key word **no-aging**, the command performs no aging on the MAC address entries.



CAUTION: The dynamic MAC address aging is completed during the second aging cycle.

Maximum MAC Address Number Learned by Ethernet Port and Forwarding Option Configuration

With MAC address learning, Switch 8800 Family switches can obtain MAC addresses of every network devices on network segments connecting to a port. As for packets destined to those MAC addresses, the switch directly uses hardware to forward them. An overlarge MAC address table may cause the low forwarding performance of the switch.

You can control the number of entries of the MAC address table by setting the maximum number of MAC addresses learned by a port. if you set the value to *count*, and when the number of MAC addresses learned by the port reaches this value, this port will no longer learn any more MAC addresses.

You can also set the switch to forward corresponding packets when the number of MAC addresses learned by the port exceeds the configured threshold.

Maximum MAC Address Number Learned by a Port and Forwarding Option Configuration Tasks

Perform the following configuration to set the maximum number of MAC addresses that can be learned by an Ethernet port and the processing policy to be adopted by the switch when this number is reached.

Table 100 Configure the maximum number of MAC addresses learned by a port and processing policy

Configuration item	Command	Description
Enter system view	<SW8800> system-view	-
Enter Ethernet port view	Interface <i>interface-type</i> <i>interface-number</i>	-
Set the maximum number of MAC addresses learned by an Ethernet port	mac-address max-mac-count <i>count</i>	By default, the switch has no limit on the maximum number of MAC addresses learned by a port.
Set the processing policy when the number of MAC addresses learned by a port reaches the threshold value	mac-address max-mac-count enable { alarm forward }*	By default, the switch forwards packets whose source MAC addresses are not learned by the port when the number of MAC addresses learned reaches the threshold value.

Configuring Maximum MAC Address Number Learned by Ethernet Port and Forwarding Option Example

Network requirements

- Set the maximum number of MAC addresses learned by Ethernet port Ethernet3/1/3 to 600
- Set the switch to drop the packets whose source MAC addresses are not learned by the port when the number of MAC addresses learned exceeds 600

Configuration procedure

- 1 Enter system view.

```
<SW8800> system-view
[SW8800]
```

- 2 Enter Ethernet port view.

```
[SW8800] interface ethernet 3/1/3
```

- 3 Set the maximum number of MAC addresses learned by Ethernet port Ethernet3/1/3 to 600.

```
[3Com-Ethernet3/1/3] mac-address max-mac-count 600
```

- 4 Set the switch to drop the packets whose source MAC addresses are not learned by the port when the number of MAC addresses learned exceeds 600.

```
[3Com-Ethernet3/1/3] undo mac-address max-mac-count enable forward
```

Configuring Max Number of MAC Addresses that can be Learned in a VLAN

The MAC address learning function enables Switch 8800 Family series switches to obtain the MAC addresses of the network devices in network segments connected to a VLAN. However, if the MAC address table in a VLAN is too big in size, the forwarding performances of the switch will be decreased.

After setting the maximum number of MAC addresses that can be learned in a VLAN, you can control the number of MAC address entries maintained by the switch. With the maximum number of MAC addresses set, the switch stops learning new MAC addresses when the set maximum number of MAC addresses is reached.

Table 101 Configure the maximum number of MAC addresses that can be learned in a VLAN

Operation	Command	Description
Enter system view	system-view	-
Enter VLAN view	vlan <i>vlan-id</i>	-
Set the maximum number of MAC addresses that can be learned in a VLAN	mac-address max-mac-count <i>max-mac-num</i>	By default, the number of MAC addresses in a VLAN is not limited.



If you execute the **mac-address max-mac-count** *max-mac-num* command with the *max-mac-num* argument specifying a number smaller than the current number of MAC addresses learned, the switch does not remove the existing MAC address entries, neither does it learn new MAC addresses. The switch resumes MAC address learning when the number of MAC addresses learned is less than the value of the *max-mac-num* argument.

Displaying and Debugging MAC Address Tables

After the above configuration, execute the **display** command in any view to display the running of the MAC address table configuration, and to verify the effect of the configuration.

Table 102 Display and debug MAC address tables

Operation	Command
Display the information in the MAC address table	display mac-address [<i>mac-addr</i> [vlan <i>vlan-id</i>]] [static dynamic] [interface <i>interface-type interface-number</i>] [vlan <i>vlan-id</i>] [count]
Display the aging time of dynamic entries in MAC address table	display mac-address aging-time

Resetting MAC Addresses

After configuration, use the **reset mac-address** command in user view to reset the configured mac-address table information.

Table 103 Reset MAC addresses

Operation	Command
Reset mac-address table information	reset mac-address { all dynamic static interface { <i>interface-type interface-number</i> } vlan <i>vlan-id</i> }

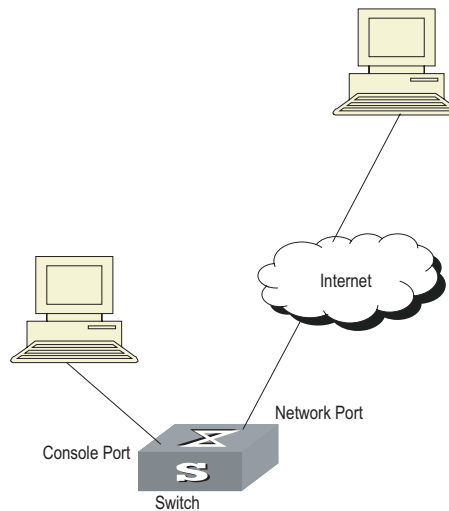
MAC Address Table Management Configuration Example

Network requirements

The user logs into the switch through the Console port to configure the address table management. It is required to set the address aging time to 500s and add a static address 00e0-fc35-dc71 to Ethernet2/1/2 in VLAN1.

Network diagram

Figure 22 Network diagram for address table management configuration



Configuration procedure

Enter the system view of the switch.

```
<SW8800> system-view
```

Add a MAC address (specify the native VLAN, port and state).

```
[SW8800] mac-address static 00e0-fc35-dc71 interface ethernet2/1/2 vlan 1
```

Set the address aging time to 500s.

```
[SW8800] mac-address timer 500
```

Display the MAC address configurations in any view.

```
[SW8800] display mac-address interface ethernet2/1/2
MAC ADDR          VLAN ID    STATE      PORT INDEX  AGING TIME(s)
00-e0-fc-35-dc-71  1          Static    Ethernet2/1/2  NOAGED
00-e0-fc-17-a7-d6  1          Learned   Ethernet2/1/2  500
00-e0-fc-5e-b1-fb  1          Learned   Ethernet2/1/2  500
00-e0-fc-55-f1-16  1          Learned   Ethernet2/1/2  500
--- 4 mac address(es) found on port Ethernet2/1/2 ---
```


17

MSTP REGION-CONFIGURATION

Introduction to MSTP

MSTP stands for Multiple Spanning Tree Protocol, which is compatible with Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

STP is not fast in state transition. Even on a point-to-point link or an edge port, it has to take an interval twice as long as forward delay before the port transits to the forwarding state.

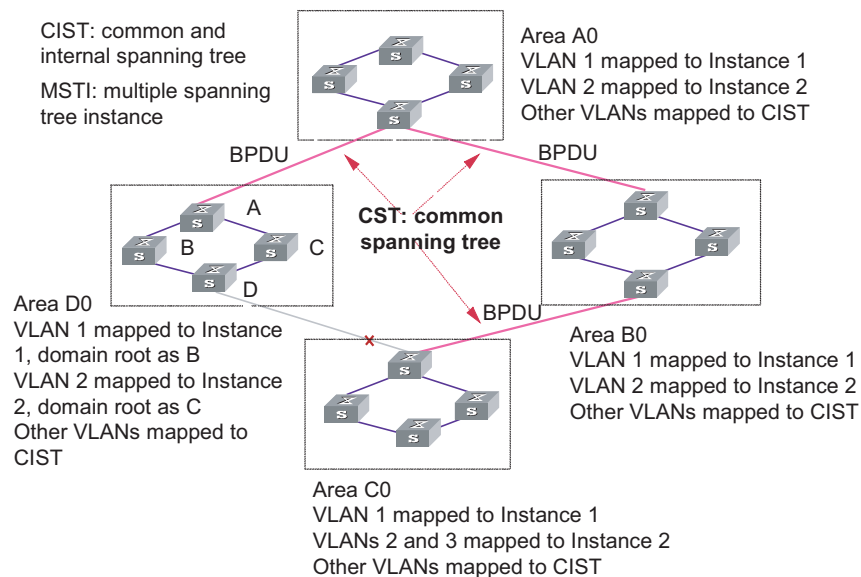
RSTP converges fast, but has the following drawback like STP: all the network bridges in a LAN share one spanning tree and the redundant links cannot be blocked based on VLANs. Packets of all VLANs are forwarded along one spanning tree.

MSTP makes up for the drawback of STP and RSTP. It not only converges fast, but also allows the traffic of different VLANs to be distributed along their respective paths, which provides a better load-balance mechanism for the redundant links.

MSTP keeps a VLAN mapping table to associate VLANs with their spanning trees. Using MSTP, you can divide one switching network into multiple regions, each of which can have multiple spanning trees with each one independent of others. MSTP prunes the ring network into a loopfree tree to avoid the generation of loops and infinite circulations. It also provides multiple redundant paths for data forwarding to implement the load-balance mechanism of the VLAN data.

MSTP Concepts

There are 4 MST regions in Figure 23. Each region consists of four switches, all of which run MSTP. The following introduces the concept of MSTP with the help of this figure.

Figure 23 Basic MSTP concepts

MSTP region

Multiple Spanning Tree Regions: A multiple spanning tree region contains several switches and the network segments between them. These MSTP switches share the same region name, VLAN-spanning tree mapping configuration, and MSTP revision level configuration, and are connected directly. There can be several MSTP regions on a switching network. You can group several switches into a MSTP region, using MSTP configuration commands. For example, in Figure 23, the four switches in MSTP region A0 are configured with the same region name, the same VLAN mapping table (VLAN1 is mapped to instance 1, VLAN 2 is mapped to instance 2, other VLANs is mapped to instance CIST), and the same revision level (not indicated in Figure 23).

VLAN mapping table

The VLAN mapping table is an attribute of MSTP region. It is used for describing the mapping relationship of VLANs and spanning tree instances (STIs). For example, in the VLAN mapping table of MSTP region A0 in Figure 23, VLAN1 is mapped to instance 1, VLAN 2 is mapped to instance 2, other VLANs is mapped to CIST.

In the same region, the mapping relationship of VLANs and STIs must be consistent on all the switches in this region. Otherwise, VLAN and STI are not in the same region.

IST

Internal Spanning Tree (IST): a spanning tree in a MSTP region. The IST and the Common Spanning Tree (CST), together make up a Common and Internal Spanning Tree (CIST) for the entire switching network. The IST in a MSTP region is a fragment of the CIST. For example, every MSTP region in Figure 23 has an IST, which is a fragment of CIST.

CST

Common Spanning Tree (CST): a LAN has only one CST. CST connects the spanning trees of all MST regions. Regard every MST region as a "switch", and the CST is generated by the computing of "switches" through STP/RSTP. For example, the red line in Figure 23 indicates the CST.

CIST

Common and Internal Spanning Tree (CIST): A single spanning tree made up of ISTs and CST. It connects all switches in a switching network. CIST of Figure 23 is composed of ISTs in all MST regions and the CST.

MSTI

Multiple Spanning Tree Instance (MSTI): multiple spanning trees can be generated with MSTP in an MST region and independent of one another. Such a spanning tree is called an MSTI. As shown in Figure 23, every MST region has many STIs. Each STI corresponds to a VLAN and is called a MSTI.

Region root

The region root refers to the root of the IST and MSTI of the MST region. The spanning trees in an MST region have different topologies and their region roots may also be different. For example, the region root of the STI 1 is the switch B and that of the STI 2 is the switch C, as shown in Figure 23.

Common Root Bridge

The Common Root Bridge refers to the root bridge of CIST. For example, the common root bridge is a certain switch in A0, as shown in Figure 23.

Edge port

The edge port refers to the port located at the MST region edge, connecting different MST regions, MST region and STP region, or MST region and RSTP region. For MSTP calculation, the edge port shall take the same role on MSTI and CIST instance. For example, as shown in Figure 23, if a switch in region A0 connects to the first port on a switch in region D0, and the common root bridge of the whole switching network is in A0, then this first port is an edge port of region D0.

Port role

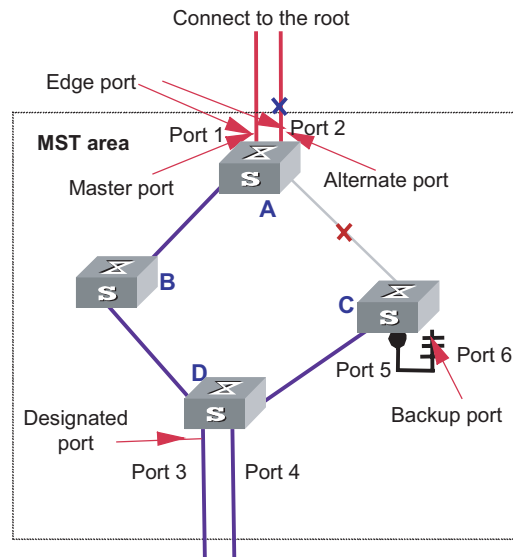
In the process of MSTP calculation, a port can serve as a designated port, root port, master port, alternate port, or backup port.

- The root port is the one through which the data are forwarded to the root.
- The designated port is the one through which the data are forwarded to the downstream network segment or switch.
- Master port is the port connecting the entire region to the Common Root Bridge and located on the shortest path between them.
- An alternate port is a backup of the master port, and also a backup port of a root port in the region. As a backup of the master port, an alternate port will become a new master port after a master port is blocked.
- If two ports of a switch are connected, there must be a loop. In this case, the switch blocks one of them. The blocked one is called a backup port.

A port can play different roles in different spanning tree instances.

The following figure illustrates the earlier-mentioned concepts for your better understanding. In this figure, the switch A, B, C, and D make up a MST region. Port 1 and 2 on switch A connects to the common root bridge; port 5 and 6 on switch C forms a loop; port 3 and 4 on switch D connects to other MST regions in the downstream direction.

Figure 24 Port roles



TC packet

Topology change (TC) means the structure of the MSTP spanning tree changes due to some bridge change or some port change on the network. In versatile routing platform (Comware) implementation, when a port state changes from discarding to forwarding, it means TC occurs.

The following section describes two kinds of STP packets:

1 MSTP BPDU packet

MSTP modules communicate with each other among bridges by MSTP BPDU packets. The following figure shows the MSTP BPDU packet format:

Figure 25 BPDU packet format

	Octet
Protocol Identifier	1–2
Protocol Version Identifier	3
BPDU Type	4
CIST Flags	5
CIST Root Identifier	6–13
CIST External Path Cost	14–17
CIST Regional Root Identifier	18–25
CIST Port Identifier	26–27
Message Age	28–29
Max Age	30–31
Hello Time	32–33
Forward Delay	34–35
Version 1 Length = 0	36
Version 3 Length	37–38
MST Configuration Identifier	39–89
CIST Internal Root Path Cost	90–93
CIST Bridge Identifier	94–101
CIST Remaining Hops	102
MSTI Configuration Messages (may be absent)	103–39 + Version 3 Length

Figure 26 MSTI information format of the last part in BPDU packets

	Octet
MSTI Flags	1
MSTI Regional Root Identifier	2–9
MSTI Internal Root Path Cost	10–13
MSTI Bridge Priority	14
MSTI Port Priority	15
MSTI Remaining Hops	16

Besides field root bridge priority, root path cost, local bridge priority and port priority, the field flags which takes one byte in an instance is also used for role selection. The following figure describes the meaning of its eight bits:

Figure 27 Meaning of 1-byte Flags in BPDU packets

7	6	5	4	3	2	1	0
TcAck	Agreement	Forwarding	Learning			Proposal	Tc

The second and third bits together indicate MSTP port role.

2 TC packet

A TC packet is also an MSTP BPDU packet, but the lowest bit of its flags field is set to 1, which endows the TC packet with special meaning. So the TC packet has its special meaning. After receiving or detecting TC packets, a port will broadcast TC packets to tell the whole network the changed topology information at the fastest speed.

MSTP Principles

MSTP divides the entire Layer 2 network into several MST regions and calculates and generates CST for them. Multiple spanning trees are generated in a region and each of them is called an MSTI. The instance 0 is called IST, and others are called MSTI. Similar to RSTP, MSTP also use configuration messages to calculate and generate spanning trees, the difference is that it is the MSTP configuration information on the switches that is carried in the configuration messages.

CIST calculation

The CIST root is the highest-priority switch elected from the switches on the entire network through comparing their configuration BPDUs. MSTP calculates and generates IST in each MST region; at the same time it regards each MST region as a single "switch" and then calculates and generates the CST between the regions. The CST and ISTs together make up the CIST which connects all the switches in the whole switching network.

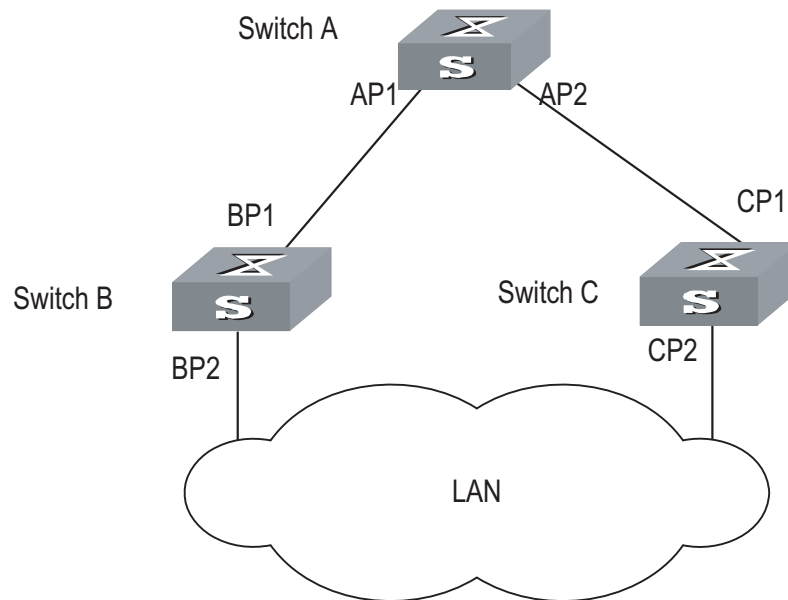
MSTI calculation

Inside an MST region, MSTP generates different MSTIs for different VLANs according to the association between VLAN and the spanning tree. The calculation process of MSTI is like that of RSTP.

The following introduces the calculation process of one MSTI.

The fundamental of STP is that the switches exchange a special kind of protocol packet (which is called configuration Bridge Protocol Data Units, or BPDU, in IEEE 802.1D) to decide the topology of the network. The configuration BPDU contains the information enough to ensure the switches to compute the spanning tree.

Figure 28 shows the Designated bridge and designated port.

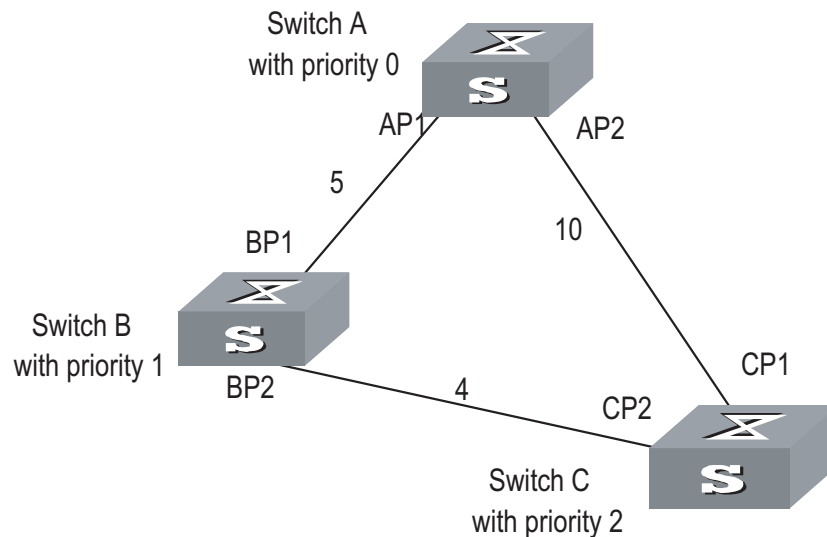
Figure 28 Designated bridge and designated port

For a switch, the designated bridge is a switch in charge of forwarding BPDU to the local switch via a port called the designated port accordingly. For a LAN, the designated bridge is a switch that is in charge of forwarding BPDU to the network segment via a port called the designated port accordingly. As illustrated in the Figure 28, Switch A forwards data to Switch B via the port AP1. To Switch B, the designated bridge is Switch A and the designated port is AP1. In the figure, Switch B and Switch C are connected to the LAN and Switch B forwards BPDU to LAN. So the designated bridge of LAN is Switch B and the designated port is BP2.

- The specific calculation process of STP algorithm.

The following example illustrates the calculation process of STP.

Figure 29 illustrates the practical network.

Figure 29 Ethernet switch networking

To facilitate the descriptions, only the first four parts of the configuration BPDU are described in the example. They are root ID (expressed as Ethernet switch priority), path cost to the root, designated bridge ID (expressed as Ethernet switch priority) and the designated port ID (expressed as the port number). As illustrated Figure 29, the priorities of Switch A, B and C are 0, 1 and 2 and the path costs of their links are 5, 10 and 4 respectively.

1 Initial state

When initialized, each port of the switches generates the configuration BPDU taking itself as the root with a root path cost as 0, designated bridge IDs as their own switch IDs and the designated ports as their ports.

Switch A:

Configuration BPDU of AP1: {0, 0, 0, AP1}

Configuration BPDU of AP2: {0, 0, 0, AP2}

Switch B:

Configuration BPDU of BP1: {1, 0, 1, BP1}

Configuration BPDU of BP2: {1, 0, 1, BP2}

Switch C:

Configuration BPDU of CP2: {2, 0, 2, CP2}

Configuration BPDU of CP1: {2, 0, 2, CP1}

2 Select the optimum configuration BPDU

Every switch transmits its configuration BPDU to others. When a port receives a configuration BPDU with a lower priority than that of its own, the switch discards

the message and keep the local BPDU unchanged. When the port receives a higher-priority configuration BPDU, the switch uses the content in the received configuration BPDU to change the content of the local BPDU of this port. Then the switch compares the configuration BPDU of this port to those of other ports on it to elect the optimum configuration BPDU.

The comparison rules are:

- The configuration BPDU with a smaller root ID has a higher priority.
- If the root IDs are the same, perform the comparison based on root path costs. The cost comparison is as follows: the path cost to the root recorded in the configuration BPDU plus the corresponding path cost of the local port is set as S , the configuration BPDU with a smaller S has a higher priority.
- If the costs of path to the root are also the same, compare in sequence the designated bridge ID, designated port ID and the ID of the port via which the configuration BPDU was received.

For the convenience of expression, this example supposes that the optimum configuration BPDU can be elected just by the comparison of root IDs.

- 3 Determine the root and designated ports, and update the configuration BPDU of designated ports.

The port receiving the optimum configuration BPDU is designated to be the root port, whose configuration BPDU remains unchanged. Switch calculates a designated port BPDU for every port: substituting the root ID with the root ID in the configuration BPDU of the root port, the cost of path to root with the value made by the root path cost plus the path cost corresponding to the root port, the designated bridge ID with the local switch ID and the designated port ID with the local port ID.

Switch compares the calculated BPDU with the BPDU of corresponding port. If the BPDU of corresponding port is better, the port is blocked, and the BPDU of the port remains unchanged. The port will not forward data and only receive but not send BPDU. If the calculated BPDU is better, the port will be the designated port, and the port BPDU will be modified by the calculated BPDU and sent out regularly.

The comparison process of each switch is as follows.

Switch A:

AP1 receives the configuration BPDU from Switch B and finds out that the local configuration BPDU priority is higher than that of the received one, so it discards the received configuration BPDU. The configuration BPDU is processed on the AP2 in a similar way. Thus Switch A finds itself the root and designated bridge in the configuration BPDU of every port. It regards itself as the root, retains the configuration BPDU of each port and transmits configuration BPDU to others regularly thereafter. By now, the configuration BPDUs of the two ports are as follows:

Configuration BPDU of AP1: {0, 0, 0, AP1}.

Configuration BPDU of AP2: {0, 0, 0, AP2}.

Switch B:

BP1 receives the configuration BPDU from Switch A and finds that the received BPDU has a higher priority than the local one, so it updates its configuration BPDU.

BP2 receives the configuration BPDU from Switch C and finds that the local BPDU priority is higher than that of the received one, so it discards the received BPDU.

By now, the configuration BPDUs of each port are as follows: Configuration BPDU of BP1: {0, 0, 0, AP1}, Configuration BPDU of BP2: {1, 0, 1, BP2}.

Switch B compares the configuration BPDUs of the ports and selects the BP1 BPDU as the optimum one because the current configuration BPDU {0, 5, 0, AP1} of BP1 has a higher priority than the configuration BPDU {1, 0, 1, BP2} of BP2. Thus BP1 is elected as the root port and the configuration BPDUs of Switch B ports are updated as follows.

The configuration BPDU of the root port BP1 retains as {0, 5, 0, AP1}. BP2 updates root ID with that in the optimum configuration BPDU, the path cost to root with 5, sets the designated bridge as the local switch ID and the designated port ID as the local port ID. Thus, the configuration BPDU becomes {0, 5, 1, BP2}.

Then, all the designated ports of Switch B transmit the configuration BPDUs regularly.

Switch C:

CP2 receives from the BP2 of Switch B the configuration BPDU {1, 0, 1, BP2} that has not been updated and then the updating process is launched. The configuration BPDU is updated as {1, 0, 1, BP2}.

CP1 receives the configuration BPDU {0, 0, 0, AP2} from Switch A and Switch C launches the updating. The configuration BPDU is updated as {0, 0, 0, AP2}.

Now, the configuration BPDU of CP1 is {0, 10, 0, AP2}, which has a higher priority than that of CP2. By comparison, CP1 configuration BPDU is elected as the optimum one. The CP1 is thus specified as the root port without modifying its configuration BPDU. However, CP2 will be blocked and its BPDU also remains unchanged, but it will not receive the data (excluding the STP packets) forwarded from Switch B until spanning tree calculation is launched again by some new events. For example, the link from Switch B to Switch C is down or the port receives any better configuration BPDU.

CP2 will receive the updated configuration BPDU, {0, 5, 1, BP2}, from Switch B. Since this configuration BPDU is better than the old one, the old BPDU will be updated to {0, 5, 1, BP2}.

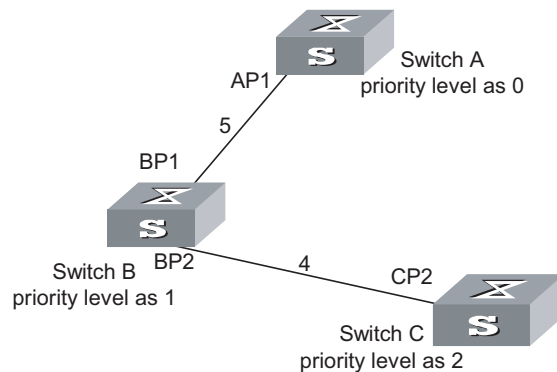
Meanwhile, CP1 receives the configuration BPDU from Switch A but its configuration BPDU is not updated and retain {0, 10, 0, AP2}.

By comparison, {0, 9, 1, BP2}, the configuration BPDU of CP2, is elected as the optimum one. Thus, CP2 is elected as the root port, whose BPDU will not change, while CP1 is blocked, its BPDU is retained, and will not receive the data forwarded from Switch A until spanning tree calculation is triggered again by some changes.

For example, the link from Switch B to Switch C is down or the port receives any better configuration BPDU

Thus, the spanning tree is stabilized. The tree with the root bridge A is illustrated in the Figure 30.

Figure 30 The final stabilized spanning tree



To facilitate the descriptions, the description of the example is simplified. For example, the root ID and the Designated bridge ID in actual calculation should comprise both switch priority and switch MAC address. Designated port ID should comprise port priority and port ID. In the updating process of a configuration BPDU, other configuration BPDUs besides the first four items will make modifications according to certain rules. The basic calculation process is described below:

In addition, with identical priority, the path cost of an aggregation port is smaller than that of a non-aggregation port. Therefore, under identical root ID, path cost value and designated switch ID, the switch will generally select the aggregation port as the root port.

- Configuration BPDU forwarding mechanism in STP:

Upon the initiation of the network, all the switches regard themselves as the roots. The designated ports send the configuration BPDUs of local ports at a regular interval of HelloTime. If it is the root port that receives the configuration BPDU, the switch will enable a timer to time the configuration BPDU as well as increase MessageAge carried in the configuration BPDU by certain rules. If a path goes wrong, the root port on this path will not receive configuration BPDUs any more and the old configuration BPDUs will be discarded due to timeout. Hence, recalculation of the spanning tree will be initiated to generate a new path to replace the failed one and thus restore the network connectivity.

However, the new configuration BPDU as now recalculated will not be propagated throughout the network right away, so the old root ports and designated ports that have not detected the topology change will still forward the data through the old path. If the new root port and designated port begin to forward data immediately after they are elected, an occasional loop may still occur. In STP, a transitional state mechanism is thus adopted to ensure the new configuration BPDU has been propagated throughout the network before the root port and

designated port begin to send data again. That is, the root port and designated port should undergo a transitional state for a period of Forward Delay before they enter the forwarding state.

And thus, the packets of a VLAN will be forwarded along the following path: in the MST region, the packets will be forwarded along the corresponding MSTI; among the regions, the packets will be forwarded along the CST.

MSTP Implementation on the Switch

MSTP is compatible with STP and RSTP. The MSTP switch can recognize both the STP and RSTP packets and calculate the spanning tree with them. Besides the basic MSTP functions, 3Com Ethernet Switch Series also provide some features easy to manage from users' point of view. These features include root bridge hold, secondary root bridge, ROOT protection, BPDU protection, loop protection, hot swapping of the interface modules, master/slave switchover, and so on. Note that the spanning tree needs to be calculated again when a master/slave switchover occurs.

Configuring MSTP

MSTP configuration includes:

- "Configuring the MST Region for a Switch"
- "Specifying the Switch as a Primary or a Secondary Root bridge"
- "Configuring the MSTP Running Mode"
- "Configuring the Bridge Priority for a Switch"
- "Configuring the Max Hops in an MST Region"
- "Configuring the Switching Network Diameter"
- "Configuring the Time Parameters of a Switch"
- "Setting the Timeout Factor of a Specific Bridge"
- "Configuring the Max Transmission Speed on a Port"
- "Configuring a Port as an Edge Port or Non-edge Port"
- "Configuring the Path Cost of a Port"
- "Configuring the Priority of a Port"
- "Configuring the Port (Not) to Connect with the Point-to-Point Link"
- "Configuring the mCheck Variable of a Port"
- "Configuring the Switch Protection Function"
- "Enabling/Disabling MSTP on the Device"
- "Enabling/Disabling MSTP on a Port"
- "Configuring the mapping relationship between a VLAN list and a Spanning Tree Instance"

Only after MSTP is enabled on the device will other configurations take effect. Before enabling MSTP, you can configure the related parameters of the device and Ethernet ports, which will take effect upon enabling MSTP and stay effective even after resetting MSTP. The **check region-configuration** command can display the region parameters that have not yet taken effect. The **display current-configuration** command shows the parameters configured before MSTP is enabled. For those configured after MSTP is enabled, you can use the related

display commands. For detailed information, refer to the "Display and Debug MSTP" section.



When GVRP and MSTP start on the switch simultaneously, GVRP packets will propagate along CIST which is a spanning tree instance. In this case, if you want to issue a certain VLAN through GVRP on the network, you should make sure that the VLAN is mapped to CIST when configuring the VLAN mapping table of MSTP.

CIST is spanning tree instance 0.

Configuring the MST Region for a Switch

Which MST region a switch belongs to is determined with the configurations of the region name, VLAN mapping table, and MSTP revision level. You can perform the following configurations to put a switch into an MST region.

Entering MST region view

Perform the following configuration in system view.

Table 104 Enter MST region view

Operation	Command
Enter MST region view (from system view)	stp region-configuration
Restore the default settings of MST region	undo stp region-configuration

Configuring parameters for the MST region

Perform the following configuration in MST region view.

Table 105 Configure the MST region for a switch

Operation	Command
Configure the MST region name	region-name <i>name</i>
Restore the default MST region name	undo region-name
Configure VLAN mapping table	instance <i>instance-id</i> vlan <i>vlan-list</i>
Restore the default VLAN mapping table	undo instance <i>instance-id</i> [vlan <i>vlan-list</i>]
Configure the MSTP revision level of MST region	revision-level <i>level</i>
Restore the MSTP revision level of MST region	undo revision-level

An MST region can contain up to 49 spanning tree instances, among which the Instance 0 is IST and the Instances 1 through 48 are MSTIs. Upon the completion of the above configurations, the current switch is put into a specified MST region. Note that two switches belong to the same MST region only if they have been configured with the same MST region name, STI-VLAN mapping tables of an MST region, and the same MST region revision level.

Configuring the related parameters, especially the VLAN mapping table, of the MST region, will lead to the recalculation of spanning tree and network topology flapping. To bate such flapping, MSTP triggers to recalculate the spanning tree according to the configurations only if one of the following conditions is met:

- A user manually activates the configured parameters related to the MST region, using the **active region-configuration** command.
- A user enables MSTP using the **stp enable** command.

By default, the MST region name is the switch MAC address, all the VLANs in the MST region are mapped to the STI 0, and the MSTP region revision level is 0. You can restore the default settings of MST region, using the **undo stp region-configuration** command in system view.

Configuring the mapping relationship between a VLAN list and a Spanning Tree Instance

MSTP describes the mapping relationship between VLAN and Spanning Tree instances through the VLAN mapping table. You can use this command to configure the VLAN mapping table: each VLAN can be allocated to different Spanning Tree instances according to your configuration.

You cannot map one VLAN to different instances. When you map a mapped VLAN to a different MSTI, the previous mapping relationship will be automatically cancelled.

The **vlan-mapping modulo** *modulo* command can specify a VLAN to each Spanning Tree instance quickly. This command maps a VLAN to the Spanning Tree instance whose ID is (VLAN ID-1) %*modulo*+1. (Note: (VLAN ID-1) %*modulo* is the modulo operation for (VLAN ID-1). If the modulo operation is based on 16, VLAN 1 is mapped to MSTI 1, VLAN 2 is mapped to MSTI 2...VLAN 16 is mapped to MSTI 16, VLAN 17 is mapped to VLAN 17, and so on.)

Perform the following configurations in MST region view.

Table 106 Map all the VLAN lists to the specific Spanning Tree instances

Operation	Command
Map all the VLAN lists to the specific Spanning Tree instances uniformly through the modulo operation	vlan-mapping modulo <i>modulo</i>
Restore the default mapping relationship between VLAN lists and Spanning Tree instances	undo vlan-mapping modulo

By default, all the VLAN lists are mapped to CIST, namely, Instance 0.

Activating the MST region configuration, and exit the MST region view

Perform the following configuration in MST region view.

Table 107 Activate the MST region configuration and exit the MST region view

Operation	Command
Show the configuration information of the MST region under revision	check region-configuration
Manually activate the MST region configuration	active region-configuration
Exit MST region view	quit

Specifying the Switch as a Primary or a Secondary Root bridge

MSTP can determine the spanning tree root through calculation. You can also specify the current switch as the root, using the command provided by the switch.

You can use the following commands to specify the current switch as the primary or secondary root of the spanning tree.

Perform the following configuration in system view.

Table 108 Specify the switch as a primary or a secondary root bridge

Operation	Command
Specify the current switch as the primary root bridge of the specified spanning tree	stp [instance <i>instance-id</i>] root primary [bridge-diameter <i>bridgenum</i>] [hello-time <i>centi-seconds</i>]
Specify the current switch as the secondary root bridge of the specified spanning tree	stp [instance <i>instance-id</i>] root secondary [bridge-diameter <i>bridgenum</i>] [hello-time <i>centi-seconds</i>]
Specify current switch not to be the primary or secondary root	undo stp [instance <i>instance-id</i>] root

After a switch is configured as the primary root bridge or the secondary root bridge, users cannot modify the bridge priority of the switch.

You can configure the current switch as the primary or secondary root bridge of the STI (specified by the **instance** *instance-id* parameter). If the *instance-id* takes 0, the current switch is specified as the primary or secondary root bridge of the CIST.

The root types of a switch in different STIs are independent of one another. The switch can be a primary or secondary root of any STI. However, it cannot serve as both the primary and secondary roots of one STI.

If the primary root is down or powered off, the secondary root will take its place, unless you configure a new primary root. Of two or more configured secondary root bridges, MSTP selects the one with the smallest MAC address to take the place of the failed primary root.

When configuring the primary and secondary switches, you can also configure the network diameter and hello time of the specified switching network. For detailed information, refer to the configuration tasks "Configure switching network diameter" and "Configure the Hello Time of the switch".



You can configure the current switch as the root of several STIs. However, it is not necessary to specify two or more roots for an STI. In other words, do not specify the root for an STI on two or more switches.

You can configure more than one secondary root for a spanning tree through specifying the secondary STI root on two or more switches.

Generally, you are recommended to designate one primary root and more than one secondary root for a spanning tree.

By default, a switch is neither the primary root nor the secondary root of the spanning tree.

Configuring the MSTP Running Mode

MSTP and RSTP are compatible and they can recognize the packets of each other. However, STP cannot recognize MSTP packets. To implement the compatibility, MSTP provides two operation modes, STP-compatible mode and MSTP mode. In STP-compatible mode, the switch sends STP packets via every port. In MSTP mode,

the switch ports send MSTP or STP packets (when connected to the STP switch) and the switch provides multiple spanning tree function.

You can use the following command to configure MSTP running mode. MSTP can intercommunicate with STP. If there is a STP switch in the switching network, you may use the command to configure the current MSTP to run in STP-compatible mode. Otherwise, configure it to run in MSTP mode.

Perform the following configuration in system view.

Table 109 Configure the MSTP running mode

Operation	Command
Configure MSTP to run in STP-compatible mode	stp mode stp
Configure MSTP to run in MSTP mode	stp mode mstp
Restore the default MSTP running mode	undo stp mode

Generally, if there is a STP switch on the switching network, the port connected to it will automatically transit from MSTP mode to STP-compatible mode. But the port cannot automatically transit back to MSTP mode after the STP switch is removed. In this case, you can execute the **stp mcheck** command to restore the MSTP mode.

By default, the switch runs in MSTP mode.

Configuring the Bridge Priority for a Switch

Whether a switch can be elected as the spanning tree root depends on its Bridge priority. The switch configured with a smaller Bridge priority is more likely to become the root. An MSTP switch may have different priorities in different STIs.

You can use the following command to configure the Bridge priorities of the Designated bridge in different STIs.

Perform the following configuration in system view.

Table 110 Configure the Bridge priority for a switch

Operation	Command
Configure the Bridge priority of the Designated bridge	stp [instance <i>instance-id</i>] priority <i>priority</i>
Restore the default Bridge priority of the Designated bridge	undo stp [instance <i>instance-id</i>] priority

When configuring the switch priority with the **instance *instance-id*** parameter as 0, you are configuring the CIST priority of the switch.



CAUTION: *In the process of spanning tree root election, of two or more switches with the same Bridge priorities, the one has a smaller MAC address is elected as the root.*

By default, the switch Bridge priority is 32768.

Configuring the Max Hops in an MST Region

The scale of MST region is limited by the max hops in an MST region, which is configured on the region root. As the BPDU travels from the spanning tree root,

each time when it is forwarded by a switch, the max hops is reduced by 1. The switch discards the configuration BPDU with 0 hops left. This makes it impossible for the switch beyond the max hops to take part in the spanning tree calculation, thereby limiting the scale of the MST region.

You can use the following command to configure the max hops in an MST region.

Perform the following configuration in system view.

Table 111 Configure the max hops in an MST region

Operation	Command
Configure the max hops in an MST region	stp max-hops <i>hop</i>
Restore the default max hops in an MST region	undo stp max-hops

The more the hops in an MST region, the larger the scale of the region. Only the max hops configured on the region root can limit the scale of MST region. Other switches in the MST region also apply the configurations on the region root, even if they have been configured with max hops.

By default, the max hop of an MST is 20.

Configuring the Switching Network Diameter

Any two hosts on the switching network are connected with a specific path carried by a series of switches. Among these paths, the one passing more switches than all others is the network diameter, expressed as the number of passed switches.

You can use the following command to configure the diameter of the switching network.

Perform the following configuration in system view.

Table 112 Configure the switching network diameter

Operation	Command
Configure the switching network diameter	stp bridge-diameter <i>bridgenum</i>
Restore the default switching network diameter	undo stp bridge-diameter

The network diameter is the parameter specifying the network scale. The larger the diameter is, the larger the scale of the network is.

When a user configures the network diameter on a switch, MSTP automatically calculates and sets the Hello Time, Forward-Delay and Max Age time of the switch to the desirable values.

Setting the network diameter takes effect on CIST only, but has no effect on MSTI.

By default, the network diameter is 7 and the three corresponding timers take the default values.



The **stp bridge-diameter** command configures the switching network diameter and determines the three MSTP time parameters (Hello Time, Forward Delay, and Max Age) accordingly.

Configuring the Time Parameters of a Switch

The switch has three time parameters, Forward Delay, Hello Time, and Max Age.

Forward Delay is the switch state transition mechanism. The spanning tree will be recalculated upon link faults and its structure will change accordingly. However, the configuration BPDU recalculated cannot be immediately propagated throughout the network. The temporary loops may occur if the new root port and designated port forward data right after being elected. Therefore the protocol adopts a state transition mechanism. It takes a Forward Delay interval for the root port and designated port to transit from the learning state to forwarding state. The Forward Delay guarantees a period of time during which the new configuration BPDU can be propagated throughout the network.

The switch sends Hello packet periodically at an interval specified by Hello Time to check if there is any link fault.

Max Age specifies when the configuration BPDU will expire. The switch will discard the expired configuration BPDU.

You can use the following command to configure the time parameters for the switch.

Perform the following configuration in system view.

Table 113 Configure the time parameters of a switch

Operation	Command
Configure Forward Delay on the switch	stp timer forward-delay <i>centi-seconds</i>
Restore the default Forward Delay of the switch	undo stp timer forward-delay
Configure Hello Time on the switch	stp timer hello <i>centi-seconds</i>
Restore the default Hello Time on the switch	undo stp timer hello
Configure Max Age on the switch	stp timer max-age <i>centi-seconds</i>
Restore the default Max Age on the switch	undo stp timer max-age

Every switch on the switching network adopts the values of the time parameters configured on the root bridge of the CIST.



CAUTION: *The Forward Delay configured on a switch depends on the switching network diameter. Generally, the Forward Delay is supposed to be longer when the network diameter is longer. Note that too short a Forward Delay may redistribute some redundant routes temporarily, while too long a Forward Delay may prolong the network connection resuming. The default value is recommended.*

A suitable Hello Time ensures the switch to detect the link fault on the network but occupy moderate network resources. The default value is recommended. If you set too long a Hello Time, when there is packet dropped over a link, the switch may consider it as a link fault and the network device will recalculate the spanning tree accordingly. However, for too short a Hello Time, the switch frequently sends configuration BPDU, which adds its burden and wastes the network resources.

Too short a Max Age may cause the network device frequently calculate the spanning tree and mistake the congestion as a link fault. However, if the Max Age is too long, the network device may not be able to discover the link fault and recalculate the spanning tree in time, which will weaken the auto-adaptation capacity of the network. The default value is recommended.

To avoid frequent network flapping, the values of Hello Time, Forward Delay and Max Age should guarantee the following formulas.

$$2 \times (\text{Forward-Delay} - 1 \text{ second}) \geq \text{Max Age}$$

$$\text{Max Age} \geq 2 \times (\text{Hello Time} + 1 \text{ second})$$

You are recommended to use the **stp bridge-diameter** command to specify the network diameter and Hello Time of the switching network, and then MSTP will automatically calculate and give the rather desirable values.

By default, Forward Delay is 15 seconds, Hello Time is 2 seconds, and Max Age is 20 seconds.

Setting the Timeout Factor of a Specific Bridge

A switch transmits hello packet regularly to the adjacent bridges to check if there is link failure. Generally, if the switch does not receive the STP packets from the upstream switch for 3 times of hello time, the switch will decide the upstream switch is dead and will recalculate the topology of the network. Then, in a steady network, the recalculation may be caused when the upstream is busy. In this case, user can redefine the timeout interval to a longer time to avoid this kind of meaningless recalculation.

You can use the following command to set the multiple value of hello time of a specified bridge.

Perform the following configurations in system view.

Table 114 Setting the timeout factor of a specific switch

Operation	Command
Set the timeout factor of a specified switch	stp timer-factor <i>number</i>
Restore the default timeout factor	undo stp timer-factor

It is recommended to set 5, 6 or 7 as the timeout factor in the steady network.

By default, the timeout factor of the switch is 3.

Configuring the Max Transmission Speed on a Port

The max transmission speed on a port specifies how many MSTP packets will be transmitted via the port every Hello Time.

The max transmission speed on a port is limited by the physical state of the port and the network structure. You can configure it according to the network conditions.

You can configure the max transmission speed on a port in the following ways.

Configuration in system view

Perform the following configuration in system view.

Table 115 Configure the max transmission speed on a port

Operation	Command
Configure the max transmission speed on a port	stp interface <i>interface-list</i> transmit-limit <i>packetnum</i>
Restore the default max transmission speed on a port	undo stp interface <i>interface-list</i> transmit-limit

Configuration in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 116 Configure the max transmission speed on a port

Operation	Command
Configure the max transmission speed on a port	stp transmit-limit <i>packetnum</i>
Restore the default max transmission speed on a port	undo stp transmit-limit

You can configure the max transmission speed on a port with either of the earlier-mentioned measures. For more about the commands, refer to the *Command Manual*.

This parameter only takes a relative value without units. If it is set too large, too many packets will be transmitted during every Hello Time and too many network resources will be occupied. The default value is recommended.

By default, the max transmission speed on every Ethernet port of the switch is 3.

Configuring a Port as an Edge Port or Non-edge Port

An edge port refers to the port not directly connected to any switch or indirectly connected to a switch over the connected network.

You can configure a port as an edge port or non-edge port in the following ways.

Configuration in system view

Perform the following configuration in system view.

Table 117 Configure a port as an edge port or a non-edge port

Operation	Command
Configure a port as an edge port	stp interface <i>interface-list</i> edged-port enable
Configure a port as a non-edge port	stp interface <i>interface-list</i> edged-port disable
Restore the default setting of the port as a non-edge port	undo stp interface <i>interface-list</i> edged-port

Configuration in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 118 Configure a port as an edge port or a non-edge port

Operation	Command
Configure a port as an edge port	stp edged-port enable
Configure a port as a non-edge port	stp edged-port disable
Restore the default setting of the port as a non-edge port	undo stp edged-port

You can configure a port as an edge port or a non-edge port with either of the earlier-mentioned measures.

After configured as an edge port, the port can fast transit from blocking state to forwarding state without any delay. You can only set the port connecting with the terminal as an edge port. The configuration of this parameter takes effect on all the STIs. In other words, if a port is configured as an edge port or non-edge port, it is configured the same on all the STIs.

If BPDU protection is enabled on the switch, the edged port is disabled when it receives BPDU packets from the user. Only the network administrators can enable the port.

By default, all the Ethernet ports of the switch have been configured as non-edge ports.



It is better to configure the port directly connected with the terminal as an edge port, and enable the BPDU function on the port. That is, to realize fast state-transition and prevent the switch from being attacked.



CAUTION: *If STP has been enabled on the equipment connected to the switch, do not configure the edged ports on the equipment. Otherwise the system will fail to delete MAC address entries and ARP address entries on the port.*

Configuring the Path Cost of a Port

Path Cost is related to the speed of the link connected to the port. On the MSTP switch, a port can be configured with different path costs for different STIs. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing.

You can configure the path cost of a port in the following ways.

Configuration in system view

Perform the following configuration in system view.

Table 119 Configure the path cost of a port

Operation	Command
Configure the path cost of a port	stp interface <i>interface-list</i> [instance <i>instance-id</i>] cost <i>cost</i>
Restore the default path cost of a port	undo stp interface <i>interface-list</i> [instance <i>instance-id</i>] cost

Configuration in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 120 Configure the path cost of a port

Operation	Command
Configure the path cost of a port	stp [instance <i>instance-id</i>] cost <i>cost</i>
Restore the default path cost of a port	undo stp [instance <i>instance-id</i>] cost

You can configure the path cost of a port with either of the earlier-mentioned measures. Upon the change of path cost of a port, MSTP will recalculate the port role and transit the state. When *instance-id* takes 0, it indicates to set the path cost on the CIST.

By default, MSTP is responsible for calculating the path cost of a port.

STP Path Cost Calculation Standards on STP port

The 3Com Switch 8800 Family Series Routing Switches support 3Com's legacy path cost calculation. DOT1T calculation and DOT1D-1998 calculation can also be used. By default, legacy standard is applied for Switch 8800 Family series.

The port rate must be obtained first before calculating the path cost of a port as the path cost is associated with the port rate. The three standards use their own way to work out the port rate, based on which each standard calculates the path cost of the by certain algorithm.

DOT1T calculation standard

- 1 Calculating the rate
 - Aggregation port

The rate of either a primary or a secondary port in an aggregation port group is the sum of the port rates in the group. If a port is down, the rate is 0.

- Non-aggregation port

The actual rate counts.

- 2 Calculating the path cost
 - Full-duplex and non-aggregation port at a rate less than 1 GE

Path cost = $[200,000,000 / (\text{rate} \times 10)] - 1$

- Other ports

Path cost = $200,000,000 / (\text{rate} \times 10)$

DOT1D-1998 calculation standard

- 1 Calculating the rate
 - Aggregation port

If the port is up, the actual rate counts. If the port is down, the rate is determined by that of the port which goes up first in the aggregation group. If all the ports in the aggregation group are down, the rate of the aggregation port is 0.

- Non-aggregation port

The actual rate counts.

2 Calculating the path cost

Table 121 details the correspondence between the rate range and the path cost values of the ports.

Table 121 Correspondence between the rate range and the PATH cost values

Rate range	PATH cost value
	99 (for full-duplex port)
[0, 10]	95 (for aggregation port) 100 (default)
(10, 100]	18 (for full-duplex port) 15 (for aggregation port) 19 (default)
(100,1000]	3 (for aggregation port) 4 (default)
(1000,10000]	1 (for aggregation port) 2 (default)
> 10000	1

3Com's legacy calculation standard

1 Calculating the rate

- Aggregation port

The rate of the primary port in an aggregation group is determined by the sum of the port rates in this group. No calculation is performed for secondary port.

- Non-aggregation port

The actual rate counts, but the rate is 0 if the port is down.

2 Calculating the path cost

Table 122 details the correspondence between the rate range and the value range of the path cost of the ports.

Table 122 Correspondence between the rate range and PATH cost range

Rate range	PATH cost range
[0, 100]	2200 to (20 × rate)
(100,1000]	220 to the integer of [(0.2 × rate)]
(1000,10000]	22 to the integer of [(0.002 × rate)]
> 10000	1

You can specify the intended standard by using the following commands.

Perform the following configuration in system view.

Table 123 Specifying the standard to be followed in path cost calculation

Operation	Command
Specify the standard to be adopted when the switch calculates the default path cost for the connected link	stp pathcost-standard { dot1d-1998 dot1t legacy }
Restore the default standard to be used	undo stp pathcost-standard

By default, the switch calculates the default path cost of a port by the legacy standard.

Configuring the Priority of a Port

For spanning tree calculation, the port priority is an importance factor to determine if a port can be elected as the root port. With other things being equal, the port with the highest priority will be elected as the root port. On the MSTP switch, a port can have different priorities in different STIs and plays different roles respectively. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing.

You can configure the port priority in the following ways.

Configuration in system view

Perform the following configuration in system view.

Table 124 Configure the port priority

Operation	Command
Configure the port priority	stp interface <i>interface-list</i> instance <i>instance-id</i> port priority <i>priority</i>
Restore the default port priority	undo stp interface <i>interface-list</i> instance <i>instance-id</i> port priority

Configuration in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 125 Configure the port priority

Operation	Command
Configure the port priority	stp [instance <i>instance-id</i>] port priority <i>priority</i>
Restore the default port priority	undo stp [instance <i>instance-id</i>] port priority

You can configure the port priority with either of the earlier-mentioned measures. Upon the change of port priority, MSTP will recalculate the port role and transit the state. Generally, a smaller value represents a higher priority. If all the Ethernet ports of a switch are configured with the same priority value, the priorities of the ports will be differentiated by the index number. The change of Ethernet port priority will lead to spanning tree recalculation. You can configure the port priority according to actual networking requirements.

By default, the priority of all the Ethernet ports is 128.

Configuring the Port (Not) to Connect with the Point-to-Point Link

The point-to-point link directly connects two switches.

You can configure the port (not) to connect with the point-to-point link in the following ways.

Configuration in system view

Perform the following configuration in system view.

Table 126 Configure the port (not) to connect with the point-to-point link

Operation	Command
Configure the port to connect with the point-to-point link	stp interface <i>interface-list</i> point-to-point force-true
Configure the port not to connect with the point-to-point link	stp interface <i>interface-list</i> point-to-point force-false
Configure MSTP to automatically detect if the port is directly connected with the point-to-point link	stp interface <i>interface-list</i> point-to-point auto
Configure MSTP to automatically detect if the port is directly connected with the point-to-point link, as defaulted	undo stp interface <i>interface-list</i> point-to-point

Configuration in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 127 Configure the port (not) to connect with the point-to-point link

Operation	Command
Configure the port to connect with the point-to-point link	stp point-to-point force-true
Configure the port not to connect with the point-to-point link	stp point-to-point force-false
Configure MSTP to automatically detect if the port is directly connected with the point-to-point link	stp point-to-point auto
Configure MSTP to automatically detect if the port is directly connected with the point-to-point link, as defaulted	undo stp point-to-point

You can configure the port (not) to connect with the point-to-point link with either of the earlier-mentioned measures. For the ports connected with the point-to-point link, upon some port role conditions met, they can transit to forwarding state fast through transmitting synchronization packet, thereby reducing the unnecessary forwarding delay. If the parameter is configured as auto mode, MSTP will automatically detect if the current Ethernet port is connected with the point-to-point link.



For a link aggregation, only the master port can be configured to connect with the point-to-point link. If a port in auto-negotiation mode operates in full-duplex mode upon negotiation, it can be configured to connect with the point-to-point link.

This configuration takes effect on the CIST and all the MSTIs. The settings of a port whether to connect the point-to-point link will be applied to all the STIs to which the port belongs. Note that a temporary loop may be redistributed if you configure a port that is not physically connected with the point-to-point link as connected to such a link by force.

By default, the parameter is configured as **auto**.

Configuring the mCheck Variable of a Port

The port of an MSTP switch operates in either STP-compatible or MSTP mode.

Suppose a port of an MSTP switch on a switching network is connected to an STP switch, the port will automatically transit to operate in STP-compatible mode. However, the port stays in STP-compatible mode and cannot automatically transit back to MSTP mode when the STP switch is removed. In this case, you can perform mCheck operation to transit the port to MSTP mode by force.

You can use the following measure to perform mCheck operation on a port.

Configuration in system view

Perform the following configuration in system view.

Table 128 Configure the mCheck variable of a port

Operation	Command
Perform mCheck operation on a port	stp interface <i>interface-list</i> mcheck



*By default, MSTP runs in MSTP mode, which is compatible with RSTP and STP (This mode can recognize MSTP BPDU, STP config BPDU and RSTP config BPDU). However, the STP switch can only recognize config BPDU (STP BPDU) sent by the STP and RSTP bridges. After the switch running STP-compatible mode switches back to MSTP mode, it will not send MSTP BPDU if you do not execute the **stp mcheck** command. Therefore, the connected device still sends config BPDU (STP BPDU) to it, causing the same configuration exists in different regions and other problems. Remember to perform **stp interface mcheck** after modifying stp mode.*

Configuration in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 129 Configure the mCheck variable of a port

Operation	Command
Perform mCheck operation on a port	stp mcheck

You can configure mCheck variable on a port with either of the earlier-mentioned measures. Note that the command can be used only if the switch runs MSTP. The command does not make any sense when the switch runs in STP-compatible mode.

Configuring the Function of Clearing Dynamic ARP Entries

Perform the following configuration in Ethernet port view or system view.

Table 130 Configure the function of clearing dynamic ARP entries

Operation	Command
Enable the function of clearing dynamic ARP entries on the switch or on a port	stp reset-arp enable
Disable the function of clearing dynamic ARP entries on the switch or on a port	stp reset-arp disable
Enable the root protection function (system view)	stp interface <i>interface-list</i> root-protection



If you enable the function of clearing dynamic ARP entries in system view, the function takes effect on all ports of the system. If you enable the function of

clearing dynamic ARP entries in port view, the function takes effect only on the specified port.

Configuring the Switch Protection Function

An MSTP switch provides BPDU protection, Root protection functions, loop protection and TC-protection.

BPDU protection

For an access device, the access port is generally directly connected to the user terminal (for example, PC) or a file server, and the access port is set to an edge port to implement fast transition. When such a port receives BPDU packet, the system will automatically set it as a non-edge port and recalculate the spanning tree, which causes the network topology flapping. In normal cases, these ports will not receive STP BPDU. If someone forges BPDU to attack the switch, the network will flap. BPDU protection function is used against such network attacks.

Root protection

The primary and secondary root bridges of the spanning tree, especially those of ICST, shall be located in the same region. It is because the primary and secondary roots of CIST are generally placed in the core region with a high bandwidth in network design. In case of configuration error or malicious attack, the legal primary root may receive the BPDU with a higher priority and then lose its place, which causes network topology change errors. Due to the illegal change, the traffic supposed to travel over the high-speed link may be pulled to the low-speed link and congestion will occur on the network. Root protection function is used against such problems.

Loop protection

The root port and other blocked ports maintain their states according to the BPDUs sent by uplink switch. Once the link is blocked or has trouble, then the ports cannot receive BPDUs and the switch will select root port again. In this case, the downstream switch selects the port role again. The downstream bridge port that cannot receive BPDUs becomes specific port and the blocked port is transferred to the forwarding state. As a result, a link loop is generated. The loop protection function can prohibit such loop.



For the loop protection-enabled port, when the loop protection takes effect because the port cannot receive the BPDU sent by the upstream switches, if the port participates in STP calculation, all the instances of the port will be always set to be in discarding state regardless of the port role.

TC-protection

As a general rule, the switch deletes the corresponding entries in the MAC address table and ARP table upon receiving TC-BPDU packets. Under malicious attacks of TC-BPDU packets, the switch shall receive a great number of TC-BPDU packets in a very short period. Too frequent delete operations shall consume huge switch resources and bring great risk to network stability.

When the protection from TC-BPDU packet attack is enabled, the switch just perform one delete operation in a specified period (generally, 15 seconds) after receiving TC-BPDU packets, as well as monitoring whether it receives TC-BPDU packets during this period. Even if it detects a TC-BPDU packet is received in a period shorter than the specified interval, the switch shall not run the delete

operation till the specified interval is reached. This can avoid frequent delete operations on the MAC address table and ARP table.

You can use the following command to configure the protection functions of the switch.

Perform the following configuration in corresponding configuration modes.

Table 131 Configure the switch protection function

Operation	Command
Configure BPDU protection of the switch (from system view)	stp bpdu-protection
Restore the disabled BPDU protection state as defaulted (from system view)	undo stp bpdu-protection
Configure Root protection of the switch (from system view)	stp interface <i>interface-list</i> root-protection
Restore the disabled Root protection state as defaulted (from system view)	undo stp interface <i>interface-list</i> root-protection
Configure Root protection of the switch (from Ethernet port view)	stp root-protection
Restore the disabled Root protection state as defaulted (from Ethernet port view)	undo stp root-protection
Configure loop protection function of the switch (from Ethernet port view)	stp loop-protection
Restore the disabled loop protection state, as defaulted (from Ethernet port view)	stp loop-protection
Enable the loop protection function of the switch (from system view)	stp interface <i>interface-list</i> loop-protection
Restore the disabled loop protection state, as defaulted (from system view)	undo stp interface <i>interface-list</i> loop-protection
Configure TC protection of the switch (from system view)	stp tc-protection enable
Disable TC protection (from system view)	stp tc-protection disable



CAUTION: If the equipment connected to the port of the switch cannot send STP packets to the switch, do not configure the **loop-protection** command. Otherwise, the port may be congested for a long time.



CAUTION: For a port that fails to receive the BPDU packets from the opposite peer, there are several situations:

- If you are not sure that STP is enabled on the opposite peer, it is not recommended to carry out the **stp loop-protection** command on this port.
- If the port is a root port or an alternate port, you can carry out the **stp loop-protection** command.
- The port is a designated port on a domain border and the **stp loop-protection** command is carried out on this port. If the number of instances on this port is greater than that on the opposite peer port, the port state on another instance and the port state on instance 0 are the same.
- Carry out the **stp loop-protection** command on the designated upstream port. If the downstream port does not contain the VLAN of the designated

upstream port, some instances of the upstream port will be congested for a long time.

By default, only the protection from TC-BPDU packet attack is enabled on the switch. BPDU protection, Root protection and loop protection are disabled.

After configured with BPDU protection, the switch will disable the edge port through MSTP which receives a BPDU, and notify the network manager at same time. These ports can be resumed by the network manager only.

The port configured with Root protection only plays a role of designated port on every instance. Whenever such port receives a higher-priority BPDU, that is, it is about to turn into non-designated port, it will be set to listening state and not forward packets any more (as if the link to the port is disconnected). If the port has not received any higher-priority BPDU for a certain period of time thereafter, it will resume the normal state.

For one port, only one configuration can be effective among loop protection, Root protection and Edge port configuration at the same moment.



The port configured with loop protection can only turn into discarding state on every instance. That such a port receives no configuration message for a long time indicates that it is about to change its state and role. Only the port role changes but the port discarding state remains unchanged, and no packets are forwarded. In this way, if the peer end cannot send BPDU packets due to error operation, and the port enters forwarding state directly for not receiving configuration message for a long time, no loop will be generated by enabling the loop protection.

Enabling/Disabling MSTP on the Device

You can use the following command to enable MSTP on the device.

Perform the following configuration in system view.

Table 132 Enable/Disable MSTP on a device

Operation	Command
Enable MSTP on a device	stp enable
Disable MSTP on a device	stp disable
Restore the disable state of MSTP, as defaulted	undo stp

Only if MSTP has been enabled on the device will other MSTP configurations take effect. If MSTP is disabled on the device, MSTP cannot be enabled on a port.

By default, MSTP is disabled.



CAUTION: *The MSTP function and the loop detection function are mutually exclusive. Before enabling the MSTP function, you must judge whether the system is detecting loops. If yes, you cannot enable the MSTP function.*

Enabling/Disabling MSTP on a Port

You can use the following command to enable/disable MSTP on a port. You may disable MSTP on some Ethernet ports of a switch to spare them from spanning tree calculation. This is a measure to flexibly control MSTP operation and save the CPU resources of the switch.

MSTP can be enabled/disabled on a port through the following ways.

Configuration in system view

Perform the following configuration in system view.

Table 133 Enable/Disable MSTP on a port

Operation	Command
Enable MSTP on a port	stp interface <i>interface-list</i> enable
Disable MSTP on a port	stp interface <i>interface-list</i> disable

Configuration in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 134 Enable/Disable MSTP on a port

Operation	Command
Enable MSTP on a port	stp enable
Disable MSTP on a port	stp disable

You can enable/disable MSTP on a port with either of the earlier-mentioned measures. Note that redundant route may be generated after MSTP is disabled.

By default, MSTP is enabled on all the ports after it is enabled on the device.

Disabling BPDU Packets from Flooding in the Default VLANs

If STP (spanning tree protocol) is not enabled, or if STP is disabled on a port though it is enabled globally, the BPDU packets through the STP-disabled port will be broadcast in the default VLAN, and these BPDU packets will affect the STP operation on other ports. The **stp non-flooding** command can discard the BPDU packets entering the STP-disabled port of the interface card, and thus prohibiting the BPDU packets from being broadcast in the VLAN.

Table 135 Disable BPDU packets from being broadcast on the default VLANs

Operation	Command	Description
Enter system view	system-view	-
Disable BPDU packets from being broadcast on STP-disabled ports	stp non-flooding [slot slotnum]	By default, BPDU packets are broadcast on STP-disabled ports.



CAUTION: *It is recommended that after enabling STP, you disable the broadcasting function of BPDU to prevent the BPDU packets, which are received by ports that did not participate in the generation of spanning trees, from being forwarded to other ports, (which can cause errors during STP generations). Avoid using this function on VPLS-enabled I/O Modules so that STP packets can be forwarded in the VPLS network transparently*

Displaying and Debugging MSTP

After the above configuration, execute the **display** command in any view to display the running of the MSTP configuration, and to verify the effect of the configuration. Execute the **reset stp** [**interface** *interface-list*] command in user view to clear the statistics of MSTP module. Execute the **debugging** command in user view to debug the MSTP module

Table 136 Display and debug MSTP

Operation	Command
Display the MSTP information about the current switch	display stp
Display the configuration information about the current port and the switch	display stp [instance <i>instance-id</i>] [interface <i>interface-list</i> slot <i>slot-num</i>] [brief]
Display the current configurations of the specified service module	display stp slot <i>number</i> [brief]
Display the configuration information about the region	display stp region-configuration
Display TC statistics	display stp [instance <i>instanceid</i>] tc { all detected received sent }
Clear the MSTP statistics information	reset stp [interface <i>interface-list</i>]
Enable event debugging of MSTP for a specified port	debugging stp [interface <i>interface-list</i>] { lacp-key packet event }
Disable debugging of MSTP for a specified port	undo debugging stp [interface <i>interface-list</i>] { packet event }
Enable event debugging of MSTP	debugging stp event
Disable event debugging of MSTP	undo debugging stp event
Enable packet debugging of MSTP	debugging stp packet
Disable packet debugging of MSTP	undo debugging stp packet
Enable global debugging	debugging stp all
Disable global debugging	undo debugging stp all
Enable instance debugging of MSTP	debugging stp instance <i>instance-id</i>
Disable instance debugging of MSTP	undo debugging stp instance <i>instance-id</i>
Enable STP global error or event debugging	debugging stp { global-error global-event }
Disable STP global error or event debugging	undo debugging stp { global-error global-event }
Enable MD5 summary debugging of Lacp protocol	debugging stp lacp-key
Disable MD5 summary debugging of Lacp protocol	undo debugging stp lacp-key
Enable debugging of the state machine	debugging stp state-machine
Disable debugging of the state machine	undo debugging stp state-machine
Enable debugging of the port information state machine	debugging stp state-machine pim
Disable debugging of the port information state machine	undo debugging stp state-machine pim
Enable debugging of the state machine for port role selection	debugging stp state-machine prs
Disable debugging of the state machine for port role selection	undo debugging stp state-machine prs
Enable debugging of the state machine for port role transition	debugging stp state-machine prt
Disable debugging of the state machine for port role transition	undo debugging stp state-machine prt
Enable debugging of the state machine for port state transition	debugging stp state-machine pst

Table 136 Display and debug MSTP

Operation	Command
Enable debugging of the state machine for port state transition	undo debugging stp state-machine pst
Enable debugging of the topology change state machine	debugging stp state-machine tcm
Disable debugging of the topology change state machine	undo debugging stp state-machine tcm
Enable debugging of the state machine for port protocol transition	debugging stp state-machine ppm
Disable debugging of the state machine for port protocol transition	undo debugging stp state-machine ppm
Enable debugging of the port transport state machine	debugging stp state-machine ptx
Disable debugging of the port transport state machine	undo debugging stp state-machine ptx
Enable debugging of the state machine for topology change protection	debugging stp state-machine tcpm
Disable debugging of the state machine for topology change protection	undo debugging stp state-machine tcpm

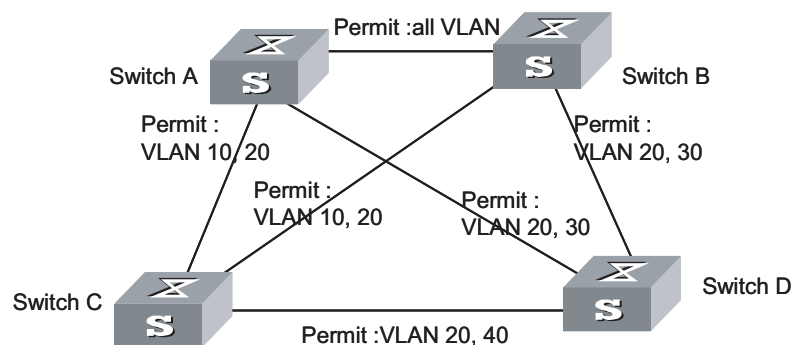
Typical MSTP Configuration Example

Network requirements

MSTP provides different forwarding paths for packets of different VLANs. The configurations are as follows: all the switches in the network belong to the same MST region, packets of VLAN 10 travels along instance 1, packets of VLAN 30 travels along instance 3, packets of VLAN 40 travels along instance 4, and that of VLAN 20 travels along instance 0.

In the following network diagram, Switch A and Switch B are devices of the convergence layer, Switch C and Switch D are devices of the access layer. VLAN 10 and 30 function at the distribution and access layers, and VLAN 40 functions at the access layer only. So the root of instance 1 can be configured as Switch A, root of instance 3 can be Switch B, and root of instance 4 can be Switch C.

Network diagram

Figure 31 Network diagram for MSTP configuration

The explanations on the above figure which goes like "permit: XXXX" means that packets of these VLANs are permitted to pass.

Configuration procedure**1** Configurations on Switch A

```
# MST region
```

```
<SW8800> system-view
[SW8800] stp region-configuration
[3Com-mst-region] region-name example
[3Com-mst-region] instance 1 vlan 10
[3Com-mst-region] instance 3 vlan 30
[3Com-mst-region] instance 4 vlan 40
[3Com-mst-region] revision-level 0
```

```
# Manually activate MST region configuration.
```

```
[3Com-mst-region] active region-configuration
```

```
# Specify Switch A as the root of instance 1
```

```
[SW8800] stp instance 1 root primary
```

2 Configurations on Switch B

```
# MST region.
```

```
[SW8800] stp region-configuration
[3Com-mst-region] region-name example
[3Com-mst-region] instance 1 vlan 10
[3Com-mst-region] instance 3 vlan 30
[3Com-mst-region] instance 4 vlan 40
[3Com-mst-region] revision-level 0
```

```
# Manually activate MST region configuration.
```

```
[3Com-mst-region] active region-configuration
```

```
# Specify Switch B as the root of instance 3
```

```
[SW8800] stp instance 3 root primary
```

3 Configurations on Switch C

```
# MST region.
```

```
[SW8800] stp region-configuration
[3Com-mst-region] region-name example
[3Com-mst-region] instance 1 vlan 10
[3Com-mst-region] instance 3 vlan 30
[3Com-mst-region] instance 4 vlan 40
[3Com-mst-region] revision-level 0
```

```
# Manually activate MST region configuration.
```

```
[3Com-mst-region] active region-configuration
```

```
# Specify Switch C as the root of instance 4.
```

```
[SW8800] stp instance 4 root primary
```

4 Configurations on Switch D

MST region

```
[SW8800] stp region-configuration
[3Com-mst-region] region-name example
[3Com-mst-region] instance 1 vlan 10
[3Com-mst-region] instance 3 vlan 30
[3Com-mst-region] instance 4 vlan 40
[3Com-mst-region] revision-level 0
```

Manually activate MST region configuration.

```
[3Com-mst-region] active region-configuration
```

18

DIGEST SNOOPING CONFIGURATION

Introduction to Digest Snooping

According to IEEE 802.1s, two connected switches can communicate with each other through multiple spanning tree instances (MSTIs) in a multiple spanning tree protocol (MSTP) region only when they are configured with the same region settings. With MSTP employed, interconnected switches determine whether or not they are in the same region by checking the configuration IDs of the bridge protocol data units (BPDUs) between them. (A configuration ID comprises information such as region ID, configuration digest.)

As switches of some manufacturers come with some proprietary protocols concerning spanning trees employed, a switch of this type cannot communicate with other switches in an MSTP region even if it is configured with the same MSTP region settings as other switches in the MSTP region.

This kind of problems can be overcome by implementing digest snooping. Digest snooping enables a switch to track and maintain configuration digests of other switches that are in the same region and come from other manufacturers by examining their BPDUs. It also enables the switch to insert corresponding configuration digests in its BPDUs destined for these switches. In this way, switches of different manufacturers are capable of communicating with each other in an MSTP region.

Note that:

- 1 When implementing digest snooping in an MSTP region, make sure that the region configurations of the switches of different manufacturers are exactly the same to prevent possible broadcast storm caused by otherwise inconsistent mapping relationships between VLANs and VPN instances of each switch.
- 2 If you want to change the configuration of a region with one or multiple of its switches being digest snooping-enabled, be sure to disable digest snooping on these switches first to prevent possible broadcast storm caused by otherwise inconsistent mapping relationships between VLANs and VPN instances of each switch.
- 3 A digest snooping-enabled switch always keeps the latest configuration digests it receives. A configuration digest remains valid even if the corresponding port goes down.

Digest Snooping Configuration

Configure digest snooping on a switch to enable it to communicate in MSTP regions through MSTI with other switches that are configured with some proprietary protocols to calculate configuration digest.

Prerequisites Switches of different manufacturers are interconnected in a network and have MSTP employed. The network operates properly.

Configuration Procedure

Table 137 Configure digest snooping

Configuration step	Command	Description
Enter system view	system-view	-
Enter Ethernet interface view	interface <i>interface-type</i> <i>interface-number</i>	<i>interface-type</i> : Interface type <i>interface-number</i> : Interface number
Enable digest snooping on the port	stp config-digest-snooping	Required. Digest snooping is disabled by default on the port.
Quit Ethernet interface view	quit	-
Enable digest snooping globally	stp config-digest-snooping	Required. Digest snooping is disabled by default.
Display current configuration information	display current-configuration	This command can be executed in any view.



- You must enable digest snooping on a port first before enabling it globally.
- Digest snooping is unnecessary if the interconnected switches are from the same manufacturer.
- To enable digest snooping, the interconnected switches must be configured with the same settings.
- To enable digest snooping, all ports in an MSTP region connecting to switches from other manufacturers must have digest snooping enabled.
- Do not enable digest snooping on border ports of an MSTP region.

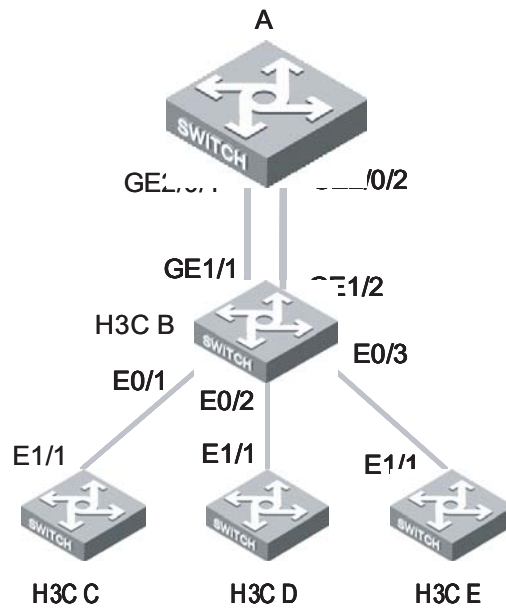
Digest Snooping Configuration Example

Network requirements

All switches in Figure 32 are MSTP-enabled and have the same region configuration. All the switches except that A are of 3Com Technology Co., Ltd.

Network diagram

Figure 32 Network diagram for digest snooping configuration



Configuration procedure

3Com B is directly connected to A through GE 1/1 and GE 1/2 ports. Enable digest snooping on these two ports by executing the following command:

```

<SW8800>system-view
System View: return to User View with Ctrl+Z.
[3ComB]interface GigabitEthernet1/1
[3ComB-GigabitEthernet1/1]stp config-digest-snooping
[3ComB-GigabitEthernet1/1] quit
[3ComB]interface GigabitEthernet1/2
[3ComB-GigabitEthernet1/2]stp config-digest-snooping
  
```

Finally, you need to enable digest snooping globally on 3Com B.

```
[3ComB]stp config-digest-snooping
```

After the above configuration, all the switches in the MSTP region can communicate with each other through MSTI.

19

FAST TRANSITION

Introduction

The designated port fast transition mechanism of RSTP and MSTP uses two types of protocol packets:

- proposal packet: Requests for fast transition.
- agreement packet: Permits the opposite end to perform fast state transition.

RSTP and MSTP request that a designated port of the upstream switch can perform fast transition after receiving the agreement packet from the downstream switch. RSTP and MSTP are different in the following:

- For MSTP, the upstream switch sends the agreement packet to the downstream switch first. After receiving the agreement packet, the downstream switch sends the agreement packet to the upstream switch.
- For RSTP, the upstream switch does not send the agreement packet to the downstream switch.

Figure 33 and Figure 34 show the designated port fast transition mechanisms of RSTP and MSTP.

Figure 33 Designated port fast transition mechanism of RSTP

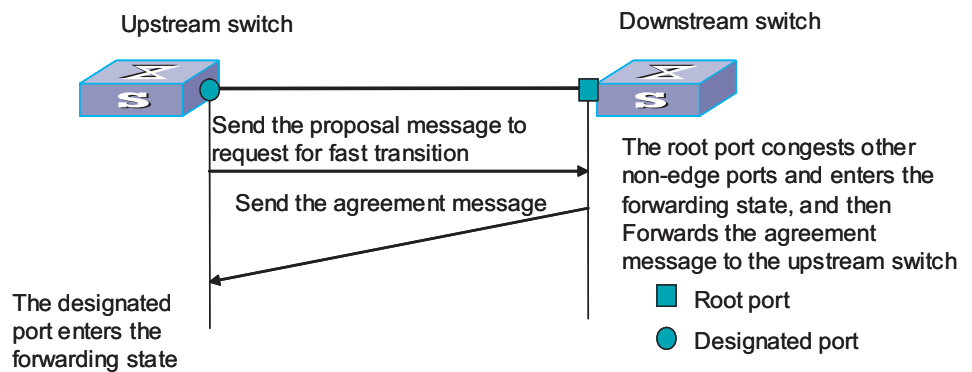
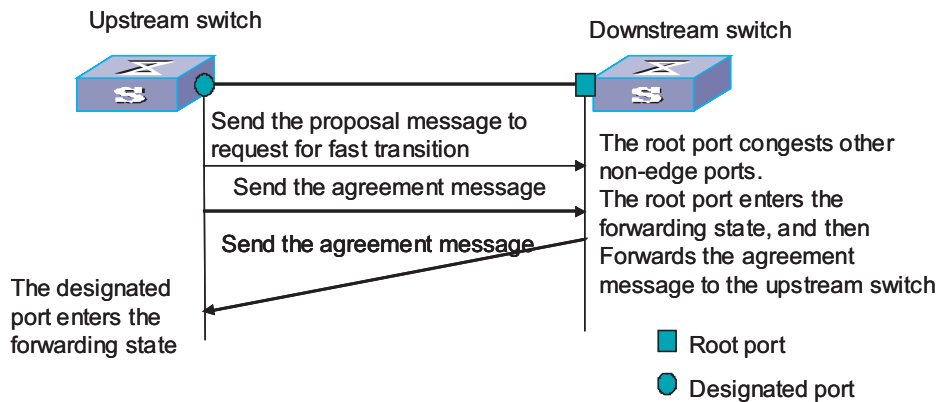


Figure 34 Designated port fast transition mechanism of MSTP

There is a certain limit on fast transition cooperation of RSTP and MSTP. For example, the upstream switch runs RSTP and the downstream switch runs MSTP, and the downstream MSTP does not support the compatible RSTP mode. As the root port of the downstream MSTP-enabled switch cannot receive the agreement packet from the upstream switch, the downstream switch does not send the agreement packet to the upstream switch. As a result, the designated port of the upstream switch cannot implement fast transition. Instead, the state becomes forwarding state after double forward delay.

In practice, since private protocols related to STP are configured on the switch of another vendor and the designated port state transition mechanism is similar to that of RSTP, the designated ports cannot implement fast state transition when these switches serving as upstream switches interconnect with the Switch 8800 Family series routing switch that runs MSTP.

To avoid such problem, Switch 8800 Family series routing switches provide fast transition. When the Switch 8800 Family series routing switch interconnects with the switches from another vendor, you can enable fast transition on the port of the S5800 switch that serves as the downstream switch. If this port is a root port, after receiving the proposal packet from the designated port of the upstream switch, the port sends the agreement packet to the upstream switch initiatively rather than sends the agreement packet after receiving the agreement packet. As a result, the upstream switch can perform fast state transition on the designated port.

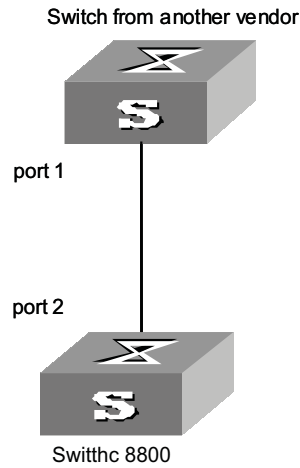
Configuring Fast transition

Configuration Preparation

The Switch 8800 Family series routing switch serves as the downstream switch and the switch from another vendor serves as the upstream switch. They have been connected correctly, as shown in Figure 35.

A private protocol related to STP is enabled on the upstream switch. The designated port state transition mechanism is similar to that of RSTP. Port 1 is a designated port.

MSTP is enabled on the downstream Switch 8800 Family switch. Port 2 is a designated port.

Figure 35 Network diagram

Configuration Tasks **Configuring fast transition in system view**

Table 138 Configure fast transition in system view

Operation	Command	Description
Enter system view	system-view	-
Enable fast transition	stp interface <i>interface-type</i> <i>interface-number</i> no-agreement-check	Required By default, port fast transition is disabled.

Configuring fast transition in Ethernet port view

Table 139 Configure fast transition in Ethernet port view

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable fast transition	stp no-agreement-check	Required By default, port fast transition is disabled.



You can configure fast transition only on a root port or an alternate port.

20

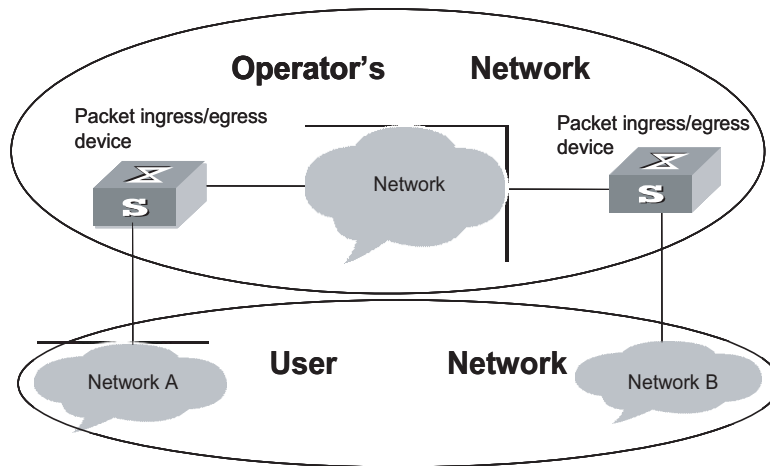
BPDU TUNNEL CONFIGURATION

BPDU Tunnel Overview

BPDU Tunnel enables geographically segmented user networks to transmit BPDU packets transparently over the specified VLAN VPN on the operator's network. This allows the user network to participate in a uniform spanning tree calculation while maintaining a separate spanning tree from the operator network.

As shown in Figure 36, the operator's network comprises packet ingress/egress devices, and the user network has networks A and B. On the operator's network, you can configure to convert the MAC addresses of the arriving BPDU packets to a special format at the ingress, and then reconvert them at the egress. This is how transparent transmission is implemented on the operator's network.

Figure 36 BPDU Tunnel implementation



Configuring BPDU Tunnel

The following table describes the BPDU Tunnel configuration tasks.

Table 140 Configure BPDU Tunnel

Operation	Command	Description
Enter system view	system-view	-
Enable BPDU TUNNEL function of the system	vlan-vpn tunnel	Configure BPDU TUNNEL function, required
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable VLAN VPN function on the Ethernet port	vlan-vpn enable	Enable VLAN VPN function on the Ethernet port, required

Enabling/disabling BPDU Tunnel

Perform the following configuration in system view.

Table 141 Enable/disable BPDU Tunnel in system view

Operation	Command
Enable BPDU Tunnel	vlan-vpn tunnel
Disable BPDU Tunnel	undo vlan-vpn tunnel

By default, BPDU Tunnel is disabled.

Enabling/disabling VLAN VPN on Ethernet port

Perform the following configuration in Ethernet port view.

Table 142 Enable/disable VLAN VPN in Ethernet port view

Operation	Command
Enable VLAN VPN	vlan-vpn enable
Disable VLAN VPN	undo vlan-vpn

By default, the VLAN VPN is disabled on all the ports.

VLAN VPN is not compatible with STP, DOT1X, GVRP, and NTDP.



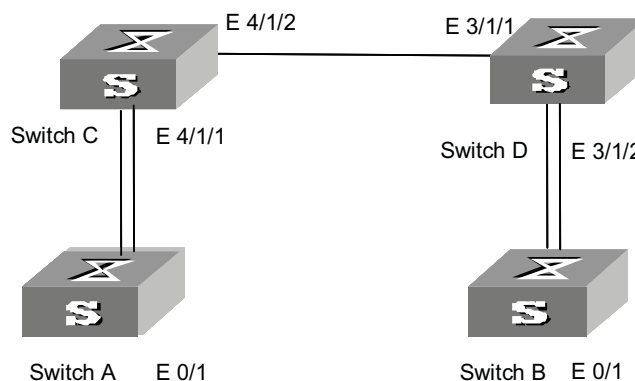
In Ethernet port view, VLAN VPN and STP are not compatible with each other and cannot function at the same time.

BPDU Tunnel Configuration Example

Network requirements

- The Switch 8800 Family Series Routing Switches are used as the access devices of the operator's network, that is, Switch C and Switch D in the following figure.
- The Switch 5500 Series Ethernet Switches are used as the access devices of the user network, that is, Switch A and Switch B in the following figure.
- Switch C and Switch D connect to each other through trunk port, enabling the BPDU Tunnel function in system view, and implementing the transparent transmission between user network and operator's network. VLAN 20 is assigned to the user network.

Network diagram

Figure 37 Network diagram for BPDU Tunnel configuration

Configuration procedure**1** Configure Switch A

Enable rapid spanning tree protocol (RSTP) on the device.

```
[Switch_A] stp enable
```

Set the port Ethernet 0/1 as a trunk port and configure it to permit VLAN 10 to pass through.

```
[Switch_A] vlan 10
[Switch_A-Ethernet 0/1] port link-type trunk
[Switch_A-Ethernet 0/1] port trunk permit vlan 10
```

2 Configure Switch B

Enable RSTP on the device.

```
[Switch_B] stp enable
```

Set the port Ethernet 0/1 as a trunk port and configure it to permit VLAN 10 to pass through.

```
[Switch_B] vlan 10
[Switch_B-Ethernet 0/1] port link-type trunk
[Switch_B-Ethernet 0/1] port trunk permit vlan 10
```

3 Configure Switch C

Enable multiple STP (MSTP) on the device.

```
[Switch_C] stp enable
```

Enable BPDU Tunnel on the device.

```
[Switch_C] vlan-vpn tunnel
```

Add the port Ethernet 4/1/1 into VLAN 20.

```
[Switch_C] vlan 20
[Switch_C-Vlan 20] port Ethernet 4/1/1
```

First disable STP and then enable VLAN VPN on the port Ethernet 4/1/1.

```
[Switch_C] interface Ethernet 4/1/1
[Switch_C-Ethernet4/1/1] stp disable
[Switch_C-Ethernet4/1/1] vlan-vpn enable
```

Set the port Ethernet 4/1/2 as a trunk port.

```
[Switch_C-Ethernet4/1/2] port link-type trunk
```

Add the trunk port into all the VLANs.

```
[Switch_C-Ethernet4/1/2] port trunk permit vlan all
```

4 Configure Switch D

```

# Enable MSTP on the device.

[Switch_D] stp enable

# Enable BPDU Tunnel on the device.

[Switch_D] vlan-vpn tunnel

# Add the port Ethernet 3/1/2 into VLAN 20.

[Switch_D] vlan 20
[Switch_D- Vlan 20 ]port Ethernet 3/1/2

# First disable the STP protocol and then enable VLAN VPN on the port Ethernet
3/1/2.

[Switch_D] interface Ethernet 3/1/2
[Switch_D-Ethernet3/1/2] stp disable
[Switch_D-Ethernet3/1/2] vlan-vpn enable

# Switch_D the port Ethernet 3/1/1 as a trunk port.

[3Com-Ethernet3/1/1] port link-type trunk

# Add the trunk port into all the VLANs.

[Switch_D-Ethernet3/1/1] port trunk permit vlan all
[Switch_D-Ethernet3/1/1] port trunk permit vlan all

# Add Ethernet3/1/3 into VLAN20.

[Switch_D] vlan 20
[Switch_D- Vlan 20] port Ethernet 3/1/3

# Disable STP Protocol on Ethernet3/1/3 and enable VLAN-VPN.

[Switch_D] interface Ethernet3/1/3
[Switch_D-Ethernet3/1/3] stp disable
[Switch_D-Ethernet3/1/3] vlan-vpn enable

```

**CAUTION:**

- The STP protocol must be enabled on those devices that have enabled BPDU TUNNEL; otherwise after BPDUs of the client network enter the switch, they will not be processed by the CPU, so their MAC addresses cannot be replaced, that is to say, they cannot be transparently transported.
- The port that has enabled VLAN-VPN must be configured as the access port; the intermediate operator network must be configured as trunk link;
- BPDU TUNNEL cannot be configured on ports that have enabled DOT1X, GVRP, GMRP, STP and NTDP protocols.

21

ACL CONFIGURATION

ACL Overview

Introduction to ACL A series match rules must be configured to recognize the packets before they are filtered. Only when packets are identified, can the network take corresponding actions, allowing or prohibiting them to pass, according to the preset policies. Access control list (ACL) is targeted to achieve these functions.

ACLs classify packets using a series of matching rules, which can be source addresses, destination addresses and port IDs. ACLs can be used globally on the switch or just at a port, through which the switch determines whether to forward or drop the packets.

The matching rules defined in ACLs can also be imported to differentiate traffic in other situations, for example, defining traffic classification rules in QoS.

An ACL rule can include many rules, which may be defined for packets within different address ranges. Matching order is involved in matching an ACL.

ACLs being activated directly on hardware

ACLs can be delivered to hardware for traffic filtering and classification.

The cases when ACLs are sent directly to hardware include: referencing ACLs to provide for QoS functions, filtering and forwarding packets with ACLs.

ACLs being referenced by upper-level modules

ACLs may also be used to filter and classify packets processed by software. Then you can define matching order for the rules in an ACL. Two matching modes are available in this case: **config** (user-defined order) and **auto** (depth first by the system). You cannot modify the matching order once you define it for an ACL rule, unless you delete the rule and redefine the matching order.

The cases when ACLs are referenced by upper-level modules include referencing ACLs to achieve routing policies, and using ACLs to control register users and so on.



*Depth first principle means putting the statement with smaller packet range in the front. You can know the packet range by comparing IP address wildcards: The smaller the wildcard is, the smaller host range is. For example, the address 129.102.1.1 0.0.0.0 specifies the host 129.102.1.1 and address 129.102.1.1 0.0.255.255 specifies the segment 129.102.1.1 to 129.102.255.255. Then 129.102.1.1 is surely put in the front. Specifically, for the statements of basic ACL rules, directly compare the wildcards of source addresses and follow **config** order if the wildcards are equal; for the ACL rules used in port packet filtering, the rules*

configured with **any** are put to the end and other rules follow **config** order; for advanced ACL rules, first compare the wildcards of source addresses, then the wildcards of destination addresses if those of source addresses are equal, then the port IDs if the wildcards of destination addresses are still equal. Follow **config** order if port IDs are also equal.



The user-defined ACL matching order takes effect only when multiple rules of one ACL are applied at the same time. For example, an ACL has two rules. If the two rules are not applied simultaneously, even if you configure the matching order to be depth first, the switch still matches them according to their application order.

If one rule is a subset of another rule in an ACL, it is recommended to apply the rules according to the range of the specified packets. The rule with the smallest range of the specified data packets is applied first, and then other rules are applied based on this principle.

ACLs Supported The switch supports these types of ACLs:

- Number-based basic ACLs
- Name-based basic ACLs
- Number-based advanced ACLs
- Name-based advanced ACLs
- Number-based Layer 2 ACLs
- Name-based Layer 2 ACLs

The requirements for the various ACLs available on the switch are listed in the following table.

Table 143 Requirements for defining ACLs

Item	Number range	Maximum number
Number-based basic ACL	2000 to 2999	1000
Number-based advanced ACL	3000 to 3999	1000
Number-based Layer 2 ACL	4000 to 4999	1000
Name-based basic ACL	-	-
Name-based advanced ACL	-	-
Name-based Layer 2 ACL	-	-
Maximum rules for an ACL	0 to 127	128
Maximum rules for the system	-	12288

Table 144 Max ACL rules that can be activated on different interface cards

Interface card suffix	MPLS support	Max number of ACL rules supported for each card/interface
B		
DA		
DB	MPLS not supported	1024
DC		

Table 144 Max ACL rules that can be activated on different interface cards

Interface card suffix	MPLS support	Max number of ACL rules supported for each card/interface
3C17511		
3C17512		
3C17513		
3C17514		
3C17516	MPLS not supported	1024
3C17526		
3C17532		
3C17532		
3C17525	MPLS supported	1023
3C17527		
3C17530		
3C17531		

A maximum of 12288 ACL rules can be activated on the whole service processor card.

ACL Configuration Tasks

The following table describes the ACL configuration tasks for interface cards.

Table 145 ACL configuration tasks on interface cards

Item	Command	Description
Enter system view	system-view	-
Configure the time range	time-range <i>time-name</i> { <i>start-time to end-time</i> <i>days-of-the-week</i> [from <i>start-time start-date</i>] [to <i>end-time end-date</i>] from <i>start-time start-date</i> [to <i>end-time end-date</i>] to <i>end-time end-date</i> }	Optional
Define a flow template	flow-template user-defined slot <i>slotid</i> <i>template-info</i>	Optional
Enter ACL view	acl { number <i>acl-number</i> name <i>acl-name</i> [advanced basic link] } [match-order { config auto }]	Required
Define a rule	rule	Required
Exit ACL view	quit	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	The value of <i>interface-type</i> can only be Ethernet port type.
Apply a defined flow template in Ethernet port view	flow-template user-defined	Optional. You can perform this operation only when a flow template has been previously defined.

Table 145 ACL configuration tasks on interface cards

Item	Command	Description
Activate the ACL	packet-filter inbound	Required

The following table describes the configuration tasks for service processor cards.

Table 146 ACL configuration tasks for service processor cards

Item	Command	Description
Enter system view	system-view	-
Configure the time range	time-range <i>time-name</i> { <i>start-time</i> to <i>end-time</i> <i>days-of-the-week</i> [from <i>start-time</i> <i>start-date</i>] [to <i>end-time</i> <i>end-date</i>] from <i>start-time</i> <i>start-date</i> [to <i>end-time</i> <i>end-date</i>] to <i>end-time</i> <i>end-date</i> }	Optional
Enter ACL view	acl { number <i>acl-number</i> name <i>acl-name</i> [advanced basic] } [match-order { config auto }]	Required. Service processor cards do not support Layer 2 ACL.
Define rules	rule	Required
Exit ACL view	quit	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure traffic redirection in Ethernet port view to redirect the packets of a specific VLAN to a service processor card	traffic-redirect inbound ip-group	Required. See section "Configuring Traffic Redirection" "Configuring Traffic Redirection"
Exit Ethernet port view	quit	-
Enter VLAN view	vlan <i>vlan-id</i>	You must enter the VLAN view specified by the redirection function.
Activate the ACL in VLAN view	packet-filter inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] slot <i>slotid</i>	Required

Configuring Time Range

You may set such items in time range configuration: The defined time range includes absolute time range and periodic time range. The absolute time range is in the form of hh:mm YYYY/MM/DD; the periodic time range is in the format of hh:mm, day.

Perform the following configurations in system view.

Table 147 Configure/Delete time range

Operation	Command
Create time range	time-range <i>time-name</i> { <i>start-time</i> to <i>end-time</i> <i>days-of-the-week</i> [from <i>start-time</i> <i>start-date</i>] [to <i>end-time</i> <i>end-date</i>] from <i>start-time</i> <i>start-date</i> [to <i>end-time</i> <i>end-date</i>] to <i>end-time</i> <i>end-date</i> }

Table 147 Configure/Delete time range

Operation	Command
Delete time range	undo time-range { <i>time-name</i> [<i>start-time</i> to <i>end-time</i> <i>days-of-the-week</i> [from <i>start-time</i> <i>start-date</i>] [to <i>end-time</i> <i>end-date</i>] from <i>start-time</i> <i>start-date</i> [to <i>end-time</i> <i>end-date</i>] to <i>end-time</i> <i>end-date</i>] all }

start-time and *end-time* *days-of-the-week* define periodic time range together. *start-time* *start-date* and *end-time* *end-date* define absolute time range together.

If a time range only defines the periodic time range, the time range is only active within the periodic time range.

If a time range defines only periodic time ranges (by repeating this time range name, you can configure multiple periodic time ranges with the same name), the time range is active only within these periodic time ranges.

If a time range only defines the absolute time range, the time range is only active within the absolute time range.

If a time range defines only absolute time ranges (by repeating this time range name, you can configure multiple absolute time ranges with the same name), the time range is active only within these absolute time ranges.

If a time range defines the periodic time range and the absolute time range, the time range is only active when the periodic time range and the absolute time range are both matched. For example, a time range defines a periodic time range which is from 12:00 to 14:00 every Wednesday, and defines an absolute time range which is from 00:00 2004/1/1 to 23:59 2004/12/31. This time range is only active from 12:00 to 14:00 every Wednesday in 2004.

If a time range defines multiple absolute time ranges and multiple periodic time ranges, the time range is active only when periodic time ranges and absolute time ranges are both matched, that is, take the union set of multiple absolute time ranges and multiple periodic time ranges, and then take the intersection set of the union set of multiple absolute time ranges and that of multiple periodic time ranges.

If neither starting time nor end time is specified, the time range is 24 hours (00:00 to 24:00).

If no end date is specified, the time range is from the date of configuration till the largest date available in the system.

Currently the largest time range is 1970/01/01 to 2100/12/31 in the system.



Do not configure multiple periodic time ranges and absolute time ranges for the same time range at a time. If you need to repeat this time range, you must configure multiple time ranges for several times.

Defining and Applying Flow Template

Defining Flow Template

Flow template defines useful information used in flow classification. For example, a template defines a quadruple: source and destination IP, source and destination

TCP ports, and then only those traffic rules including all these elements can be sent to target hardware and referenced for such QoS functions as packet filtering, traffic policing, priority re-labeling. Otherwise, the rules cannot be activated on the hardware and referenced.

Perform the following configurations in system view.

Table 148 Define/Delete flow template

Operation	Command
Define flow template	flow-template user-defined slot <i>slotid</i> <i>template-info</i>
Delete flow template	undo flow-template user-defined slot <i>slotid</i>

Note that the sum of all elements should not be more than 16 bytes in length. The following table lists the length of the elements involved.

Table 149 Length of template elements

Name	Description	Length in template
bt-flag	BT flag bit	6 bytes
cos	The 802.1p priority in the most external 802.1QTag carried by the packet	2 bytes
s-tag-vlan	VLAN ID in the most exterior 802.1QTag carried by the packet	
dip	Destination IP field in IP packet header	4 bytes
dmac	Destination MAC field in Ethernet packet header	6 bytes
dport	Destination port field	2 bytes
dscp	DSCP field in IP packet header	
ip-precedence	IP precedence field in IP packet header	1 byte
tos	ToS field in IP packet header	
exp	EXP field in MPLS packet	
ethernet-protocol	Protocol field in Ethernet packet header	6 bytes
fragment-flags	Flag field of fragment in IP packed header	No bytes
icmp-code	ICMP code field	1 byte
icmp-type	ICMP type field	1 byte
mac-type	MAC-TYPE field in the packet	No bytes
c-tag-cos	The 802.1p priority in the internal 802.1QTag carried by the packet	2 bytes
c-tag-vlanid	The VLAN ID in the internal 802.1QTag carried by the packet	
ip-protocol	Protocol field in IP packet header	1 byte
sip	Source IP field in IP packet header	4 bytes
smac	MAC field in Ethernet packet header	6 bytes
sport	Source port field	2 bytes
tcp-flag	Flag field in TCP packet header	1 byte

Table 149 Length of template elements

Name	Description	Length in template
vlanid	Vlan ID that the switch assigns to the packet	2 bytes
vpn	The flow template pre-defined for MPLS2VPN	2 bytes



- The numbers listed in the table are not the actual length of these elements in IP packets, but their length in flow template. DSCP field is one byte in flow template, but six bits in IP packets. You can determine whether the total length of template elements exceeds 16 bytes using these numbers.
- The dscp, exp, ip-precedence and tos fields jointly occupy one byte. One byte is occupied no matter you define one, two or three of these fields.
- The cos and s-tag-vlan fields jointly occupy two bytes. Two bytes are occupied no matter you define one or two of them. The c-tag-cos and c-tag-vlanid fields jointly occupy two bytes. Two bytes are occupied no matter you define one or two of them.
- The fragment-flags and mac-type fields are 0 in length in flow template, so they can be ignored when you determine whether the total length of template elements exceeds 16 bytes.

You can either use the default template or define a flow template based on your needs.



Default flow template:

```
ip-protocol tcp-flag sport dport icmp-type icmp-code sip 0.0.0.0 dip 0.0.0.0
vlanid.
```

You cannot modify or delete the default flow template.

Applying Flow Template

Perform the following configurations in Ethernet port view to apply the user-defined flow template to current port.

Table 150 Apply/Cancel flow template

Operation	Command
Apply the user-defined flow template	flow-template user-defined
Cancel the applied flow template	undo flow-template user-defined

Defining ACL The switch supports several types of ACLs, which are described in this section.

Follow these steps to define an ACL

- 1 Enter the corresponding ACL view
- 2 Define ACL rules



- If the **time-range** keyword is not selected, the ACL will be effective at any time after being activated.
- You can define multiple sub rules for the ACL by using the **rule** command several times.
- When the QoS/ACL action is configured under the port, if the QoS/ACL is applied without sub rules, the QoS/ACL is matched as per the matching order defined in the ACL rule; if applied with specific sub rules, the QoS/ACL is matched as per the sequence applied under the port.
- By default, ACL rules are matched in **config** order.
- If you want to replace an existing rule, you are recommended to use the **undo** command to delete the original rule first and then reconfigure the rule.

Defining basic ACL

Basic ACLs only make rules and process packets according to the source IP addresses.

Perform the following configurations in the specified views.

Table 151 Define basic ACL

Operation	Command
Enter basic ACL view (system view)	acl { number <i>acl-number</i> name <i>acl-name</i> basic } [match-order { config auto }]
Define an ACL rule (basic ACL view)	rule [<i>rule-id</i>] { permit deny } [source { <i>source-addr wildcard</i> any }] [fragment time-range <i>name</i> vpn-instance <i>instance-name</i>]*
Delete an ACL rule (basic ACL view)	undo rule <i>rule-id</i> [source fragment time-range vpn-instance <i>instance-name</i>]*
Delete an ACL or all ACLs (system view)	undo acl { number <i>acl-number</i> name <i>acl-name</i> all }

Defining advanced ACL

Advanced ACLs define classification rules and process packets according to the attributes of the packets such as source and destination IP addresses, TCP/UDP ports used, and packet priority. ACLs support three types of priority schemes: ToS (type of service) priority, IP priority and DSCP priority.

Perform the following configurations in the specified view.

Table 152 Define advanced ACL

Operation	Command
Enter advanced ACL view (system view)	acl { number <i>acl-number</i> name <i>acl-name</i> advanced } [match-order { config auto }]
Define an ACL rule (advanced ACL view)	rule [<i>rule-id</i>] { permit deny } <i>protocol</i> [source { <i>source-addr wildcard</i> any }] [destination { <i>dest-addr wildcard</i> any }] [source-port <i>operator port1</i> [<i>port2</i>]] [destination-port <i>operator port1</i> [<i>port2</i>]] [icmp-type <i>type code</i>] [established] [[precedence <i>precedence</i> tos <i>tos</i>]* dscp <i>dscp</i>] [fragment] [bt-flag] [time-range <i>name</i>] [vpn-instance <i>instance-name</i>]

Table 152 Define advanced ACL

Operation	Command
Delete an ACL rule (advanced ACL view)	undo rule <i>rule-id</i> [source destination source-port destination-port icmp-type precedence tos dscp fragment bt-flag time-range vpn-instance]*
Delete an ACL or all ACLs (system view)	undo acl { number <i>acl-number</i> name <i>acl-name</i> all }

**CAUTION:**

- The *port1* and *port2* parameters in the command listed in Table 152 should be TCP/UDP ports for higher-layer applications. For some common ports, you can use mnemonic symbols to replace the corresponding port numbers. For example, you can use "bgp" to represent TCP port 179, which is for BGP protocol.
- The rules with specified **bt-flag** cannot be used in the **traffic-redirect** command.

Defining Layer 2 ACLs

Layer 2 ACLs define the Layer 2 information such as source and destination MAC addresses, source VLAN ID, and Layer 2 protocol type in their rules and process packets according to these attributes.

Perform the following configurations in the specified view.

Table 153 Define Layer 2 ACLs

Operation	Command
Enter Layer 2 ACL view (system view)	acl { number <i>acl-number</i> name <i>acl-name</i> link } [match-order { config auto }]
Define an ACL rule (in Layer 2 ACL view)	rule [<i>rule-id</i>] { permit deny } [cos <i>cos-value</i> c-tag-cos <i>c-cos-value</i> exp <i>exp-value</i> <i>protocol-type</i> mac-type { any-broadcast-packet arp-broadcast-packet non-arp-broadcast-packet } [{ unicast-packet multicast-packet } [known unknown]]] ingress { { <i>source-vlan-id</i> [to <i>source-vlan-id-end</i>] <i>source-mac-addr</i> <i>source-mac-wildcard</i> c-tag-vlan <i>c-tag-vlanid</i> }* any } egress { <i>dest-mac-addr</i> <i>dest-mac-wildcard</i> any } s-tag-vlan <i>s-tag-vlanid</i> time-range <i>name</i>]*
Delete an ACL rule (Layer 2 ACL view)	undo rule <i>rule-id</i>
Delete an ACL or all ACLs (system view)	undo acl { number <i>acl-number</i> name <i>acl-name</i> all }

Activating ACL

After defining an ACL, you must activate it. This configuration activates those ACLs to filter or classify the packets forwarded by hardware.

For interface cards, perform the following configurations in Ethernet port view.

Table 154 Activate ACL

Operation	Command
Activate IP group ACL	packet-filter inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]]

Table 154 Activate ACL

Operation	Command
Deactivate IP group ACL	undo packet-filter inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>]
Activate IP group ACL and link group ACL at same time	packet-filter inbound ip-group { <i>acl-number</i> <i>acl-name</i> } { rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] } link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> }
Deactivate IP group ACL and link group ACL at same time	undo packet-filter inbound ip-group { <i>acl-number</i> <i>acl-name</i> } { rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] } link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> }
Activate link group ACL	packet-filter inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]]
Deactivate link group ACL	undo packet-filter inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>]

For service processor cards, perform the following configurations in VLAN view.

Table 155 Activate ACL

Operation	Command
Activate ip group ACL	packet-filter inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] [system-index <i>index</i>] slot <i>slotid</i>
Deactivate ip group ACL	undo packet-filter inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] slot <i>slotid</i>

system-index *index* here is the system index for an ACL rule. When delivering a rule, the system assigns a globally unique index to it, for convenience of later retrieval. You can also assign a system index for it when delivering an ACL rule with this command, but the index value may change while the system is running. You are not recommended to assign a system index if not urgently necessary.

Displaying and Debugging ACL Configurations

After these configurations are completed, you can use the **display** command in any view to view ACL running to check configuration result. You can clear ACL statistics using the **display** command in user view.

Table 156 Display and debug ACL configurations

Operation	Command
Display the configuration and status of the current time range	display time-range { all <i>name</i> }
Display ACL configuration	display acl config { all <i>acl-number</i> <i>acl-name</i> }
Display the total number of ACL rules applied on the specified card	display acl remaining entry slot <i>slotid</i>
Display ACL application information	display acl running-packet-filter { all interface <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-id</i> }
Display the configuration information of the flow template	display flow-template [default interface <i>interface-type</i> <i>interface-number</i> slot <i>slotid</i> user-defined]

Table 156 Display and debug ACL configurations

Operation	Command
Clear ACL statistics	reset acl counter { all <i>acl-number</i> <i>acl-name</i> }

The **display acl config** command only displays the ACL matching information processed by the CPU.

See the corresponding *Command Manual* for description of parameters.

ACL Configuration Example

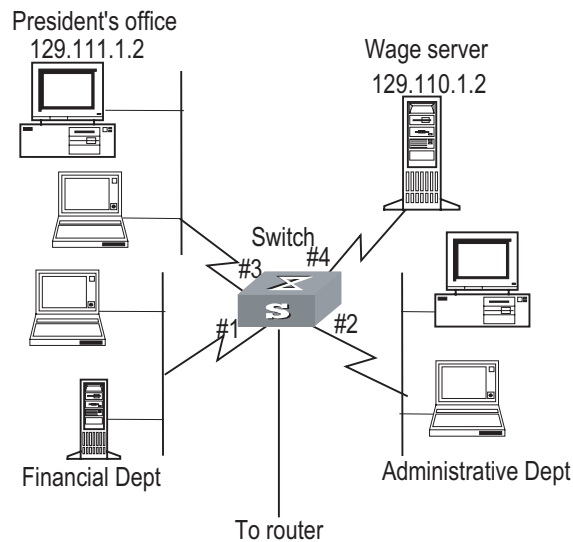
Advanced ACL Configuration Example

Network requirements

The departments in the intranet are connected through 100 Mbps ports of the switches. The research and development (R&D) department is connected through the port Ethernet2/1/1. The wage server of the financial department is at 129.110.1.2. The requirement is to configure ACLs correctly to limit that the R&D department can only access the wage server at working time from 8:00 to 18:00.

Network diagram

Figure 38 Network diagram for advanced ACL configuration



Configuration procedure



Only the commands concerning ACL configuration are listed here.

- 1 Define the time range.

Define the time range from 8:00 to 18:00.

```
[SW8800] time-range 3Com 8:00 to 18:00 working-day
```

- 2 Define inbound traffic to the wage server.

Create a name-based advanced ACL "traffic-of-payserver" and enter it.

```
[SW8800] acl name traffic-of-payserver advanced
```

Define ACL rule for the wage server.

```
[3Com-acl-adv-traffic-of-payserver] rule 1 deny ip source any destination
129.110.1.2 0.0.0.0 time-range 3Com
```

- 3 Activate the ACL.

Activate the ACL "traffic-of-payserver".

```
[3Com-Ethernet2/1/1] packet-filter inbound ip-group traffic-of-payserver
```

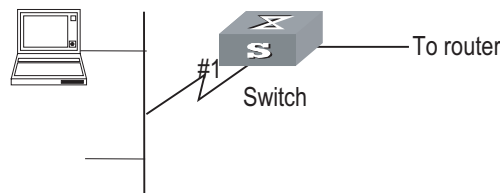
Basic ACL Configuration Example

Network requirements

With proper basic ACL configuration, during the time range from 8:00 to 18:00 everyday the switch filters the packets from the host with source IP 10.1.1.1 (the host is connected through the port Ethernet2/1/1 to the switch.)

Network diagram

Figure 39 Network diagram for basic ACL configuration



Configuration procedure



Only the commands concerning ACL configuration are listed here.

- 1 Define the time range.

Define the time range from 8:00 to 18:00.

```
[SW8800] time-range 3Com 8:00 to 18:00 daily
```

- 2 Define the traffic with source IP 10.1.1.1.

Create a name-based basic ACL "traffic-of-host" and enter it.

```
[SW8800] acl name traffic-of-host basic
```

Define ACL rule for source IP 10.1.1.1.

```
[3Com-acl-basic-traffic-of-host] rule 1 deny source 10.1.1.1 0 time-range 3Com
```

- 3 Activate the ACL.

Activate the ACL "traffic-of-host".

```
[3Com-Ethernet2/1/1] packet-filter inbound ip-group traffic-of-host
```

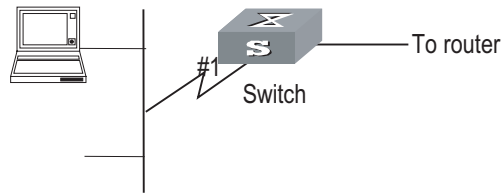
Layer 2 ACL Configuration Example

Network requirements

With proper Layer 2 ACL configuration, during the time range from 8:00 to 18:00 everyday the switch filters the packets with source MAC 00e0-fc01-0101 and destination MAC 00e0-fc01-0303 (configuring at the port Ethernet2/1/1 to the switch.)

Network diagram

Figure 40 Network diagram for Layer 2 ACL configuration



Configuration procedure



Only the commands concerning ACL configuration are listed here.

- 1 Define the time range.

```
# Define the time range from 8:00 to 18:00.
```

```
[SW8800] time-range 3Com 8:00 to 18:00 daily
```

- 2 Define a user-defined flow template

```
[SW8800] flow-template user-defined slot 2 ethernet-protocol smac 0-0-0 dmac
0-0-0
```

- 3 Define the traffic with source MAC 00e0-fc01-0101 and destination MAC 00e0-fc01-0303.

```
# Create a name-based Layer 2 ACL "traffic-of-link" and enter it.
```

```
[SW8800] acl name traffic-of-link link
```

```
# Define an ACL rule for the traffic with the source MAC address of
00e0-fc01-0101 and the destination MAC address of 00e0-fc01-0303.
```

```
[3Com-acl-link-traffic-of-link] rule 1 deny ingress 00e0-fc01-0101 0-0-0
egress 00e0-fc01-0303 0-0-0 time-range 3Com
[3Com-acl-link-traffic-of-link] quit
```

- 4 Apply the user-defined flow template to the port and activate the ACL.

```
# Apply the user-defined flow template to Ethernet2/1/1.
```

```
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] flow-template user-defined
```

```
# Activate the ACL "traffic-of-link".
```

```
[3Com-Ethernet2/1/1] packet-filter inbound link-group traffic-of-link
```

Example of BT Traffic Control Configuration

Network requirements

BitTorrent (BT) is a kind of shared software for file download. Its feature is as follows: The more people are using it to download a file, the faster the file downloads. While BT download greatly reduces the burden of the download server, it also brings dramatic increase of download traffic on the internet. As a result, the network bandwidth is greatly occupied by the BT download traffic, which influences other network services seriously. Therefore, it is necessary to control the BT traffic effectively.

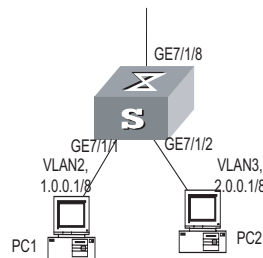
The purpose of the configuration is to prohibit the BT data traffic passing through port GE7/1/8 by configuring proper ACL rules.



CAUTION: 3C17526 series cards do not support BT traffic control configuration.

Network diagram

Figure 41 Network diagram for BT traffic control



Configuration procedure

- 1 Define a user-defined flow template

```
[SW8800] flow-template user-defined slot 7 ip-protocol bt-flag sip 0.0.0.0
dport
```

- 2 Define an advanced ACL rule

```
[SW8800] acl number 3000
[3Com-acl-adv-3000] rule 0 deny tcp bt-flag
[3Com-acl-adv-3000] quit
```

- 3 Enter the port GE7/1/8 and configure BT traffic control on the port

```
[SW8800] interface GigabitEthernet 7/1/8
[3Com-GigabitEthernet7/1/8] flow-template user-defined
[3Com-GigabitEthernet7/1/8] packet-filter inbound ip-group 3000 rule 0
```

22

QoS CONFIGURATION

QoS Overview

Conventional packet network treats all packets equally. Each switch/router processes all packets in First-in-First-out (FIFO) mode and then transfers them to the destination in the best effort, but it provides no commitment and guarantee to such transmission performance as delay and jitter.

With fast growth of computer networks, more and more data like voice and video that are sensitive to bandwidth, delay and jitter are transmitted over the network. This makes growing demands on quality of service (QoS) of networks.

Ethernet technology is a widely-used network technology dominant for independent LANs and many LANs based on Ethernet are organic parts of the Internet. In addition, Ethernet access is becoming one of the major access modes for Internet users. Therefore it is inevitable to consider Ethernet QoS if we want to achieve point-to-point global QoS solution. Ethernet switching devices then naturally need to provide different QoS guarantee for different types of services, especially for those which are sensitive to delay and jitter.

The following terms are involved in QoS.

Flow

It refers to all packets passing through the switch.

Traffic classification

Traffic classification is the technology that identifies the packets with a specified attribute according to a specific rule. Classification rule refers to a packet filtering rule configured by an administrator. A classification rule can be very simple. For example, the switch can identify the packets of different priority levels according to the ToS (type of service) field in the packet headers. It can also be very complex. For example, it may contain information of the link layer (layer 2), network layer (layer 3) and transport layer (layer 4) and the switch classifies packets according to such information as MAC address, IP protocol, source address, destination address and port ID. Classification rule often is limited to the information encapsulated at the packet header, rarely using packet contents.

Packet filtering

Packet filtering refers to filtering operation applied to traffic flow. For example, the deny operation drops the traffic flow which matches the classification rule and allows other traffic to pass. Ethernet switches use complex classification rules, so that traffic flow can be filtered purposefully to enhance network security.

There are two key steps in packet filtering:

Step 1: Classify the traffic at the port according to a specific rule.

Step 2: Run filtering operation (deny or permit) to the identified traffic. By default, permit operation is selected.

Traffic policing

QoS can police traffic at the ingress port, to provide better services with the limited network resources.

Redirection

You can re-specify forwarding direction for packets, based on QoS policy.

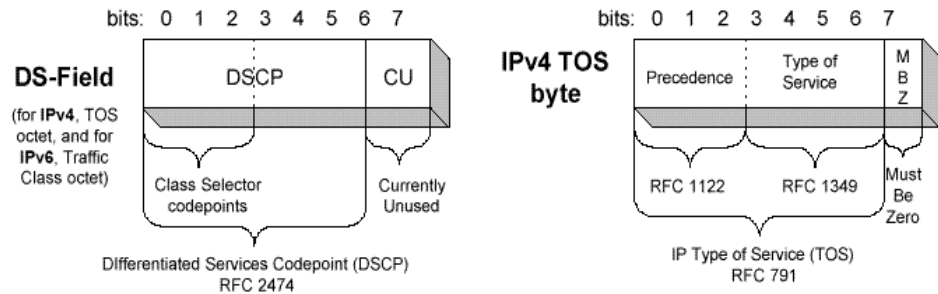
Traffic priority

Ethernet switches can provide priority tags, including ToS, DSCP, 802.1p, and so on, for specific packets. These priority tags are applicable to different QoS models.

The following describes IP priority, ToS priority, DCSP priority, Exp priority and 802.1p priority.

1 IP priority, ToS priority, DSCP priority and Exp priority

Figure 42 DS field and ToS byte

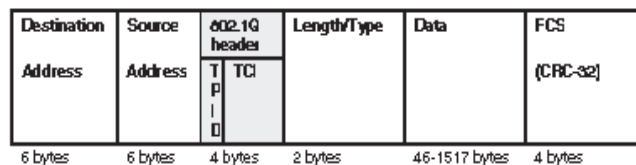


As shown in Figure 42, the ToS field in the IP header contains 8 bits. The first three bits represent IP priority, in the range of 0 to 7; bits 3-6 stand for ToS priority, in the range of 0 to 15. RFC2474 redefines the ToS field in IP packets as DS (differentiated services) field. The first six bits denote DSCP (differentiated services codepoint) priority, in the range of 0 to 63, the latter two bits are reserved. The first three bits (bit 0~2) of DSCP priority represent Exp priority, in the range of 0 to 7.

2 802.1p priority

802.1p priority is stored in the header of Layer 2 packets and is suitable for the case where only Layer 2 QoS guarantee, not L3 header analysis, is required.

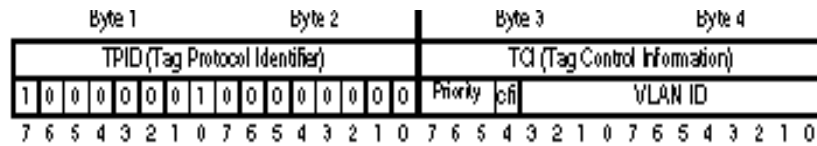
Figure 43 Ethernet frame with 802.1Q tag header



In the above figure, each host supporting 802.1Q protocol adds a 4-byte 802.1Q tag header after the source address in Ethernet header.

The 802.1Q tag header contains a 2-byte TPID (Tag protocol Identifier, with the value 8100) and a 2-byte TCI (tag control information). TPID is newly defined by IEEE to represent a packet with 802.1Q tag added. The contents of 802.1Q tag header are shown in Figure 44.

Figure 44 802.1Q tag header



In the figure, the priority field in TCI stands for 802.1p priority, which consists of three bits. There are eight priority levels, numbered as 0 to 7, for determining to send which packets first when switch congestion takes place.

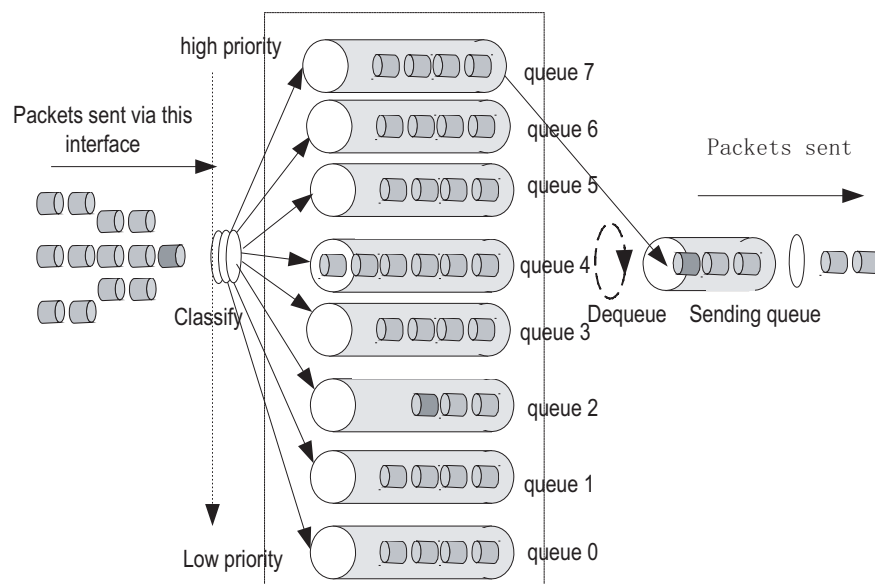
Since their applications are defined in detail in the 802.1p Recommendation, they are named as 802.1p priority levels.

Queue scheduling

Queue scheduling is used to resolve problems of resource contention by many packets. These algorithms are often used in queue scheduling: strict priority (SP) algorithm and weighted round Robin (WRR) algorithm.

1 SP algorithm

Figure 45 Priority queues



SP algorithm is designed for key services. One of the characteristics of key services is these services should be processed first to minimize response delay during switch congestion. For example, there are eight outbound queues at the port, numbered respectively as 7 to 0, with priority levels in descending order.

In SP mode, the system first sends those packets of higher priority in strict accordance with priority order. Only when packets in high priority queue are all

sent can those in lower priority queue be sent. This manner of putting key-service packets into high priority queue and non-key service packets into low priority queue does ensure that key-service packets are sent first, while non-key service packets are sent during the interval when no key-service packets needs to be processed.

SP algorithm also has its disadvantages: If high priority queues are full, then packets from the low priority queues may not be forwarded.

2 WRR algorithm

Each port supports eight outbound queues except that port of the GV48D/GP48D/XP4 non-wire-speed card only supports four queues. In WRR mode, the system processes the queues by turn, so every queue can have a service period.

See the case where the port supports eight outbound queues. Every queue is assigned with a weight value (respectively numbered as w7, w6, w5, w4, w3, w2, w1 and w0), which indicates the weight in obtaining resources. For a 100 Mbps port, the weight values are set as 50, 30, 10, 10, 50, 30, 10 and 10 (corresponding respectively to w7, w6, w5, w4, w3, w2, w1 and w0). The even the queue with the lowest priority can be allocated with a 5 Mbps bandwidth.

Another merit for WRR algorithm: Though the queues are scheduled by turn, they are not configured with fixed time quantum. If a queue has no packets, the system immediately schedules the next queue. Then bandwidth resources can be fully utilized.

Traffic mirroring

Traffic mirroring duplicates specified packets to CPU for network test and troubleshooting.

Port mirroring

Port mirroring duplicates all packets at a specified port to the monitoring port for network test and troubleshooting.

Flow-based traffic statistics

The system can make traffic statistics based on flow for further analysis.

Introduction to QoS Configuration Based on Port Groups

To help you configure the same QACL rule on multiple ports, Switch 8800 Family series switches implement the function of configuring QACL based on port groups. You only need to create a port group and configure QACL for the port group. The configuration is valid for all the member ports in the port group, thus avoiding configuring QACL on multiple ports respectively. After a port group is configured, the QACL configuration of all the member ports in the port group keeps the same all the time.

Configuring QoS Based on Port Groups

Perform the following configuration to configure QoS based on port groups (assume that the flow template and ACL have been defined):

Table 157 Configure QoS based on port groups

Configuration procedure	Command	Description
Enter system view	system-view	-
Enable descriptor share on the specified card	share descriptors <i>slotid</i>	This function is disabled by default. Required
Enter port group view	port-group <i>index</i>	<i>index</i> : Port group number. The port group number of a common interface card ranges from 1 to 128. Required
Add a port to the port group	port <i>interface-list</i>	<i>interface-list</i> ={ <i>interface-type</i> <i>interface-number</i> [to <i>interface-type</i> <i>interface-number</i>] }&<1-n> Optional
Display the configured information of the port group	display port-group [<i>index</i>]	This command can be executed in any view Optional
Apply the flow template	flow-template user-defined	See "Defining and Applying Flow Template" "Defining and Applying Flow Template" Optional
Activate the ACL	packet-filter inbound	See "Activating ACL" "Activating ACL" Optional
Configure local priority of the port group	priority { <i>priority-level</i> trust }	See "Configuring Service Parameter Allocation Rule" "Configuring Service Parameter Allocation Rule" Optional
Configure traffic policing	traffic-limit inbound	See "Configuring Traffic Policing" "Configuring Traffic Policing" Optional
Configure traffic shaping	traffic-shape [queue <i>queue-id</i>] <i>max-rate burst-size</i>	See "Configuring Traffic Shaping" "Configuring Traffic Shaping" Optional
Configure packet priority	traffic-priority inbound	See "Configuring Traffic Priority" "Configuring Traffic Priority" Optional
Configure packet redirection	traffic-redirect inbound	See "Configuring Traffic Redirection" "Configuring Traffic Redirection"
Configure queue scheduling algorithm	queue-scheduler wrr { group1 { <i>queue-id</i> <i>queue-weight</i> } &<1-8> group2 { <i>queue-id</i> <i>queue-weight</i> } &<1-8> }*	Optional See "Configuring Queue Scheduling" "Configuring Queue Scheduling"

Table 157 Configure QoS based on port groups

Configuration procedure	Command	Description
Configure the drop mode on a port	drop-mode { tail-drop wred } [<i>wred-index</i>]	Optional See "Configuring WRED Parameters" "Configuring WRED Parameters"
Configure traffic mirroring	mirrored-to inbound	Optional See "Configuring Traffic Mirroring" "Configuring Traffic Mirroring"
Configure traffic statistics	traffic-statistic inbound	Optional See "Configuring Traffic Statistics" "Configuring Traffic Statistics" This command can be executed in any view.
Display the configured information	display	See "Displaying and Debugging QoS Configuration" "Displaying and Debugging QoS Configuration"

When you configure the port group of the common interface card except for the XP4 card, notice that:

- Do not add the ports of different cards to the same port group. Do not add the same port to multiple port groups.
- After a port is added to the port group, the port configuration is overwritten by that of the port group. You cannot apply the ACL rule as per port.
- You are not allowed to add aggregated ports in the port group. If a port in the port group needs to be aggregated, the port must quit the port group. After the port is aggregated, the port configuration is overwritten by that of the primary port in the aggregation group.
- When the port group is null, it is not allowed to configure QACL. After all the members quit the port group, the QACL configuration of the port group still remains. When a new port joins the port group, QACL will be applied to the port automatically.

By default, two port groups of the XP4 card are created. The member ports are port 0 to 1 and port 2 to 3 respectively. The system allocates port group numbers automatically. They are $300 + 2 \times \text{slot-no.}$ and $300 + 2 \times \text{slot-no.} + 1$ respectively. "slot-no" indicates the number of the slot where the XP4 card resides. For example, when the XP4 card resides in slot 1, the corresponding port group numbers are 302 and 303. The following section describes the special limits on the port group configuration of the XP4 card:

- It is not allowed to configure a new port group. No port is allowed to join or quit the port group.
- All the QACL configuration commands that can be formerly performed on individual ports can only be performed on port groups now.
- Traffic shaping is not supported.

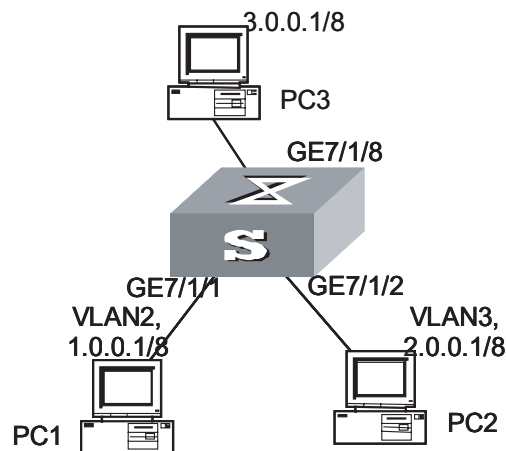
- The XP4 card does not support inter-group port mirroring. A port group can have an inbound and an outbound monitoring port. There is only one monitoring port in other types of interface cards.
- The XP4 card does not support queue scheduling.

Configuration Example Network requirements

Set the next-hop address of the packets forwarded by GE7/1/1 and GE7/1/2 from 8:00 to 18:00 to 3.0.0.1.

Network diagram

Figure 46 Example of configuring packet redirection



Configuration procedure

- 1 Define a time range.

Define a time range from 8:00 to 18:00.

```
[SW8800] time-range 3Com 8:00 to 18:00 daily
```

- 2 Define the ACL rule of the PC packet.

Enter ACL rule view identified with the number 2000.

```
[SW8800] acl number 2000
```

Define the traffic classification rule.

```
[3Com-acl-basic-2000] rule 0 permit source any time-range 3Com
```

```
[3Com-acl-basic-2000] quit
```

- 3 Create a port group.

Create a port group. The port group number is 1.

```
[SW8800] port-group 1
```

Add GE7/1/1 and GE7/1/2 to port group 1.

```
[3Com-port-group1] port GigabitEthernet 7/1/1 GigabitEthernet 7/1/2
```

4 Redirect the packet forwarded to the port group.

```
# Set the next hop of the packet forwarded to the port in port group 1 to 3.0.0.1.
```

```
[3Com-port-group1] traffic-redirect inbound ip-group 2000 rule 0 next-hop
3.0.0.1
```

QoS Configuration

The following sections describe QoS configuration tasks.

- “Configuring Service Parameter Allocation Rule”
- “Configuring Traffic Policing”
- “Configuring Traffic Shaping”
- “Configuring Traffic Priority”
- “Configuring Traffic Redirection”
- “Configuring Queue Scheduling”
- “Configuring Traffic Mirroring”
- “Configuring Port Mirroring”
- “Configuring Traffic Statistics”



- Before initiating any of these QoS configuration tasks, you should first define the corresponding ACL. Then you can achieve packet filtering just by activating the right ACL.
- To configure packet filtering, you need only to activate corresponding ACL. For more details, refer to the section “Activating ACL”.

Some of QoS terms are listed in the following table.

Table 158 QoS terms

Term	Description
CoS	It has the same meaning as 802.1p priority. Both refer to the priority at packet header, with the value ranging from 0 to 7.
Service parameters	Switch allocates a set of parameters, which are used in achieving QoS functions, upon receiving a packet. Four items are included: 802.1p priority, DSCP priority, local precedence and drop precedence.
Drop-precedence	One of service parameters, ranging from 0 to 2. Drop precedence is allocated when the switch receives the packet and may be when the packet is processed. Allocating drop precedence to the packet is also called coloring the packet: the packet with drop precedence 2 as red, that with drop precedence 1 as yellow and that with drop precedence 0 as green. Drop precedence is referred to when switch needs to drop packets in its congestion.

Table 158 QoS terms

Term	Description
Conform-Level	The result calculated from the user-defined CIR, CBS, EBS, PIR and actual traffic when the switch runs traffic policing, in the range of 0 to 2. The parameter is used to select the remark service parameters, such as remark-cos and remark-drop, in traffic policing by means of the traffic-limit command. The packets with different conform-levels query different mapping tables. The conform-level of the packets whose traffic is smaller than cir is 0, the conform-level of the packets whose traffic is bigger than cir and smaller than pir is 1, and the conform-level of the packets whose traffic is bigger than pir is 2. It is also involved in the DSCP + Conform level -> Service parameter mapping table which is used in re-allocating service parameters to a packet with the traffic-priority command. Then Conform-Level must be 0.

Configuring Service Parameter Allocation Rule

QoS is based on service parameters, a set of parameters for a packet, including 802.1p priority (CoS priority), DSCP priority, EXP priority, local precedence and drop precedence.

After receiving a packet, the switch allocates a set of service parameters to it according to a specific rule. The switch first gets its local precedence and drop precedence according to the packet 802.1p priority value, by searching in the CoS -> Local-precedence mapping table and the CoS -> Drop-precedence mapping table. Default values are available for the two mapping tables, but you can also configure the mapping tables according to your needs. If the switch fails in allocating local precedence for the packet, it configures the local precedence of the packet to be the precedence of the port that receives this packet. After obtaining the packet CoS value by inverse-searching the CoS -> Local-precedence mapping table, the switch then gets its drop precedence from the CoS -> Drop-precedence mapping table.



*If a port is not configured by means of the **priority** command (namely, the default priority 0 is used), all tagged packets through this port will not be mapped to the local precedence according to the 802.1p priority in the tag;*

When the **priority** command is used on the port and the parameter of the command is not 0, or when the **traffic-priority** command is used to mark the priority of the packet, all the tagged packets through the port will be mapped to the local precedence according to the 802.1p priority in the Tag.

Configuring mapping table

Perform the following configurations in system view.

Table 159 Configure mapping tables

Operation	Command
Configure the CoS -> Drop-precedence mapping table	qos cos-drop-precedence-map cos0-map-drop-prec cos1-map-drop-prec cos2-map-drop-prec cos3-map-drop-prec cos4-map-drop-prec cos5-map-drop-prec cos6-map-drop-prec cos7-map-drop-prec
Restore the default values of CoS -> Drop-precedence mapping table	undo qos cos-drop-precedence-map

Table 159 Configure mapping tables

Operation	Command
Configure the CoS -> Local-precedence mapping table	qos cos-local-precedence-map <i>cos0-map-local-prec cos1-map-local-prec cos2-map-local-prec cos3-map-local-prec cos4-map-local-prec cos5-map-local-prec cos6-map-local-prec cos7-map-local-prec</i>
Restore the default values of CoS -> Local-precedence mapping table	undo qos cos-local-precedence-map

By default, the switch obtains local precedence and drop precedence according to the default mapping values.

Configuring default local precedence

Perform the following configurations in Ethernet port view.

Table 160 Configure default local precedence for port

Operation	Command
Configure default local precedence for a port	priority <i>priority-level</i>
Restore the default local precedence for a port	undo priority

Perform the following configuration in port group view.

Table 161 Configure priority for the port group

Operation	Command
Configure local priority for the port group	priority { <i>priority-level</i> trust }
Restore the local priority of the port group to the default value	undo priority

Configuring Traffic Policing

Traffic policing refers to rate limit based on traffic. If the traffic threshold is exceeded, corresponding measures will be taken, for example, dropping the excessive packets or re-defining their priority levels.

In the traffic supervision action, the switch uses the service parameters allocated according to the DSCP + Conform-Level -> Service parameter mapping table and the EXP + Conform-Level -> Service parameter mapping table and the 802.1p priority values allocated according to the Local-precedence+Conform-Level -> 802.1p priority mapping table. So you should configure these three mapping tables or use their default values.

Configuring mapping tables

Perform the following configurations in the specified views.

Table 162 Configure mapping table

Operation	Command
Enter conform level view (System view)	qos conform-level <i>conform-level-value</i>
Configure the DSCP + Conform-Level -> Service parameters mapping table (conform level view)	dscp <i>dscp-list : dscp-value exp-value cos-value local-precedence-value drop-precedence</i>

Table 162 Configure mapping table

Operation	Command
Restore the default values of the DSCP + Conform-Level -> Service parameters mapping table (conform level view)	undo dscp <i>dscp-list</i>
Configure the EXP + Conform-Level -> Service parameters mapping table (conform level view)	exp <i>exp-list</i> : <i>dscp-value exp-value cos-value local-precedence-value drop-precedence</i>
Restore the default values of the EXP + Conform-Level -> Service parameters mapping table (conform level view)	undo exp <i>exp-list</i>
Configure the Local-precedence + Conform-Level -> mapping table (conform level view)	local-precedence <i>cos-value0 cos-value1 cos-value2 cos-value3 cos-value4 cos-value5 cos-value6 cos-value7</i>
Restore the default values of the Local-precedence + Conform-Level -> mapping table (conform level view)	undo local-precedence

The system provides default mapping tables.

Configuring traffic parameters (optional)

Use the following command to set the traffic parameters required before configuring traffic policing on service processor cards.



CAUTION: This operation is not required for configuring traffic policing on common cards.

Perform the following configuration in system view.

Table 163 Configure traffic parameters

Operation	Command
Configure traffic parameters	traffic-params <i>traffic-index cir committed-info-rate cbs committed-base-size ebs exceed-base-size</i> [pir <i>peak-info-rate</i>]

Configuring traffic policing

The purpose of this configuration task is to implement traffic policing on ACL-matched data streams, and then take normal actions on data streams within the traffic limit and take other actions (discarding packets, for example) on those exceeding the limit.

For interface cards, perform the following configurations in Ethernet port view.

Table 164 Configure traffic policing

Operation	Command
Configure traffic policing which only applies IP group ACL	traffic-limit inbound ip-group { <i>acl-number acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] [tc-index <i>index</i>] <i>cir cbs ebs</i> [<i>pir</i>] [conform { { remark-cos remark-drop-priority }* remark-policed-service }] [exceed { forward drop }]
Remove traffic policing setting which only applies IP group ACL	undo traffic-limit inbound ip-group { <i>acl-number acl-name</i> } [rule <i>rule</i>]

Table 164 Configure traffic policing

Operation	Command
Configure traffic policing which applies IP group ACL and link group ACL at same time	traffic-limit inbound ip-group { <i>acl-number</i> <i>acl-name</i> } { rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> } [tc-index <i>index</i>] <i>cir cbs ebs</i> [<i>pir</i>] [conform { { remark-cos remark-drop-priority }* } remark-policed-service }] [exceed { forward drop }]
Remove traffic policing setting which applies IP group ACL and link group ACL at same time	undo traffic-limit inbound ip-group { <i>acl-number</i> <i>acl-name</i> } { { rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> }
Configure traffic policing which only applies link group ACL	traffic-limit inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] [tc-index <i>index</i>] <i>cir cbs ebs</i> [<i>pir</i>] [conform { { remark-cos remark-drop-priority }* } remark-policed-service }] [exceed { forward drop }]
Remove traffic policing setting which only applies link group ACL	undo traffic-limit inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>]



It is required that CIR is less than or equal to PIR and CBS is less than or equal to EBS. You are recommended to configure CBS and EBS to numbers that are 100 to 150 times of CIR.

For service processor cards, perform the following configurations in VLAN view.

Table 165 Configure traffic policing

Operation	Command
Configure traffic policing which only applies IP group ACL	traffic-limit inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] traffic-index <i>index</i>] [conform { { remark-cos remark-policed-service } }] [exceed { forward drop }] slot <i>slotid</i>
Remove traffic policing setting which only applies IP group ACL	undo traffic-limit inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] slot <i>slotid</i>

**CAUTION:**

- Before executing the **traffic-limit** command on a service processor card, you must first configure traffic redirection in Ethernet port view to redirect the packets of a specific VLAN to the service processor card.
- Before configuring traffic policing, you must first define corresponding ACLs and configure the DSCP+ Conform-Level -> Service parameters mapping table and the Local-precedence + Conform-Level -> 802.1p priority mapping table.

You must first define the corresponding ACL and configure the DSCP + Conform-Level -> Service parameters mapping table and Local-precedence + Conform-Level -> mapping table before starting this configuration.

This configuration achieves traffic policing for the packets that match the ACL. If the traffic rate threshold is exceeded, corresponding measures will be taken, for example, dropping excessive packets.

system-index *index* here is the system index for an ACL rule. When delivering a rule, the system assigns a globally unique index to it, for convenience of later

retrieval. You can also assign a system index for it when delivering an ACL rule with this command, but the index value may change while the system is running. However, you are not recommended to assign a system index if not urgently necessary.

tc-index *index* here is traffic policing index. If you configure the same index for different ACL rules during setting traffic policing, then the sum of traffic shall be limited by the traffic policing-related parameters predefined. For example, if CIR (committed information rate) of the traffic that matches ACL1 is set to 10 kbps and that for ACL2 to 10 kbps, and their traffic policing indexes are the same, then the average rate of the traffic that matches ACL1 and ACL2 shall be limited to 10kbps.



When you specify the same tc-index for different traffics, the traffic policing-related parameter settings must be consistent with each other. Otherwise, the system will prompt an error.

See the corresponding Command Manual for details of the commands.

Configuring Traffic Shaping

Traffic shaping controls the rate of outbound packets, to ensure they are sent at relatively average rates. Traffic shaping measure tries to match packet transmission rate with the capacity of downstream devices. Its major difference from traffic policing is: Traffic shaping buffers packets at over-threshold rates to make them sent at average rates, while traffic policing drops excessive packets. Therefore, traffic shaping may increase transmission delay, but not for traffic policing.

Perform the following configurations in Ethernet port view.

Table 166 Configure traffic shaping

Operation	Command
Configure traffic shaping	traffic-shape [queue <i>queue-id</i>] <i>max-rate burst-size</i>
Remove traffic shaping setting	undo traffic-shape [queue <i>queue-id</i>]

The switch supports traffic shaping based on port, that is, all traffic on the port is shaped. It also supports traffic shaping for a specific queue. You can choose to achieve one of them by selecting different parameters in the command.

See the corresponding Command Manual for details of the commands.

Configuring Traffic Priority

This configuration re-labels priority value for the packets that match the ACL in these ways: using the service parameters allocated by the switch, re-allocating service parameters by searching the mapping table based on the packet DSCP value, re-allocating service parameters by searching the mapping table based on the specified DSCP value and EXP value, customizing service parameters for the packets.

For interface cards, perform the following configurations in Ethernet port view.

Table 167 Configure traffic priority

Operation	Command
Configure traffic priority which only applies IP group ACL	traffic-priority inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] { auto remark-policed-service { trust-dscp dscp <i>dscp-value</i> untrusted dscp <i>dscp-value</i> cos <i>cos-value</i> local-precedence <i>local-precedence</i> drop-priority <i>drop-level</i> } }
Remove traffic priority setting which only applies IP group ACL	undo traffic-priority inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>]
Configure traffic priority which applies IP group ACL and link group ACL at same time	traffic-priority inbound ip-group { <i>acl-number</i> <i>acl-name</i> } { rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> } { auto remark-policed-service { trust-dscp dscp <i>dscp-value</i> untrusted dscp <i>dscp-value</i> cos <i>cos-value</i> local-precedence <i>local-precedence</i> drop-priority <i>drop-level</i> } }
Remove traffic priority setting which applies IP group ACL and link group ACL at same time	undo traffic-priority inbound ip-group { <i>acl-number</i> <i>acl-name</i> } { rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> }
Configure traffic priority which only applies link group ACL	traffic-priority inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] { auto remark-policed-service { trust-dscp dscp <i>dscp-value</i> untrusted dscp <i>dscp-value</i> cos <i>cos-value</i> local-precedence <i>local-precedence</i> drop-priority <i>drop-level</i> } }
Remove traffic priority setting which only applies link group ACL	undo traffic-priority inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>]

For service processor cards, perform the following configurations in VLAN view.

Table 168 Mark packet priority

Operation	Command
Mark the packets matching Layer 3 ACL rule with priority	traffic-priority inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] { auto remark-policed-service { trust-dscp dscp <i>dscp-value</i> untrusted dscp <i>dscp-value</i> cos <i>cos-value</i> local-precedence <i>local-precedence</i> drop-priority <i>drop-level</i> } } slot <i>slotid</i>
Remove the mark	undo traffic-priority inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] slot <i>slotid</i>

**CAUTION:**

- Before executing the **traffic-priority** command on a service processor card, you must first configure traffic redirection in Ethernet port view to redirect the packets of a specific VLAN to the service processor card.
- Before performing this configuration, you must first define the corresponding ACL and configure the DSCP + Conform-Level -> Service parameters mapping table and the EXP + Conform-Level -> Service parameters mapping table.

system-index *index* here is the system index for an ACL rule. When delivering a rule, the system assigns a globally unique index to it, for convenience of later retrieval. You can also assign a system index for it when delivering an ACL rule with this command, but the index value may change while the system is running.

However, you are not recommended to assign a system index if not urgently necessary.



- For MPLS packets, other than that the dscp-value stands for their DSCP priority value, the dscp-value is also mapped to the EXP. You set the EXP value when defining the dscp-value. Note that when the Switch 8800 Family switch is used as the ingress PE: for IP packets, EXP is matched according to the "DSCP+Conform-Level -> Service parameters" mapping table; for TCP and UDP packets, the value of EXP is the lower 3 bits of *dscp-value*. When the Switch 8800 Family switch is used as ingress P, the value of EXP is the lower 3 bits of *dscp-value*.
- The DSCP + Conform-Level 0 -> Service parameters mapping table and the EXP + Conform-Level -> Service parameters mapping table (the mapping table for conform level 0) is used here.

See the corresponding Command Manual for details of the commands.

Configuring Traffic Redirection

Traffic redirection changes packet forwarding direction, to CPU, other ports, other IP addresses or other cards.

For interface cards, perform the following configurations in Ethernet port view.

Table 169 Configure traffic redirection

Operation	Command
Configure traffic redirection which only applies IP group ACL	traffic-redirect inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] { cpu interface <i>interface-type</i> <i>interface-number</i> <i>destination-vlan</i> { I2-vpn I3-vpn } next-hop <i>ip-addr1</i> [<i>ip-addr2</i>] [invalid { forward drop }] slot <i>slotid</i> { <i>vlanid</i> designated-vlan <i>vlanid</i> } [join-vlan] }
Remove traffic redirection setting which only applies IP group ACL	undo traffic-redirect inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>]
Configure traffic redirection which applies IP group ACL and link group ACL at same time	traffic-redirect inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] { cpu interface <i>interface-type</i> <i>interface-number</i> <i>destination-vlan</i> { I2-vpn I3-vpn } next-hop <i>ip-addr1</i> [<i>ip-addr2</i>] [invalid { forward drop }] slot <i>slotid</i> designated-vlan <i>vlanid</i> [join-vlan] }
Remove traffic redirection setting which applies IP group ACL and link group ACL at same time	undo traffic-redirect inbound ip-group { <i>acl-number</i> <i>acl-name</i> } { rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> } or undo traffic-redirect inbound link-group { <i>acl-number</i> <i>acl-name</i> } { rule <i>rule</i> ip-group { <i>acl-number</i> <i>acl-name</i> } ip-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> }
Configure traffic redirection which only applies link group ACL	traffic-redirect inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] { cpu interface <i>interface-type</i> <i>interface-number</i> <i>destination-vlan</i> { I2-vpn I3-vpn } next-hop <i>ip-addr1</i> [<i>ip-addr2</i>] [invalid { forward drop }] slot <i>slotid</i> designated-vlan <i>vlanid</i> [join-vlan] }

Table 169 Configure traffic redirection

Operation	Command
Remove traffic redirection setting which only applies link group ACL	undo traffic-redirect inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>]

For service processor cards, perform the following configurations in VLAN view.

Table 170 Configure traffic redirection

Operation	Command
Configure traffic redirection on packets matching Layer 3 ACL rule.	traffic-redirect { inbound outbound } ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] { cpu next-hop <i>ip-addr1</i> [<i>ip-addr2</i>] [invalid { forward drop }] } [slot <i>slotid</i>]
Remove this traffic redirection configuration on the packets matching Layer 3 ACL rule.	undo traffic-redirect inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] [slot <i>slotid</i>]

system-index *index* here is the system index for an ACL rule. When delivering a rule, the system assigns a globally unique index to it, for convenience of later retrieval. You can also assign a system index for it when delivering an ACL rule with this command, but the index value may change while the system is running. However, you are not recommended to assign a system index if not urgently necessary.



- Traffic redirection setting is only available for the permitted rules in the ACL.
- The packet redirected to the CPU cannot be forwarded normally.
- You can achieve policy route by selecting the **next-hop** keyword.
- Before executing the **traffic-redirect** command on a service processor card, you must first configure traffic redirection in Ethernet port view to redirect the packets in Layer 3 to the service processor card and specific VLAN.
- Multicast packets are not allowed to be redirected to the service processor cards.

See the corresponding Command Manual for details of the commands. Refer to the "VLAN&QinQ" section in the manual for detailed information on the **traffic-redirect** { **nested-vlan** | **modified-vlan** } command.

Configuring Queue Scheduling

Each port supports eight outbound queues except that ports of GV48D/GP48D/XP4 non-wire-speed cards only support four queues. The switch puts the packets into the queues according to the local precedence of packets. Queue scheduling is used to resolve problems of resource contention by many packets. The switch supports SP algorithm and WRR algorithm.

Different outbound queues at the port may use different algorithms. The switch supports three scheduling modes:

- 1 All-SP scheduling mode
- 2 All-WRR mode: A queue is selected from each of the two WRR groups during scheduling, and then the two queues are compared for priority. The queue with higher priority will be scheduled. After scheduling, another queue is selected from the WRR group containing the queue with higher priority, and the newly selected queue will be compared with the previously selected queue that has lower priority.
- 3 SP plus WRR mode: The outbound queues are put into different scheduling groups. SP group uses SP algorithm, WRR groups use WRR algorithm. The select one queue respectively from SP group, WRR group 1 and WRR group 2 and schedule them using SP algorithm.

Perform the following configurations in Ethernet port view.

Table 171 Configure queue scheduling

Operation	Command
Configuring queue scheduling	queue-scheduler wrr { group1 { <i>queue-id</i> <i>queue-weight</i> } &<1-8> group2 { <i>queue-id</i> <i>queue-weight</i> } &<1-8> }*
Restore the default setting	undo queue-scheduler [<i>queue-id</i>] &<1-8>

By default, the switch uses all-SP mode, so those queues not configured with WRR algorithm are SP mode.

See the corresponding Command Manual for details of the commands.

Configuring WRED Parameters

In the case of network congestion, the switch drops packets to release system resources. And then no packets are put into long-delay queues.

The switch allocates drop precedence for it when receiving a packet (also called coloring the packet). The drop precedence values range from 0 to 2, with 2 for red, 1 for yellow and 0 for green. In congestion, red packets will be first dropped, and green packets last.

You can configure drop parameters and thresholds by queue or drop precedence.

The following two drop modes are available:

- 1 Tail drop mode: Different queues (red, yellow and red) are allocated with different drop thresholds. When these thresholds are exceeded respectively, excessive packets will be dropped.
- 2 WRED drop mode: Drop precedence is taken into account in drop action. When only min-thresholds of red, yellow and green packets are exceeded, excessive packets are dropped randomly at given probability. But when max-thresholds of red, yellow and green packets are exceeded, all excessive packets will be dropped.

You must first configure WRED parameters for every outbound queue in defining drop precedence.

Configuring WRED parameters

The switch provides four sets of default WRED parameters, respectively numbered as 0 to 3. Each set includes 80 parameters, 10 parameters for each of the eight queues. The ten parameters are *green-min-threshold*, *yellow-min-threshold*, *red-min-threshold*, *green-max-threshold*, *yellow-max-threshold*, *red-max-threshold*, *green-max-prob*, *yellow-max-prob*, *red-max-prob* and *exponent*. Red, yellow and green packets respectively refer to those with drop precedence levels 2, 1 and 0.

Perform the following configurations in the specified views.

Table 172 Configure WRED parameters

Operation	Command
Enter WRED index view (system view)	wred <i>wred-index</i>
Restore the default WRED parameters (system view)	undo wred <i>wred-index</i>
Configure WRED parameters (WRED index view)	queue <i>queue-id</i> <i>green-min-threshold</i> <i>green-max-threshold</i> <i>green-max-prob</i> <i>yellow-min-threshold</i> <i>yellow-max-threshold</i> <i>yellow-max-prob</i> <i>red-min-threshold</i> <i>red-max-threshold</i> <i>red-max-prob</i> <i>exponent</i>
Restore the default WRED parameters (WRED index)	undo queue <i>queue-id</i>
Exit WRED index view (WRED index view)	quit

The command restores the parameters of the specified WRED index as the default setting. The command restores the WRED parameters related to the queue as the default setting.

The switch provides four sets of WRED parameters by default.



CAUTION: When multicast packets are sent through a certain port outbound queue, it is necessary to use the **queue** command to increase appropriately the length parameter of the corresponding queue where packets are all dropped to ensure the best effect of the replication capability of the egress port.

See the corresponding Command Manual for details of the commands.

Configuring drop algorithm

Please perform the following configurations in Ethernet port view.

Table 173 Configure drop algorithm

Operation	Command
Configure drop algorithm	drop-mode { tail-drop wred } [<i>wred-index</i>]
Restore the default algorithm	undo drop-mode

By default, tail drop mode is selected.

See the corresponding Command Manual for details of the commands.

Configuring Traffic Mirroring

Traffic mirroring duplicates the traffic that matches ACL rules to the CPU or the designated destination port, for traffic analysis and monitoring.

Perform the following configurations in Ethernet port view.

Table 174 Configure traffic mirroring

Operation	Command
Configure traffic mirroring which only applies IP group ACL	mirrored-to inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] { cpu interface <i>interface-type</i> <i>interface-number</i> }
Remove traffic mirroring setting which only applies IP group ACL	undo mirrored-to inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>]
Configure traffic mirroring which applies IP group ACL and link group ACL at same time	mirrored-to inbound ip-group { <i>acl-number</i> <i>acl-name</i> } { rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> } { cpu interface <i>interface-type</i> <i>interface-number</i> }
Remove traffic mirroring setting which applies IP group ACL and link group ACL at same time	undo mirrored-to inbound ip-group { <i>acl-number</i> <i>acl-name</i> } { rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> }
Configure traffic mirroring which only applies link group ACL	mirrored-to inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] { cpu interface <i>interface-type</i> <i>interface-number</i> }
Remove traffic mirroring setting which only applies link group ACL	undo mirrored-to inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>]



The **traffic-statistic** command is used to make statistics of traffic statistics information of all the ports in the port group. To display the traffic statistics information of the specified port, you must input the specific port information in the command line.

system-index *index* here is the system index for an ACL rule. When delivering a rule, the system assigns a globally unique index to it, for convenience of later retrieval. You can also assign a system index for it when delivering an ACL rule with this command, but the index value may change while the system is running. However, you are not recommended to assign a system index if not urgently necessary.

See the corresponding Command Manual for details of the commands.

Configuring Port Mirroring

Port mirroring duplicates data on the monitored port to the designated monitoring port, for purpose of data analysis and supervision. The switch supports multiple-to-one mirroring, that is, you can duplicate packets from multiple ports to a monitoring port.

You can also specify the monitoring direction:

- Only inbound packets
- Only outbound packets

Perform the following configurations in system view.

Table 175 Configure port mirroring

Operation	Command
Configure port mirroring	mirroring-group <i>groupid</i> { inbound outbound } <i>mirroring-port-list</i> mirrored-to <i>monitor-port</i>
Remove port mirroring setting	undo mirroring-group <i>groupid</i>

You can implement port mirroring configuration by setting mirroring groups at the port. Up to 20 mirroring groups can be configured at a port, with each group including one monitoring port and multiple monitored ports.



Switch 8800 Family series support cross-card mirroring, that is, the monitoring and monitored ports can be at different cards.

Consider these issues when configuring port mirroring:

- For intra-card mirroring, only one monitoring port can be configured for the mirroring groups in the same direction.
- For cross-card mirroring, only one monitoring port (which is on another card) can be configured for the mirroring groups in the same direction.
- You can only configure eight monitored ports for all the mirroring groups in transmit group.
- One port can act as mirroring port and mirrored port at the same time for different mirroring group.

More issues for the GV48 or GP48 card:

- For the mirroring (including incoming port mirroring and outgoing port mirroring) on the same GV48 or GP48 card, only one monitoring port is allowed.
- For all mirroring groups configured in the system, only one monitoring port is allowed on the same GV48 or GP48 card.

By default, two port groups of the XP4 card are created. The member ports are port 0-1 and port 2-3 respectively. Consider these issues when configuring port mirroring:

- The XP4 card does not support cross-group port mirroring, that is, the monitoring ports and monitored ports in the same port mirroring group can only be port 0 to 1 or port 2 to 3.
- You can configure an inbound monitoring port and an outbound monitoring port in a port group respectively. There is only one monitoring port in other types of interface cards.

See the corresponding Command Manual for details of the commands.

Configuring Traffic Statistics

Traffic statistics count packets of designated service traffic, that is, the packets match the defined ACL among those forwarded. You can view the information with the **display qos-interface traffic-statistic** command.

Perform the following configurations in Ethernet port.

Table 176 Configure traffic statistics

Operation	Command
Configure traffic statistics which only applies IP group ACL	traffic-statistic inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] [system-index <i>index</i>] [tc-index <i>index</i>]
Remove traffic statistics setting which only applies IP group ACL	undo traffic-statistic inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>]
Configure traffic statistics which only applies link group ACL	traffic-statistic inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] [system-index <i>index</i>] [tc-index <i>index</i>]
Remove traffic statistics setting which only applies link group ACL	undo traffic-statistic inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>]
Configure traffic statistics which applies IP group ACL and link group ACL	traffic-statistic inbound ip-group { <i>acl-number</i> <i>acl-name</i> } { rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } } [rule <i>rule</i>] [system-index <i>index</i>] link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> } [tc-index <i>index</i>]
Remove traffic statistics setting which applies IP group ACL and link group ACL	traffic-statistic inbound ip-group { <i>acl-number</i> <i>acl-name</i> } { rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } } [rule <i>rule</i>] [system-index <i>index</i>] link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> } [tc-index <i>index</i>]
Display the port traffic statistics information or the information of the rate at which traffics pass	display qos-interface [<i>interface-type</i> <i>interface-number</i>] traffic-statistic [rate [<i>timeinterval</i>]]

system-index index here is the system index for an ACL rule. When delivering a rule, the system assigns a globally unique index to it, for convenience of later retrieval. You can also assign a system index for it when delivering an ACL rule with this command, but the index value may change while the system is running. However, you are not recommended to assign a system index if not urgently necessary.

See the corresponding Command Manual for details of the commands.

Displaying and Debugging QoS Configuration

After these configurations are completed, you can use the **display** command in any view to view QoS running and check configuration result. You can clear QoS statistics using the **reset traffic-statistic** command in Ethernet port view.

Table 177 Display and debug QoS configurations

Operation	Command
Display traffic mirroring configuration of a port	display qos-interface [<i>interface-type</i> <i>interface-number</i>] mirrored-to
Display traffic priority configuration of a port	display qos-interface [<i>interface-type</i> <i>interface-number</i>] traffic-priority
Display traffic redirection configuration of a port	display qos-interface [<i>interface-type</i> <i>interface-number</i>] traffic-redirect
Display traffic statistics of a port	display qos-interface [<i>interface-type</i> <i>interface-number</i>] traffic-statistic
Display port mirroring configuration	display mirroring-group [<i>groupid</i>]

Table 177 Display and debug QoS configurations

Operation	Command
Display QoS configurations of all ports or the specified port	display qos-interface [<i>interface-type</i> <i>interface-number</i>] all
Display the drop mode of the port outbound queue	display qos-interface [<i>interface-type</i> <i>interface-number</i>] drop-mode
Display traffic limit configuration of a port	display qos-interface [<i>interface-type</i> <i>interface-number</i>] traffic-limit
Display queue scheduling configuration of a port	display qos-interface [<i>interface-type</i> <i>interface-number</i>] queue-scheduler
Display traffic shaping configuration of a port	display qos-interface [<i>interface-type</i> <i>interface-number</i>] traffic-shape
Display the parameter settings for traffic policing	display traffic-params [<i>traffic-index</i>]
Display QoS configuration of a VLAN	display qos-vlan [<i>vlan-id</i>] all
Display traffic priority configuration of a VLAN	display qos-vlan [<i>vlan-id</i>] traffic-priority
Display traffic limit configuration of a VLAN	display qos-vlan [<i>vlan-id</i>] traffic-limit
Display traffic direction configuration of a VLAN	display qos-vlan [<i>vlan-id</i>] traffic-redirect
Display traffic statistics of a VLAN	display qos-vlan [<i>vlan-id</i>] traffic-statistic
Display the DSCP + Conform-level -> Service parameter, EXP + Conform-level -> Service parameter and Local-precedence + Conform-level -> 802.1p priority mapping tables	display qos conform-level [<i>conform-level-value</i>] { dscp-policed-service-map [<i>dscp-list</i>] exp-policed-service-map local-precedence-cos-map }
Display the CoS -> Drop-precedence mapping table	display qos cos-drop-precedence-map
Display the CoS -> Local-precedence mapping table	display qos cos-local-precedence-map
Clear traffic statistics	reset traffic-statistic inbound { { ip-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } }* { ip-group { <i>acl-number</i> <i>acl-name</i> } link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> }* ip-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> link-group { <i>acl-number</i> <i>acl-name</i> } rule <i>rule</i> } }

See the corresponding Command Manual for description of display information and parameters.

QoS Configuration Example

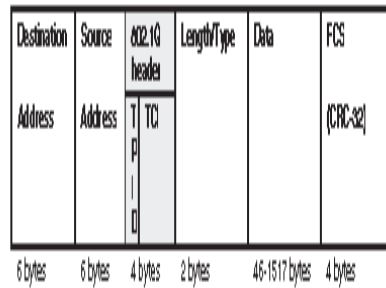
Traffic Shaping Configuration Example

Network requirements

Set traffic shaping for the outbound queue 2 at the port GE7/1/8, with the maximum rate of 650 Kbps and the burst size of 12 KB.

Network diagram

Figure 47 Network diagram for QoS configuration



Configuration procedure

Enter Ethernet port view.

```
[SW8800] interface GigabitEthernet 7/1/8
[3Com-GigabitEthernet7/1/8]
```

Set traffic shaping for the outbound queue 2 at the port: maximum rate 650 Kbps, burst size 12 KB.

```
[3Com-GigabitEthernet7/1/8] traffic-shape queue 2 650 12
```

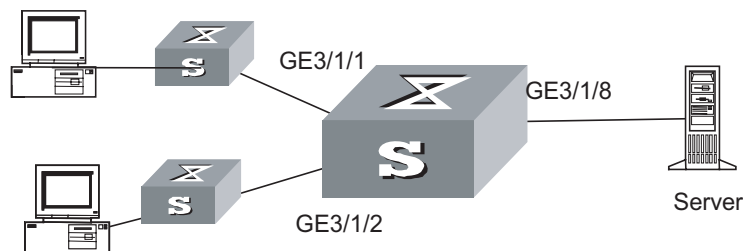
Port Mirroring Configuration Example

Network requirements

Use one server to monitor the packets of two ports. R&D department is accessed from the port GE3/1/1 and sales department from the port GE3/1/2. The server is connected to the port GE3/1/8.

Network diagram

Figure 48 Networking for port mirroring configuration



Configuration procedure

Define a mirroring group, with monitoring port as GigabitEthernet3/1/8.

```
[SW8800] mirroring-group 1 inbound gigabitethernet3/1/1 gigabitethernet3/1/2
mirrored-to gigabitethernet3/1/8
[SW8800] mirroring-group 2 outbound gigabitethernet3/1/1 gigabitethernet3/1/2
mirrored-to gigabitethernet3/1/8
```

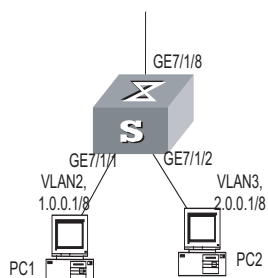
Traffic Priority Configuration Example

Network requirements

Re-allocate service parameters according to the mapping table for DSCP 63 for the packets from PC 1 (IP 1.0.0.1) during the time range 8:00 to 18:00 everyday.

Network diagram

Figure 49 Network diagram for priority configuration



Configuration procedure

- 1 Define the time range.

Define the time range from 8:00 to 18:00.

```
[SW8800] time-range 3Com 8:00 to 18:00 daily
```

- 2 Define the traffic from PC1.

Create a number-based basic ACL 2000 and enter it.

```
[SW8800] acl number 2000
```

Define ACL rule for the traffic from PC1.

```
[3Com-acl-basic-2000] rule 0 permit source 1.0.0.1 0 time-range 3Com
```

- 3 Define the CoS-> Conform-Level mapping table.

Define the CoS-> Conform-Level mapping table. The switch allocates drop precedence (all as 0 for the sake of simplification) for them when receiving packets.

```
[SW8800] qos cos-drop-precedence-map 0 0 0 0 0 0 0 0
```

The modified CoS-> Conform-Level mapping table:

Table 178 Modified CoS-> Conform-Level mapping table

CoS Value	Drop-precedence
0	0
1	0
2	0
3	0
4	0
5	0

Table 178 Modified CoS-> Conform-Level mapping table

CoS Value	Drop-precedence
6	0
7	0

4 Define the DSCP + Conform-Level -> Service parameter mapping table.

Define the DSCP + Conform-Level -> Service parameter mapping table. Allocate a set of service parameters for the packets from PC1 according the mapping table for DSCP 63.

```
[SW8800] qos conform-level 0
[3Com-conform-level-0] dscp 63 : 32 4 4 4 0
```

The modified DSCP + Conform-Level -> Service parameter mapping table:

Table 179 Modified DSCP + Conform-Level -> Service parameter mapping table

DSCP	CL	Policed-DSCP	Policed-exp	Policed-802.1p	Policed-Localprec	Policed-Drop Precedence
63	0	32	4	4	4	0

5 Re-allocate service parameters for the packets from PC1.

Re-allocate service parameters for the packets from PC1.

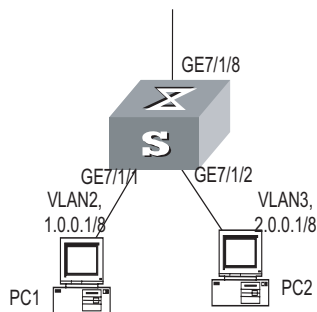
```
[3Com-GigabitEthernet7/1/1] traffic-priority inbound ip-group 2000
remark-policed-service dscp 63
```

Traffic Redirection Configuration Example

Network requirements

Forward the packets sent from PC1 (IP 1.0.0.1) during the time range from 8:00 to 18:00 every day to the address 2.0.0.1.

Network diagram

Figure 50 Network diagram for traffic redirection configuration

Configuration procedure

1 Define the time range.

Define the time range from 8:00 to 18:00.

```
[SW8800] time-range 3Com 8:00 to 18:00 daily
```

2 Define the traffic from PC1.

```
# Create a number-based basic ACL 2000 and enter it.
```

```
[SW8800] acl number 2000
```

```
# Define ACL rule for the traffic from PC1.
```

```
[3Com-acl-basic-2000] rule 0 permit source 1.0.0.1 0 time-range 3Com
```

3 Modify the next hop for the packets from PC1.

```
# Define the next hop for the packets from PC1 as 2.0.0.1.
```

```
[3Com-GigabitEthernet7/1/1] traffic-redirect inbound ip-group 2000 rule 0
next-hop 2.0.0.1
```

Queue Scheduling Configuration Example

Network requirements

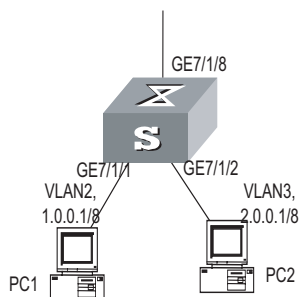
Modify the correspondence between 802.1p priority levels and local priority levels to change the mapping between 802.1p priority levels and queues. That is, put packets into outbound queues according to the new mapping. Use WRR algorithm for the queues 0 to 5 at the port GE7/1/1. Set the queues 0, 1 and 2 into WRR queue 1, with weight respectively as 20, 20 and 30; set the queues 3, 4 and 5 into WRR queue 2, with weight respectively as 20, 20 and 40. The queues 6 and 7 use SP algorithm. See Queue Scheduling for the default mapping.

Table 180 802.1p priority -> Local precedence mapping table

802.1p priority	Local precedence
0	7
1	6
2	5
3	4
4	3
5	2
6	1
7	0

Network diagram

Figure 51 Network diagram for queue-schedule configuration



Configuration procedure

Re-specify the mapping between 802.1p priority and local precedence.

```
[SW8800] qos cos-local-precedence-map 7 6 5 4 3 2 1 0
```

Use WRR algorithm for the queues 0 to 5. Set the queues 0, 1 and 2 into WRR queue 1, with weight respectively as 20, 20 and 30; set the queues 3, 4 and 5 into WRR queue 2, with weight respectively as 20, 20 and 40. Use SP algorithm for the queues 6 and 7.

```
[3Com-GigabitEthernet7/1/1] queue-scheduler wrr group1 0 20 1 20 2 30 group2
3 20 4 20 5 40
```

```
[SW8800] display qos-interface GigabitEthernet7/1/1 queue-scheduler
```

GigabitEthernet7/1/1 Port scheduling:

QID:	scheduling-group	weight
0 :	wrr , group1	20
1 :	wrr , group1	20
2 :	wrr , group1	30
3 :	wrr , group2	20
4 :	wrr , group2	20
5 :	wrr , group2	40
6 :	sp	0
7 :	sp	0

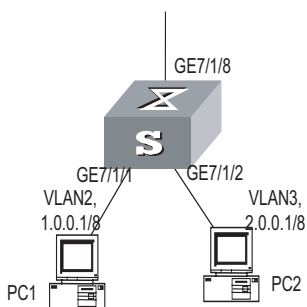
WRED Parameters Configuration Example

Network requirements

Set WRED parameters and drop algorithm for packets at the port GE7/1/1: Configure parameters for WRED 0; outbound queue ID is 7; *green-min-threshold* is 150; *green-max-threshold* is 500; *green-max-prob* is 5; *yellow-min-threshold* is 100; *yellow-max-threshold* is 150; *yellow-max-prob* is 10; *red-min-threshold* is 50; *red-max-threshold* is 100; *red-max-prob* is 15; *exponent* is 10; the port is in WRED drop mode; import the parameters of WRED 0.

Network diagram

Figure 52 Network diagram for WRED parameters configuration



Configuration procedure

1 Configure WRED parameters

Configure parameters for WRED 0.

```
[SW8800] wred 0
```

```
[3Com-wred-0] queue 7 150 500 5 100 150 10 50 100 15 10
```

2 Set drop algorithm and thresholds.

Define the port GE7/1/1 in WRED drop mode, set the parameters of WRED 0.

```
[3Com-GigabitEthernet7/1/1] drop-mode wred 0
```

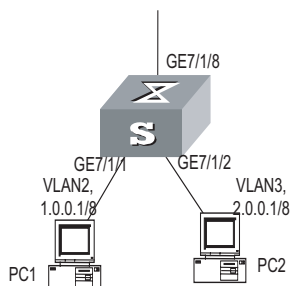
Traffic Statistics Configuration Example

Network requirements

Suppose the IP address of PC1 is 1.0.0.1 and that of PC2 is 2.0.0.1. The switch is up-linked through the port GE7/1/8. Count the packets sent from the switch to PC1 during the time range from 8:00 to 18:00 every day.

Network diagram

Figure 53 Network diagram for traffic statistics configuration



Configuration procedure

1 Define the time range.

Define the time range from 8:00 to 18:00.

```
[SW8800] time-range 3Com 8:00 to 18:00 daily
```

2 Define the traffic from PC1.

Define ACL rule for the traffic from PC1.

```
[SW8800] acl number 2000
[3Com-acl-basic-2000] rule 0 permit source 1.0.0.1 0.0.0.0 time-range 3Com
```

3 Count the packets to PC1 and display the result using the **display** command.

```
[3Com-GigabitEthernet7/1/1] traffic-statistic inbound ip-group 2000 rule 0
[SW8800] display qos-interface GigabitEthernet7/1/1 traffic-statistic
GigabitEthernet7/1/1: traffic-statistic
Inbound:
  Matches: Acl 2000 rule 0 running
           12002688 bytes (green 1270244416 byte(s), yellow 1895874880 byte(s),
           red 704683968 byte(s) )
           3333270 packets (green 0 byte(s), yellow 0 byte(s), red 0 byte(s) )
```


23

LOGON USER ACL CONTROL CONFIGURATION

Overview

Currently, an Switch 8800 Family series switch provides the following three measures for remote access:

- Telnet
- Security shell (SSH)
- Simple network management protocol (SNMP)

An Switch 8800 Family series switch provides security control for these three access measures to prevent unauthorized users from logging in/and accessing it. There are two levels of security controls.

- The first level is implemented by applying ACLs to filter the users that are to connect to the switch. Only authorized users are capable of accessing the switch.

At the second level, a connected user can log into the switch only after passing the password authentication.

This chapter mainly describes how to configure the first level security control over these access measures, that is, how to filter the users logging onto the switch with ACL. For detailed description about how to configure the second level security, refer to the Getting Started part of this manual.

Configuring ACL for Telnet/SSH Users

You can configure ACLs for the users who access the switch through Telnet or SSH to filter out the malicious or unauthorized connection requests before the password authentication to secure the switch.

Configuration Prerequisites

You have correctly configured the switch using Telnet or SSH.

Configuration Tasks

Table 181 Configuration tasks

Configuration procedure	Command	Description
Enter system view	system-view	-
Define an ACL and enter ACL view	acl number <i>acl-number</i> [match-order { config auto }]	Required. The command can only define a number-identified ACL

Table 181 Configuration tasks

Configuration procedure		Command	Description
	Basic ACL view	rule [<i>rule-id</i>] { permit deny } [source { <i>source-addr wildcard</i> any }] [fragment time-range <i>name</i> vpn-instance <i>instance-name</i>]*	
	Advanced ACL view	rule [<i>rule-id</i>] { permit deny } <i>protocol</i> [source { <i>source-addr wildcard</i> any }] [destination { <i>dest-addr wildcard</i> any }] [source-port <i>operator port1</i> [<i>port2</i>]] [destination-port <i>operator port1</i> [<i>port2</i>]] [icmp-type <i>type code</i>] [established] [precedence <i>precedence</i> tos <i>tos</i>]* dscp <i>dscp</i>] [fragment] [bt-flag] [time-range <i>name</i>] [vpn-instance <i>instance-name</i>]	When Telnet and SSH users use basic and advanced ACLs, only the parameters <i>source-addr</i> and the <i>wildcard</i> , <i>dest-addr</i> and the <i>wildcard</i> parameter, and the time-range keyword in the command are valid.
	Define rules	rule [<i>rule-id</i>] { permit deny } [cos <i>cos-value</i> c-tag-cos <i>c-cos-value</i> exp <i>exp-value</i> <i>protocol-type</i> mac-type { any-broadcast-packet arp-broadcast-packet non-arp-broadcast-packet { unicast-packet multicast-packet }] [known unknown] }] [ingress { { <i>source-vlan-id</i> <i>source-vlan-id-end</i> } <i>source-mac-addr</i> <i>source-mac-wildcard</i> c-tag-vlan <i>c-tag-vlanid</i> }* any }] [egress { <i>dest-mac-addr</i> <i>dest-mac-wildcard</i> any }] [s-tag-vlan <i>s-tag-vlanid</i> time-range <i>name</i>]*	
	Layer 2 ACL view	rule [<i>rule-id</i>] { permit deny } [cos <i>cos-value</i> c-tag-cos <i>c-cos-value</i> exp <i>exp-value</i> <i>protocol-type</i> mac-type { any-broadcast-packet arp-broadcast-packet non-arp-broadcast-packet { unicast-packet multicast-packet }] [known unknown] }] [ingress { { <i>source-vlan-id</i> <i>source-vlan-id-end</i> } <i>source-mac-addr</i> <i>source-mac-wildcard</i> c-tag-vlan <i>c-tag-vlanid</i> }* any }] [egress { <i>dest-mac-addr</i> <i>dest-mac-wildcard</i> any }] [s-tag-vlan <i>s-tag-vlanid</i> time-range <i>name</i>]*	When Telnet and SSH users use an Layer 2 ACL, only the <i>source-mac-addr</i> and the <i>source-mac-wildcard</i> parameter, and the time-range keyword in the command are valid.
	Exit ACL view	quit	-
	Enter user interface view	user-interface [<i>type</i>] <i>first-number</i>	-
Apply ACLs to restrict inbound/outbound requests of Telnet or SSH users	Apply basic or advanced ACLs	acl <i>acl-number1</i> { inbound outbound }	The <i>acl-number1</i> parameter indicates the number of the basic or advanced ACLs, in the range of 2,000 to 3,999.
	Apply Layer 2 ACLs	acl <i>acl-number2</i> inbound	The <i>acl-number2</i> parameter indicates the number of the Layer 2 ACL, in the range of 4,000 to 4,999.

By default, the system does not restrict incoming/outgoing requests.



- You can only use number-based ACLs to implement the ACL control to Telnet or SSH users.
- When you use the basic or advanced ACL to implement the ACL control to Telnet or SSH users, the incoming/outgoing requests are restricted based on the source or destination IP addresses. Therefore, only the *source-addr* and the *wildcard*, and *dest-addr* and the *wildcard* parameters, and the **time-range** keyword in the corresponding command are valid. Similarly, when you use the Layer 2 ACL to implement the ACL control to the Telnet or SSH users, the incoming/outgoing requests are restricted based on the source MAC address. Therefore, only the *source-mac-addr* and the *source-mac-wildcard* parameters, and the **time-range** keyword in the corresponding command are valid.
- When you use Layer 2 ACLs to implement the ACL control to the Telnet or SSH users, only incoming requests are restricted.
- If a user fails to log in due to ACL restriction, the system logs the user failure, including the IP address, login method, user interface index value and failure reason.

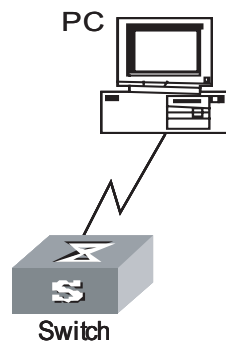
Layer 2 ACL Control Configuration Example

Network requirements

Only the Telnet users with source MAC addresses 00e0-fc01-0101 and 00e0-fc01-0303 are allowed to access the switch.

Network diagram

Figure 54 Network diagram for source MAC address control over Telnet users



Configuration procedure

Define an Layer 2 ACL.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] acl number 4000 match-order config
```

Define rules.

```
[3Com-acl-link-4000] rule 1 permit ingress 00e0-fc01-0101 0000-0000-0000 [3Com-acl-link-4000] rule 2 permit ingress 00e0-fc01-0303 0000-0000-0000
[3Com-acl-link-4000] rule 3 deny ingress any
[3Com-acl-link-4000] quit
```

Enter user interface view

```
[SW8800] user-interface vty 0 4

# Apply the Layer 2 ACL to restrict incoming requests.

[3Com-user-interface-vty0-4] acl 4000 inbound
```

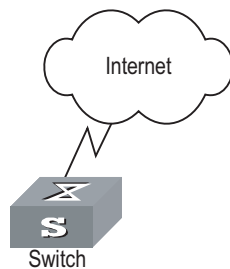
Basic ACL Control Configuration Example

Network requirements

Only the Telnet users with IP addresses of 10.110.100.52 and 10.110.100.46 can access the switch.

Network diagram

Figure 55 Network diagram for source IP control over Telnet users



Configuration procedure

Define a basic ACL.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] acl number 2000 match-order config
```

Define rules.

```
[3Com-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[3Com-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[3Com-acl-basic-2000] rule 3 deny source any
[3Com-acl-basic-2000] quit
```

Enter user interface view.

```
[SW8800] user-interface vty 0 4
```

Apply the ACL.

```
[3Com-user-interface-vty0-4] acl 2000 inbound
```

Configuring ACL for SNMP Users

Switch 8800 Family series switches can be managed remotely through network management software (NMS). Administrators can use SNMP to access an Switch 8800 Family series switch. Proper ACL configuration can prevent unauthorized network management users from logging onto the switch.

Configuration Prerequisites

You have correctly configured log into the switch using SNMP.

Configuration Tasks

Table 182 Configuration tasks

Configuration procedure	Command	Description
Enter system view	system-view	-
Define an ACL and enter ACL view	acl number <i>acl-number</i> [match-order { config auto }]	Required. This command can only define a number-based basic ACL. The <i>acl-number</i> parameter ranges from 2,000 to 2,999.
Define basic ACL rules	rule [<i>rule-id</i>] { permit deny } [source { <i>source-addr wildcard</i> any }] fragment time-range <i>name</i> vpn-instance <i>instance-name</i>]*	Required
Exit ACL view	quit	-
Apply the ACL in the snmp-agent community command	snmp-agent community { read write } <i>community-name</i> [mib-view <i>view-name</i>] [acl <i>acl-number</i>]	The SNMP community name is a feature of SNMP V1 and SNMP V2. Applying an ACL in the snmp-agent community command filters the network management systems based on SNMP V1 and SNMP V2.
Apply the ACL to control SNMP users	snmp-agent group { v1 v2c } <i>group-name</i> [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-number</i>] snmp-agent group v3 <i>group-name</i> [authentication privacy] [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-number</i>] snmp-agent usm-user { v1 v2c } <i>user-name</i> <i>group-name</i> [acl <i>acl-number</i>]	The SNMP group and user name are features of SNMP V2 and later. Applying ACLs in the snmp-agent group , snmp-agent group v3 , snmp-agent usm-user , and snmp-agent usm-user v3 commands filters the network management systems based on SNMP V2 and later.
Import the ACL into the snmp-agent usm-user command	snmp-agent usm-user v3 <i>user-name</i> <i>group-name</i> [authentication-mode { md5 sha } <i>auth-password</i>] [privacy-mode des56 <i>priv-password</i>] [acl <i>acl-number</i>]	If you apply ACLs in these two groups of commands simultaneously, the switch filters network management users according to the both features.



- you can apply different ACLs in the **snmp-agent community**, **snmp-agent group** and **snmp-agent usm-use** commands.
- You can only apply number-based basic ACLs to implement ACL control over SNMP users.

For the detailed description of these commands, refer to the *Command Manual*.

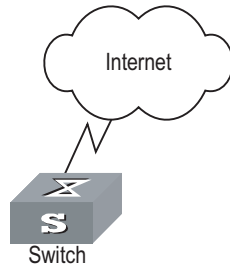
ACL Control over SNMP Users Configuration Example

Network requirements

Only SNMP users from 10.110.100.52 and 10.110.100.46 can access the switch.

Network diagram

Figure 56 Network diagram for ACL control over SNMP users



Configuration procedure

Define a basic ACL and the rules.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] acl number 2000 match-order config
[3Com-acl-baisc-2000] rule 1 permit source 10.110.100.52 0
[3Com-acl-baisc-2000] rule 2 permit source 10.110.100.46 0
[3Com-acl-basic-2000] rule 3 deny source any
[3Com-acl-baisc-2000] quit
```

Apply the ACL.

```
[SW8800] snmp-agent community read 3Com acl 2000
[SW8800] snmp-agent group v3 3Comgroup acl 2000
[SW8800] snmp-agent usm-user v3 3Comuser 3Comgroup acl 2000
```

24

VLAN-ACL CONFIGURATION

VLAN-ACL Overview

VLAN-ACL is VLAN-based ACL. You can configure QACL for a VLAN to control accesses made to all ports in the VLAN.

VLAN-ACL enables you to manage a network in an easier way. After you configure QACL for a VLAN, the system synchronizes the configuration to all member ports in the VLAN automatically. Therefore you need not to configure QACL for every port.

VLAN-ACL Configuration

Configuration Prerequisites

The VLAN for which you configure QACL must meet the following requirements:

- The VLAN has member ports.
- The VLAN has no MPLS intermixing ports.
- The default flow template is applied to ports in the VLAN.

Configuring a VLAN-ACL

Table 183 Configure a VLAN-ACL

Configuration step	Command	Description
Enter system view	system-view	-
Create an ACL and enter the corresponding view	acl { number <i>acl-number</i> name <i>acl-name</i> [advanced basic] } [match-order { config auto }]	Only basic or advanced ACL and the rules are applicable to VLAN-ACL.
Define a rule	rule	Required
Quit ACL view	quit	-
Enter VLAN view	vlan <i>vlan-id</i>	VLAN-ACL is prohibited from being applied to the VLAN containing MPLS intermixing ports.
Configure packet filtering (activating ACLs)	packet-filter inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]]	Optional
Configure traffic policing	traffic-limit inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] [tc-index <i>index</i>] { traffic-index <i>traffic-index</i> <i>cir cbs ebs</i> [<i>pir</i>] } { conform { remark-cos remark-policed-service } exceed { forward drop } }*	Optional

Table 183 Configure a VLAN-ACL

Configuration step	Command	Description
Tag priority for packets	traffic-priority inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] { auto remark-policed-service { trust-dscp dscp <i>dscp-value</i> untrusted dscp <i>dscp-value</i> cos <i>cos-value</i> local-precedence <i>local-precedence</i> drop-priority <i>drop-level</i> } }	Optional
Configure packet redirection	traffic-redirect inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] { cpu next-hop <i>ip-addr1</i> [<i>ip-addr2</i>] [invalid { forward drop } } }	Optional When executed in VLAN view, the traffic-redirect command only redirects packets to the next hop and CPU instead of ports or service processor cards. In this case, the nested-vlan or modified-vlan keyword are not supported.
Configure traffic mirroring	mirrored-to inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] cpu	Optional
Configure traffic statistics	traffic-statistic inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] [tc-index <i>index</i>]	Optional
Quit VLAN view	quit	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	The port type can only be Ethernet.
Synchronize manually QACL configuration to specified ports	port can-access vlan-acl vlan <i>vlan-id</i>	Optional
View the ports to which the VLAN-ACL configuration is synchronized in the VLAN	display vlan-acl-member-ports vlan <i>vlan-id</i>	You can use this command in any view.

The VLAN-ACL configuration is subject to the following limitations:

1 Limitations on flow templates:

- The system only applies VLAN-ACL to ports with the default flow template applied. The applied ACL rule field must be specified by the default flow template.
- If no port in a VLAN has ACL rules applied to, the system checks all ports in the VLAN when applying an ACL rule in VLAN view and prohibits the ACL rule from being applied if a port in the VLAN has a customized flow template applied to.
- If a VLAN-ACL is applied to some of the ports in a VLAN, a port with a customized flow template applied to can be added to the VLAN. But the system will fail to apply the VLAN-ACL to the newly added port. That is, you can apply the VLAN-ACL in VLAN view to all the ports in the VLAN except the

newly added one. However, if the port delete the self-defined flow template, the system will apply QACL rules in the VLAN to the new port automatically.

- You will fail to change the flow template applied to a port with a VLAN-ACL already applied to a customized flow template.
- 2 If both a VLAN and one of its ports have QACL rules applied, only those applied to the port work. In this case, the VLAN-ACL takes effect only after the QACL rules and the self-defined flow template on the port are deleted.
 - 3 When the VLAN contains no ports, the system is prohibited from applying VLAN-ACL (including adding and deleting rules).
 - 4 Two ports differing in VLAN-ACL configuration cannot be aggregated dynamically.
 - 5 A VLAN-ACL is prohibited from being applied to a VLAN containing intermixing ports. Similarly, a VLAN with a VLAN-ACL applied to is prohibited from being used for MPLS intermixing.



CAUTION: VLAN-ACL does not take effect on the ports of the XP4 card.

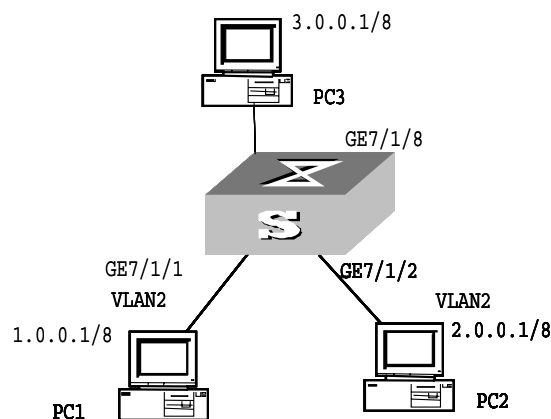
VLAN-ACL Configuration Example

Network requirements

Set the next hop IP address of all the packets forwarded by GigabitEthernet7/1/1 and GigabitEthernet7/1/2 ports from 8:00 to 18:00 every day to 3.0.0.1.

Network diagram

Figure 57 Network diagram for VLAN-ACL configuration



Configuration procedure

- 1 Define the time range.

Define the time range from 8:00 to 18:00.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] time-range 3Com 8:00 to 18:00 daily
```

- 2 Define traffic rules.

Create ACL 2000 and enter the corresponding view.

```
[SW8800] acl number 2000
```

Define traffic classification rules for packets , and allow packets to pass during the specified time period.

```
[3Com-acl-basic-2000] rule 0 permit source any time-range 3Com
[3Com-acl-basic-2000] quit
```

3 Configure packet redirection in VLAN 2.

Set the next hop IP addresses of all the packets forwarded on ports in VLAN 2 to 3.0.0.1.

```
[SW8800] vlan 2
[3Com-vlan2] traffic-redirect inbound ip-group 2000 rule 0 next-hop
3.0.0.1
```

4 View configuration.

View whether VLAN-ACL is configured on all ports in VLAN 2 (ports GigabitEthernet7/1/1 and GigabitEthernet7/1/2).

```
[3Com-vlan2] display vlan-acl-member-ports vlan 2
Vlan-acl member port(s):
    GigabitEthernet7/1/1      GigabitEthernet7/1/2
```


25

802.1X CONFIGURATION

802.1x Overview

802.1x Standard Overview

IEEE 802.1x (hereinafter simplified as 802.1x) is a port-based network access control protocol that is used as the standard for LAN user access authentication.

In the LANs complying with the IEEE 802 standards, the user can access the devices and share the resources in the LAN through connecting the LAN access control device like the LAN Switch. However, in telecom access, commercial LAN (a typical example is the LAN in the office building) and mobile office etc., the LAN providers generally hope to control the user's access. In these cases, the requirement on the above-mentioned "Port Based Network Access Control" originates.

As the name implies, "Port Based Network Access Control" means to authenticate and control all the accessed devices on the port of LAN access control device. If the user's device connected to the port can pass the authentication, the user can access the resources in the LAN. Otherwise, the user cannot access the resources in the LAN. It equals that the user is physically disconnected.

802.1x defines port based network access control protocol and only defines the point-to-point connection between the access device and the access port. The port can be either physical or logical. The typical application environment is as follows: Each physical port of the LAN Switch only connects to one user workstation (based on the physical port) and the wireless LAN access environment defined by the IEEE 802.11 standard (based on the logical port), etc.

802.1x System Architecture

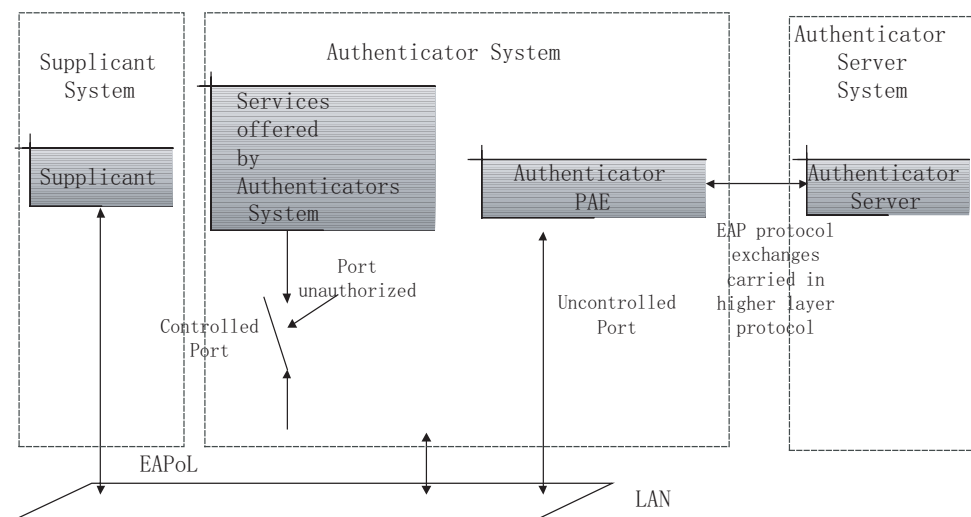
The system using the 802.1x is the typical C/S (Client/Server) system architecture. It contains three entities, which are illustrated in Figure 58: Supplicant System, Authenticator System and Authentication Sever System.

The LAN access control device needs to provide the Authenticator System of 802.1x. The devices at the user side such as the computers need to be installed with the 802.1x client Supplicant software, for example, the 802.1x client provided by 3Com Corporation Co., Ltd. (or by Microsoft Windows XP). The 802.1x Authentication Sever system normally stays in the carrier's AAA center.

Authenticator and Authentication Sever exchange information through EAP (Extensible Authentication Protocol) frames. The Supplicant and the Authenticator exchange information through the EAPoL (Extensible Authentication Protocol over LANs) frame defined by IEEE 802.1x. Authentication data are encapsulated in the EAP frame, which is to be encapsulated in the packets of other AAA upper layer protocols (e.g. RADIUS) so as to go through the complicated network to reach the Authentication Server. Such procedure is called EAP Relay.

There are two types of ports for the Authenticator. One is the Uncontrolled Port, and the other is the Controlled Port. The Uncontrolled Port is always in bi-directional connection state. The user can access and share the network resources any time through the ports. The Controlled Port will be in connecting state only after the user passes the authentication. Then the user is allowed to access the network resources.

Figure 58 802.1x system architecture



802.1x Authentication Process

802.1x configures EAP frame to carry the authentication information. The Standard defines the following types of EAP frames:

- EAP-Packet: Authentication information frame, used to carry the authentication information.
- EAPoL-Start: Authentication originating frame, actively originated by the Supplicant.
- EAPoL-Logoff: Logoff request frame, actively terminating the authenticated state.
- EAPoL-Key: Key information frame, supporting to encrypt the EAP packets.
- EAPoL-Encapsulated-ASF-Alert: Supports the Alerting message of Alert Standard Forum (ASF).

The EAPoL-Start, EAPoL-Logoff and EAPoL-Key only exist between the Supplicant and the Authenticator. The EAP-Packet information is re-encapsulated by the Authenticator System and then transmitted to the Authentication Server System. The EAPoL-Encapsulated-ASF-Alert is related to the network management information and terminated by the Authenticator.

802.1x provides an implementation solution of user ID authentication. However, 802.1x itself is not enough to implement the scheme. The administrator of the access device should configure the AAA scheme by selecting RADIUS or local authentication so as to assist 802.1x to implement the user ID authentication. For detailed description of AAA, refer to the "AAA&RADIUS&HWTAWACS" part in this document.

Implementing 802.1x on Ethernet Switches

3Com Series Ethernet Switches not only support the port access authentication method regulated by 802.1x, but also extend and optimize it in the following way:

- Support to connect several End Stations in the downstream via a physical port.
- The access control (or the user authentication method) can be based on port or MAC address.

In this way, the system becomes much securer and easier to manage.

802.1x Configuration

The configuration tasks of 802.1x itself can be fulfilled in system view of the Ethernet switch. After the global 802.1x is enabled, the user can configure the 802.1x state of the port. The configured items will take effect after the global 802.1x is enabled.



*When 802.1x is enabled on a port, the max number of MAC address learning which is configured by the command **mac-address max-mac-count** cannot be configured on the port, and vice versa.*

The following sections describe 802.1x configuration tasks.

- "Enabling/Disabling 802.1x"
- "Setting the Port Access Control Mode"
- "Setting Port Access Control Method"
- "Checking the Users that Log on the Switch via Proxy"
- "Setting Supplicant Number on a Port"
- "Setting the Authentication in DHCP Environment"
- "Configuring Authentication Method for 802.1x User"
- "Configuring Guest VLAN"
- "Setting the Maximum times of authentication request message retransmission"
- "Configuring 802.1x Timers"
- "Enabling/Disabling Quiet-Period Timer"

Among the above tasks, the first one "enabling 802.1x" is compulsory; otherwise 802.1x will not take any effect. The other tasks are optional. You can perform the configurations at requirements.

Enabling/Disabling 802.1x

The following command can be used to enable/disable the 802.1x on the specified port or globally. When it is used in system view, if the parameter *interface-list* is not specified, 802.1x will be globally enabled. If the parameter *interface-list* is specified, 802.1x will be enabled on the specified port. When this command is used in Ethernet port view, other ports cannot be specified and 802.1x can only be enabled on the current port.

Perform the following configuration in system view or Ethernet port view.

Table 184 Enable/Disable 802.1x

Operation	Command
Enable the 802.1x	dot1x [interface <i>interface-list</i>]
Disable the 802.1x	undo dot1x [interface <i>interface-list</i>]

By default, 802.1x authentication has not been enabled globally and on any port.

You cannot enable 802.1x on a port before you enable it globally. And you must disable 802.1x on each port before you disable 802.1x globally.

Setting the Port Access Control Mode

The following commands can be used for setting 802.1x access control mode on the specified port. When no port is specified, the access control mode of all ports is configured.

Perform the following configuration in system view or Ethernet port view.

Table 185 Set the port access control mode

Operation	Command
Set the port access control mode	dot1x port-control { authorized-force unauthorized-force auto } [interface <i>interface-list</i>]
Restore the default access control mode of the port	undo dot1x port-control [interface <i>interface-list</i>]

auto (automatic identification mode, which is also called protocol control mode). That is, the initial state of the port is unauthorized. It only permits EAPoL packets receiving/transmitting and does not permit the user to access the network resources. If the authentication flow is passed, the port will be switched to the authorized state and permit the user to access the network resources.

The **authorized-force** keyword specifies the port to operate in authorized-force mode. Ports in this mode are always authorized. Users can access a network through this kind of port without being authorized.

The **unauthorized-force** keyword specifies the port to operate in unauthorized-force mode. Ports in this mode are always unauthorized. They do not respond to authorization requests. Users cannot access a network through this kind of port.

By default, the mode of 802.1x performing access control on the port is **auto** (automatic identification mode).

Setting Port Access Control Method

The following commands are used for setting 802.1x access control method on the specified port. When no port is specified in system view, the access control method of all ports is configured.

Perform the following configuration in system view or Ethernet port view.

Table 186 Set port access control method

Operation	Command
Set port access control method	dot1x port-method { macbased portbased } [interface <i>interface-list</i>]
Restore the default port access control method	undo dot1x port-method [interface <i>interface-list</i>]

The **macbased** keyword specifies to authenticate each user accessing through the port. And disconnection of a user does not affect other users. Whereas if you specify the **portbased** keyword, users can access a network without being authenticated if a user passes the authentication previously. But these users are denied when the one who passes the authentication first goes offline.

By default, 802.1x authentication method on the port is **macbased**. That is, authentication is performed based on MAC addresses.



*Without NMM Application Module, the system cannot perform traffic statistics for **macbased** users. Because the system performs traffic statistics only for ports instead of multiple users connecting with the same port, the system can perform traffic statistics only for **portbased** users.*

Checking the Users that Log on the Switch via Proxy

The following commands are used for checking the users that log on the switch via proxy.

Perform the following configuration in system view or Ethernet port view.

Table 187 Check the users that log on the switch via proxy

Operation	Command
Enable the check for access users via proxy	dot1x supp-proxy-check { logoff trap } [interface <i>interface-list</i>]
Cancel the check for access users via proxy	undo dot1x supp-proxy-check { logoff trap } [interface <i>interface-list</i>]

These commands take effect on the ports specified by the *interface-list* parameter when executed in system view. The parameter *interface-list* cannot be input when the command is executed in Ethernet Port view and it has effect only on the current interface. After globally enabling proxy user detection and control in system view, only if you enable this feature on a specific port can this configuration take effects on the port.

Setting Supplicant Number on a Port

The following commands are used for setting number of users allowed by 802.1x on specified port. When no port is specified, all the ports accept the same number of supplicants.

Perform the following configuration in system view or Ethernet port view.

Table 188 Setting maximum number of users via specified port

Operation	Command
Set maximum number of users via specified port	dot1x max-user <i>user-number</i> [interface <i>interface-list</i>]

Table 188 Setting maximum number of users via specified port

Operation	Command
Restore the maximum number of users on the port to the default value	undo dot1x max-user [interface interface-list]

By default, 802.1x allows up to 1024 supplicants on each port for 3Com Switch 8800 Family Series Routing Switches (hereinafter referred to as Switch 8800 Family series), and an Switch 8800 Family series routing switch can accommodate total of 2048 supplicants.

Setting the Authentication in DHCP Environment

If in DHCP environment the users configure static IP addresses, you can set 802.1x to disable the switch to trigger the user ID authentication over them with the following command.

Perform the following configuration in system view.

Table 189 Set the Authentication in DHCP Environment

Operation	Command
Disable the switch to trigger the user ID authentication over the users who configure static IP addresses in DHCP environment	dot1x dhcp-launch
Enable the switch to trigger the authentication over them	undo dot1x dhcp-launch

By default, the switch can trigger the user ID authentication over the users who configure static IP addresses in DHCP environment.

Configuring Authentication Method for 802.1x User

The following commands can be used to configure the authentication method for 802.1x user. Three kinds of methods are available: PAP authentication (RADIUS server must support PAP authentication), CHAP authentication (RADIUS server must support CHAP authentication), EAP relay authentication (switch send authentication information to RADIUS server in the form of EAP packets directly and RADIUS server must support EAP authentication).

Perform the following configuration in system view.

Table 190 Configure authentication method for 802.1x user

Operation	Command
Configure authentication method for 802.1x user	dot1x authentication-method { chap pap eap md5-challenge}
Restore the default authentication method for 802.1x user	undo dot1x authentication-method

By default, CHAP authentication is used for 802.1x user authentication.



When you are configuring authentication methods for 802.1x users, the authentication method on the switch must be consistent with that on the authentication server.

Configuring Guest VLAN

If Guest VLAN is enabled, a switch broadcasts active authentication packets to all 802.1x-enabled ports. The ports not sending response packets are added to Guest

VLAN when the maximum number of re-authentications is reached. Users in a Guest VLAN can utilize resources in the Guest VLAN without undergoing the 802.1x authentication, but they can utilize the resources outside the Guest VLAN only when they have passed the 802.1x authentication. In this way, unauthenticated users can still perform operations such as accessing some resources with the 802.1x client not installed, and upgrading 802.1x client.

Perform the following configuration in system view or Ethernet interface view.

Table 191 Configure Guest VLAN

Operation	Command
Enable Guest VLAN	dot1x guest-vlan <i>vlan-id</i> [interface <i>interface-list</i>]
Disable Guest VLAN	undo dot1x guest-vlan <i>vlan-id</i> [interface <i>interface-list</i>]

Note that:

- Guest VLAN is only supported when the switch performs port-based authentication.
- A switch can have only one Guest VLAN.
- Users who are not authenticated, fail to be authenticated, or are offline are all members of the Guest VLAN.
- Guest VLANs can only be configured on Access ports.
- You must use an existing VLAN ID, and the corresponding VLAN cannot be a Super VLAN isolate-user-vlan.
- You must perform corresponding configuration manually to isolate the Guest VLAN from other VLAN interfaces.

Setting the Maximum times of authentication request message retransmission

The following commands are used for setting the maximum retransmission times of the authentication request message that the switch sends to the supplicant.

Perform the following configuration in system view.

Table 192 Set the maximum times of the authentication request message retransmission

Operation	Command
Set the maximum times of the authentication request message retransmission	dot1x retry <i>max-retry-value</i>
Restore the default maximum retransmission times	undo dot1x retry

By default, the *max-retry-value* is 2. That is, the switch can retransmit the authentication request message to a supplicant for 2 times at most.

Configuring 802.1x Timers

The following commands are used for configuring the 802.1x timers.

Perform the following configuration in system view.

Table 193 Configure 802.1x timers

Operation	Command
Configure timers	dot1x timer { handshake-period <i>handshake-period-value</i> quiet-period <i>quiet-period-value</i> tx-period <i>tx-period-value</i> supp-timeout <i>supp-timeout-value</i> server-timeout <i>server-timeout-value</i> }
Restore default settings of the timers	undo dot1x timer { handshake-period quiet-period tx-period supp-timeout server-timeout }

handshake-period: This timer begins after the user has passed the authentication. After setting handshake-period, system will send the handshake packet by the period. Suppose the dot1x retry time is configured as N, the system will consider the user having logged off and set the user as logoff state if system doesn't receive the response from user for consecutive N times.

handshake-period-value: Handshake period. The value ranges from 1 to 1024 in units of second and defaults to 30.

quiet-period: Specifies the quiet timer. If an 802.1x user has not passed the authentication, the Authenticator will keep quiet for a while (which is specified by quiet-period timer) before launching the authentication again. During the quiet period, the Authenticator does not do anything related to 802.1x authentication.

quiet-period-value: Specifies how long the quiet period is. The value ranges from 10 to 120 in units of second and defaults to 60.

server-timeout: Specifies the timeout timer of an Authentication Server. If an Authentication Server has not responded before the specified period expires, the Authenticator will resend the authentication request.

server-timeout-value: Specifies how long the duration of a timeout timer of an Authentication Server is. The value ranges from 100 to 300 in units of second and defaults to 100 seconds.

supp-timeout: Specifies the authentication timeout timer of a Supplicant. After the Authenticator sends Request/Challenge request packet which requests the MD5 encrypted text, the supp-timeout timer of the Authenticator begins to run. If the Supplicant does not respond back successfully within the time range set by this timer, the Authenticator will resend the above packet.

supp-timeout-value: Specifies how long the duration of an authentication timeout timer of a Supplicant is. The value ranges from 10 to 120 in units of second and defaults to 30.

tx-period: Has two major effects, which are described in detail in the following section.

- Specifies the transmission timeout timer. After the Authenticator sends the Request/Identity request packet which requests the user name or user name and password together, the tx-period timer of the Authenticator begins to run. If the Supplicant does not respond back with authentication reply packet successfully, then the Authenticator will resend the authentication request packet.

- Specifies the interval of multicasting 802.1x request packets periodically. In order to be compatible with clients who do not send EAPoL-Start frames actively, Switch 8800 Family switches will multicast 802.1x request packets periodically. The clients will respond after receiving these packets. tx-period specifies the period of multicasting 802.1x request packets.

tx-period-value: Specifies how long the duration of the transmission timeout timer is. The value ranges from 10 to 120 in units of second and defaults to 30.



It is recommended to configure different handshake period value and handshake timeout times according to the number of users:

- When the number of users is 2048, the handshake period value should be no smaller than 2 minutes, and the handshake timeout times should be no less than 3 times;
- When the number of users is 1024, the handshake period value should be no smaller than 1 minutes, and the handshake timeout times should be no less than 3 times
- When the number of users is 512, the handshake period value should be no smaller than 30 seconds, and the handshake timeout times should be no less than 2 times.

Enabling/Disabling Quiet-Period Timer

You can use the following commands to enable/disable a Quiet-Period timer of an Authenticator (such as a 3Com Series Switch). If an 802.1x user has not passed the authentication, the Authenticator will keep quiet for a while (which is specified by **dot1x timer quiet-period** command) before launching the authentication again. During the Quiet Period, the Authenticator does not do anything related to 802.1x authentication.

Perform the following configuration in system view.

Table 194 Enable/Disable a Quiet-Period timer

Operation	Command
Enable a quiet-period timer	dot1x quiet-period
Disable a quiet-period timer	undo dot1x quiet-period

By default, Quiet-Period timer is disabled.

Displaying and Debugging 802.1x

After the above configuration, execute **display dot1x** command in any view to display the running of the 802.1x configuration, and to verify the effect of the configuration. Execute **reset dot1x statistics** command in user view to reset 802.1x statistics. Execute **debugging** command in user view to debug 802.1x.

Table 195 Display and debug 802.1x

Operation	Command
Display the configuration, running and statistics information of 802.1x	display dot1x [sessions statistics enabled-interface guest vlan] [interface interface-list sessions statistics]
Reset the 802.1x statistics information	reset dot1x statistics [interface interface-list]

Table 195 Display and debug 802.1x

Operation	Command
Enable the error/event/packet/all debugging of 802.1x	debugging dot1x { error event packet all }
Disable the error/event/packet/all debugging of 802.1x.	undo debugging dot1x { error event packet all }

Packet Attack Prevention Configuration

With the expansion of Internet scale and the increase of Internet users, the possibility that networking equipment gets attacked is increasing. Specific to some typical attack modes, the Switch 8800 Family series switches provides a series of schemes of preventing attacks against packets to protect the networking equipment against attacked from IP, ARP, 802.1x and unknown multicast packets.

- IP Packet attack: It refers to such a situation that the Switch 8800 Family switch receives too many IP packets whose destination addresses and VLAN interface addresses are within the same network segment, while the corresponding forwarding entries do not exist on the switch. Such packets will be delivered to the CPU for processing. They occupy lots of CPU resources, and even affect the forwarding of normal packets.
- ARP packet attack: It refers to such a situation that the Switch 8800 Family switch receives a large number of ARP request packets with the same or similar source MAC addresses. These packets affect the normal ARP learning.
- 802.1x packet attack: It refers to such a situation that the Switch 8800 Family switch receives a large number of 802.1x authentication packets with the same or similar source MAC addresses. These packets largely occupy the CPU resources.

Perform the following configuration in system view.

Table 196 Enable/disable packet attack prevention

Operation	Command
Enable/Disable packet attack prevention	anti-attack { arp dot1x ip } { disable enable }

By default, IP packet attack prevention is enabled while ARP packet attack prevention and dot1x packet attack prevention are disabled by default.

802.1x Configuration Example

Network requirements

As shown in Figure 59, the workstation of a user is connected to the port Ethernet 3/1/1 of the Switch.

The switch administrator will enable 802.1x on all the ports to authenticate the supplicants so as to control their access to the Internet. The access control mode is configured as based on the MAC address

All the supplicants belong to the default domain 3Com163.net, which can contain up to 30 users. RADIUS authentication is performed first. If there is no response from the RADIUS server, local authentication will be performed. For accounting, if the RADIUS server fails to account, the user will be disconnected. In addition,

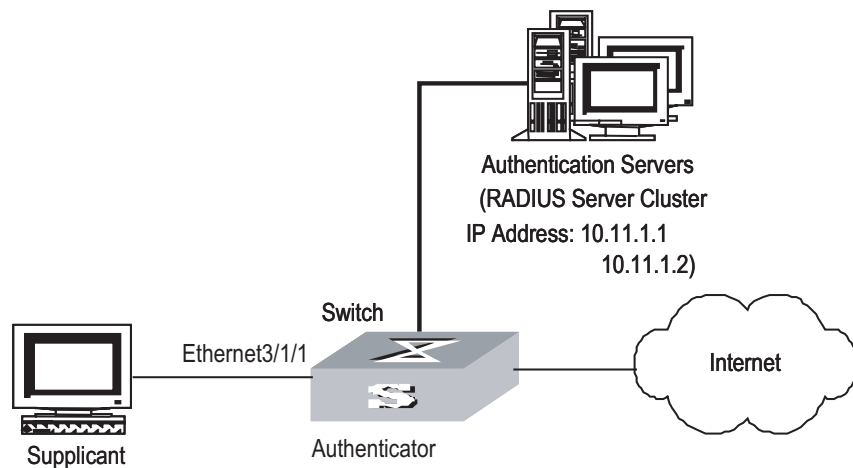
when the user is accessed, the domain name does not follow the user name. Normally, if the user's traffic is less than 2000 Byte/s consistently over 20 minutes, he will be disconnected.

A server group, consisting of two RADIUS servers at 10.11.1.1 and 10.11.1.2 respectively, is connected to the switch. The former one acts as the primary-authentication/secondary-accounting server. The latter one acts as the secondary-authentication/primary-accounting server. Set the encryption key as "name" when the system exchanges packets with the authentication RADIUS server and "money" when the system exchanges packets with the accounting RADIUS server. Configure the system to retransmit packets to the RADIUS server if no response received in 5 seconds. Retransmit the packet no more than 5 times in all. Configure the system to transmit a real-time accounting packet to the RADIUS server every 15 minutes. The system is instructed to transmit the user name to the RADIUS server after removing the user domain name from the user name.

The user name of the local 802.1x access user is localuser and the password is localpass (input in plain text). The idle cut function is enabled.

Network diagram

Figure 59 Enable 802.1x and RADIUS to perform AAA on the supplicant



Configuration procedure



The following examples concern most of the AAA/RADIUS configuration commands. For details, refer to the "AAA&RADIUS&HWTACAS" part in this document.

The configurations of access user workstation are omitted.

RADIUS server configuration is carried out in terms of RADIUS schemes. A RADIUS scheme actually can either be a stand-alone RADIUS server or two mutually backed up RADIUS servers with the same configuration and different IP addresses. So, for each RADIUS scheme, you need to configure the IP addresses for the primary and secondary RADIUS servers, and the shared key.

Enable 802.1x globally.

```
[SW8800] dot1x
```

Enable the 802.1x performance on the specified port Ethernet 3/1/1.

```
[SW8800] dot1x interface Ethernet 3/1/1
```

Set the access control mode. (This command could not be configured, when it is configured as MAC-based by default.)

```
[SW8800] dot1x port-method macbased interface Ethernet 3/1/1
```

Create the RADIUS scheme radius1 and enters its configuration mode.

```
[SW8800] radius scheme radius1
```

Set IP address of the primary authentication/accounting RADIUS servers.

```
[3Com-radius-radius1] primary authentication 10.11.1.1
[3Com-radius-radius1] primary accounting 10.11.1.2
```

Set the IP address of the secondary authentication/accounting RADIUS servers.

```
[3Com-radius-radius1] secondary authentication 10.11.1.2
[3Com-radius-radius1] secondary accounting 10.11.1.1
```

Set the encryption key when the system exchanges packets with the authentication RADIUS server.

```
[3Com-radius-radius1] key authentication name
```

Set the encryption key when the system exchanges packets with the accounting RADIUS server.

```
[3Com-radius-radius1] key accounting money
```

Set the timeouts and times for the system to retransmit packets to the RADIUS server.

```
[3Com-radius-radius1] timer 5
[3Com-radius-radius1] retry 5
```

Set the interval for the system to transmit real-time accounting packets to the RADIUS server.

```
[3Com-radius-radius1] timer realtime-accounting 15
```

Configure the system to transmit the user name to the RADIUS server after removing the domain name.

```
[3Com-radius-radius1] user-name-format without-domain
[3Com-radius-radius1] quit
```

Create the user domain 3Com163.net and enters its configuration mode.

```
[SW8800] domain 3Com163.net
```

Specify radius1 as the RADIUS scheme for the users in the domain 3Com163.net.


```
[3Com-isp-3Com163.net] radius-scheme radius1

# Set a limit of 30 users to the domain 3Com163.net.

[3Com-isp-3Com163.net] access-limit enable 30

# Enable idle cut function for the user and set the idle cut parameter in the
domain 3Com163.net.

[3Com-isp-3Com163.net] idle-cut enable 20 2000

# Add a local supplicant and sets its parameter.

[SW8800] local-user localuser
[3Com-luser-localuser] service-type lan-access
[3Com-luser-localuser] password simple localpass
```


26

AAA AND RADIUS/HWTACACS PROTOCOL CONFIGURATION

AAA and RADIUS/HWTACACS Protocol Overview

AAA Overview Authentication, Authorization and Accounting (AAA) provide a uniform framework used for configuring these three security functions to implement the network security management.

The network security mentioned here refers to access control and it includes:

- Which user can access the network server?
- Which service can the authorized user enjoy?
- How to keep accounts for the user who is using network resource?

Accordingly, AAA shall provide the following services:

- Authentication: authenticates if the user can access the network sever.
- Authorization: authorizes the user with specified services.
- Accounting: traces network resources consumed by the user.

Generally, AAA adopts Client/Server architecture, with its client running at the managed side and its server centralizes and stores the user information. Therefore AAA framework takes good scalability, and is easy to realize the control and centralized management of user information.

RADIUS Protocol Overview As mentioned above, AAA is a management framework, so it can be implemented by some protocols. RADIUS is such a protocol frequently used.

What is RADIUS

Remote Authentication Dial-In User Service, RADIUS for short, is a kind of distributed information switching protocol in Client/Server architecture. RADIUS can prevent the network from interruption of unauthorized access and it is often used in the network environments requiring both high security and remote user access. For example, it is often used for managing a large number of scattering dial-in users who use serial ports and modems. RADIUS system is the important auxiliary part of Network Access Server (NAS).

After RADIUS system is started, if the user wants to have right to access other network or consume some network resources through connection to NAS (dial-in access server in PSTN environment or Ethernet switch with access function in Ethernet environment), NAS, namely RADIUS client end, will transmit user AAA

request to the RADIUS server. RADIUS server has a user database recording all the information of user authentication and network service access. When receiving user's request from NAS, RADIUS server performs AAA through user database query and update and returns the configuration information and accounting data to NAS. Here, NAS controls supplicant and corresponding connections, while RADIUS protocol regulates how to transmit configuration and accounting information between NAS and RADIUS.

NAS and RADIUS exchange the information with UDP packets. During the interaction, both sides encrypt the packets with keys before uploading user configuration information (like password etc.) to avoid being intercepted or stolen.



The authentication and authorization of a RADIUS scheme cannot be performed separately.

RADIUS operation

RADIUS server generally uses proxy function of the devices like access server to perform user authentication. The operation process is as follows: First, the user send request message (the client username and encrypted password is included in the message) to RADIUS server. Second, the user will receive from RADIUS server various kinds of response messages in which the ACCEPT message indicates that the user has passed the authentication, and the REJECT message indicates that the user has not passed the authentication and needs to input username and password again, otherwise access will be rejected.

HWTACACS Protocol Overview

HWTACACS SPECIALITY

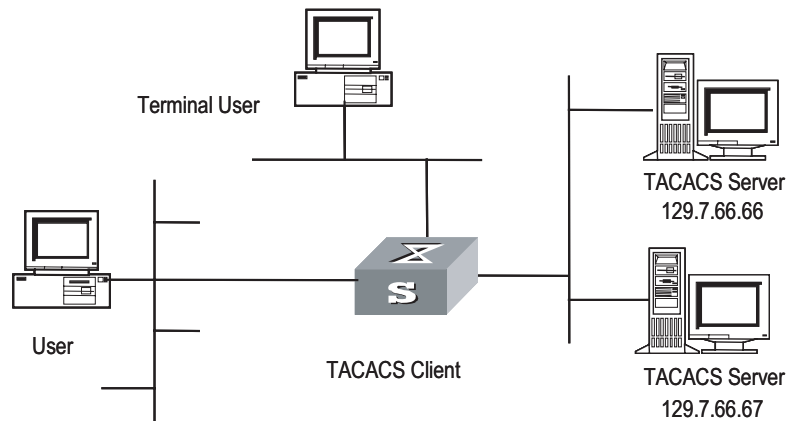
HWTACACS is an enhanced security protocol based on TACACS (RFC 1492). Similar to the RADIUS protocol, it implements AAA for different types of users through communications with TACACS servers in the Server/Client model. HWTACACS can be used for the authentication, authorization and accounting of PPP and VPDN access users and Login users.

Compared with RADIUS, HWTACACS provides more reliable transmission and encryption, and therefore is more suitable for security control. The following table lists the primary differences between HWTACACS and RADIUS protocols:

Table 197 HWTACACS vs. RADIUS

HWTACACS	RADIUS
Adopts TCP, providing more reliable network transmission.	Adopts UDP.
Encrypts the entire packet except for the standard HWTACACS header.	Encrypts only the password field in authentication packets.
Separates authentication from authorization. For example, you can use RADIUS to authenticate but HWTACACS to authorize.	Binds authentication with authorization.
Suitable for security control.	Suitable for accounting.
Supports the authorization of different users to use the configuration commands of the routing module of the switch.	Not support.

Working as a client of HWTACACS, the switch sends the username and password to the TACACS server for authentication, as shown in the following figure:

Figure 60 Network diagram for HWTACACS

Basic message exchange procedures in HWTACACS

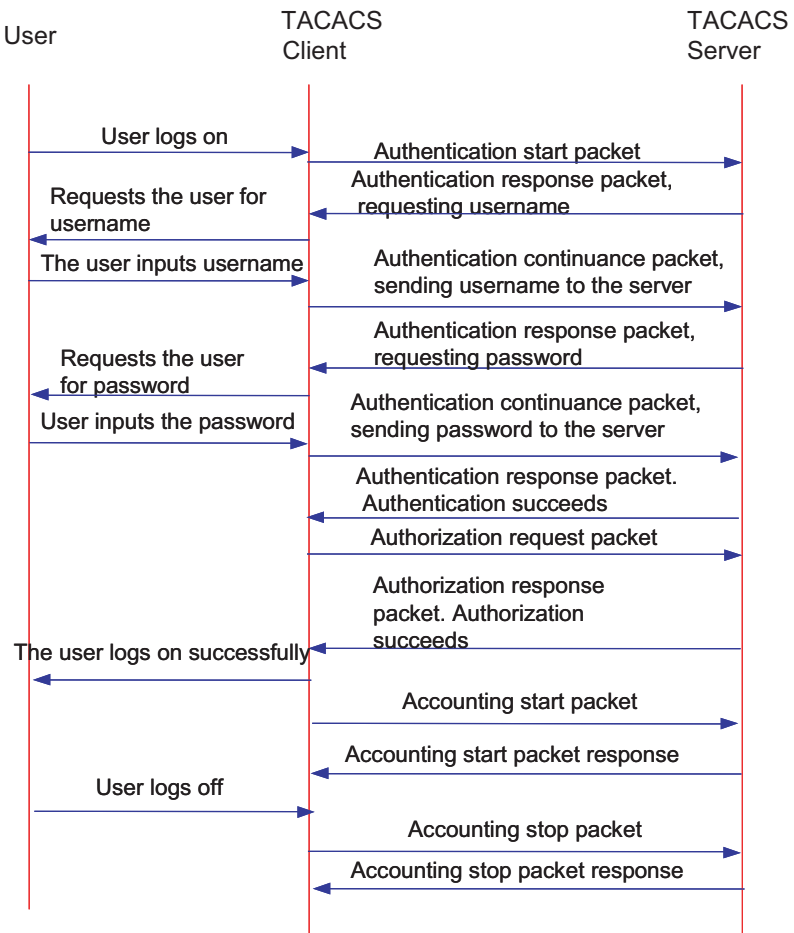
For example, use HWTACACS to implement authentication, authorization, and accounting for a telnet user. The basic message exchange procedures are as follows:

- A user requests access to the switch; the TACACS client sends a start-authentication packet to TACACS server upon receiving the request.
- The TACACS server sends back an authentication response requesting for the username; the TACACS client asks the user for the username upon receiving the response.
- The TACACS client sends an authentication continuance packet carrying the username after receiving the username from the user.
- The TACACS server sends back an authentication response, requesting for the login password. Upon receiving the response, the TACACS client requests the user for the login password.
- After receiving the login password, the TACACS client sends an authentication continuance packet carrying the login password to the TACACS server.
- The TACACS server sends back an authentication response indicating that the user has passed the authentication.
- The TACACS client sends the user authorization packet to the TACACS server.
- The TACACS server sends back the authorization response, indicating that the user has passed the authorization.
- Upon receipt of the response indicating an authorization success, the TACACS client pushes the configuration interface of the switch to the user.
- The TACACS client sends a start-accounting request to the TACACS server.
- The TACACS server sends back an accounting response, indicating that it has received the start-accounting request.
- The user logs off; the TACACS client sends a stop-accounting request to the TACACS server.
- The TACACS server sends a stop-accounting response to the client, which indicates it has received the stop-accounting request packet.

The following figure illustrates the basic message exchange procedures:

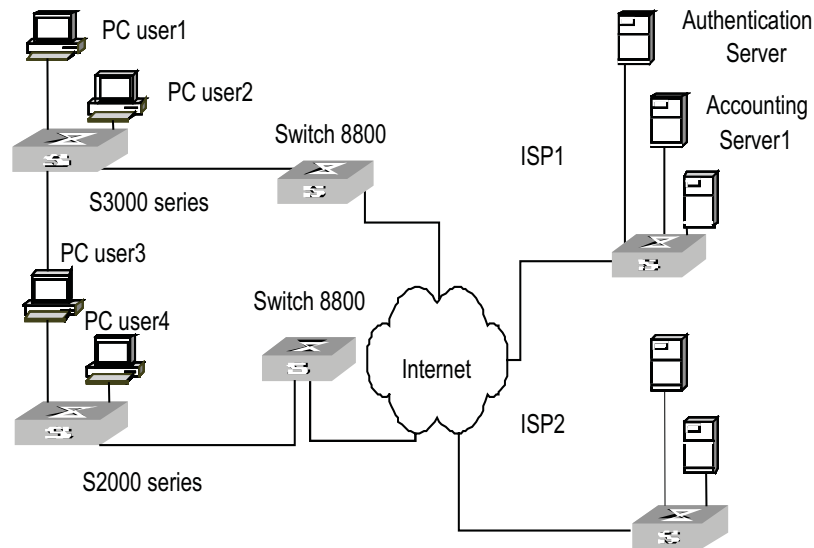
Figure 61 illustrates the basic message exchange procedures.

Figure 61 Basic message exchange procedures



Implementing AAA/RADIUS on a Switch

By now, we understand that in the above-mentioned AAA/RADIUS framework, 3Com Series Switches, serving as the user access device (NAS), is the client end of RADIUS. In other words, the AAA/RADIUS concerning client-end is implemented on 3Com Series Switches. Figure 62 illustrates the RADIUS authentication network including 3Com Series Switches.

Figure 62 Network diagram for using RADIUS to authenticate

AAA Configuration

The following sections describe AAA configuration tasks.

- "Creating/Deleting an ISP Domain"
- "Configuring Relevant Attributes of an ISP Domain"
- "Configuring Self-Service Server URL"
- "Creating/Deleting a Local User"
- "Setting the Attributes of a Local User"
- "Disconnecting a User by Force"
- "Configuring Dynamic VLAN Delivering"

Among the above configuration tasks, creating ISP domain is compulsory; otherwise the supplicant attributes cannot be distinguished. The other tasks are optional. You can configure them at requirements.

Creating/Deleting an ISP Domain

What is Internet Service Provider (ISP) domain? To make it simple, ISP domain is a group of users belonging to the same ISP. Generally, for a username in the `userid@isp-name` format, taking `gw20010608@3Com163.net` as an example, the `isp-name` (i.e. `3Com163.net`) following the `@` is the ISP domain name. When 3Com Series Switches control user access, as for an ISP user whose username is in `userid@isp-name` format, the system will take `userid` part as username for identification and take `isp-name` part as domain name.

The purpose of introducing ISP domain settings is to support the multi-ISP application environment. In such environment, one access device might access users of different ISP. Because the attributes of ISP users, such as username and password formats, etc, may be different, it is necessary to differentiate them through setting ISP domain. In 3Com Series Switches ISP domain view, you can configure a complete set of exclusive ISP domain attributes on a per-ISP domain basis, which includes AAA policy (RADIUS scheme applied etc.)

For 3Com Series Switches, each supplicant belongs to an ISP domain. Up to 16 domains can be configured in the system. If a user has not reported its ISP domain name, the system will put it into the default domain.

Perform the following configuration in system view.

Table 198 Create/Delete an ISP domain

Operation	Command
Create ISP domain or enter the view of a specified domain	domain <i>isp-name</i>
Remove a specified ISP domain	undo domain <i>isp-name</i>
Enable the default ISP domain specified by <i>isp-name</i>	domain default enable <i>isp-name</i>
Restore the default ISP domain to "system"	domain default disable

By default, a domain named "system" has been created in the system. The attributes of "system" are all default values.

Configuring Relevant Attributes of an ISP Domain

The relevant attributes of ISP domain include the adopted RADIUS scheme, ISP domain state, maximum number of supplicants, accounting optional enable/disable state, address pool definition, IP address assignment for PPP domain users, and user idle-cut enable/disable state where:

- The adopted RADIUS scheme is the one used by all the users in the ISP domain. The RADIUS scheme can be used for RADIUS authentication or accounting. By default, the default RADIUS scheme is used. The command shall be used together with the commands of setting RADIUS server and server cluster. For details, refer to the following Configuring RADIUS section of this chapter. If Local is configured as the first scheme, only the Local scheme will be adopted, neither RADIUS nor HWTACACS scheme will be adopted. When Local scheme is adopted, only authentication and authorization will be performed, accounting will not be performed. None has the same effect as Local. The usernames used for Local authentication carry no domain name, so if the Local scheme is configured, pay attention not to add domain name to the username when you configure a Local user.
- Every ISP domain has two states: Active and Block. If an ISP domain is in Active state, the users in it are allowed to request network services, while in Block state, its users are inhibit from requesting any network service, which will not affect the users already online. An ISP is in Active state once it is created, that is, at that time, all the users in the domain are allowed to request network services.
- Maximum number of supplicants specifies how many supplicants can be contained in the ISP. For any ISP domain, there is no limit to the number of supplicants by default.
- The idle cut function means: If the traffic from a certain connection is lower than the defined traffic, cut off this connection.
- The PPP access users can obtain IP addresses through the PPP address negotiation function.

Perform the following configuration in ISP domain view.

Table 199 Configure relevant attributes of an ISP domain

Operation	Command
Configure the AAA scheme used by an ISP domain	scheme { radius-scheme <i>radius-scheme-name</i> [local] hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] local none }
Restore the default AAA scheme used by an ISP domain	undo scheme { radius-scheme hwtacacs-scheme none }
Configure the RADIUS scheme used by an ISP domain	radius-scheme <i>radius-scheme-name</i>
Delete the specified RADIUS scheme	undo radius scheme <i>radius-server-name</i>
Set the state of ISP domain	state { primary secondary } { accounting authentication } { block active }
Set a limit to the amount of supplicants	access-limit { disable enable <i>max-user-number</i> }
Restore the limit to the default setting	undo access-limit
Enable accounting to be optional	accounting optional
Disable accounting to be optional	undo accounting optional
Set the Idle-cut	idle-cut { disable enable <i>minute flow</i> }
Define an address pool to assign IP addresses to users	ip pool <i>pool-number low-ip-address</i> [<i>high-ip-address</i>]
Delete the specified address pool	undo ip pool <i>pool-number</i>

Both the **radius-scheme** and **scheme radius-scheme** commands can be used to specify the RADIUS scheme for an ISP domain with the same effect, and the system adopts the last configuration.

By default, the Local scheme is adopted, an ISP domain is in Active state once it is created, no limit is set to the amount of supplicants, accounting optional is disabled, idle-cut is disabled, and no IP address pool is defined.

Configuring Self-Service Server URL

The **self-service-url enable** command must be incorporated with a RADIUS server that supports self-service, such as comprehensive access management server (CAMS). Self-service means that users can manage their accounts and card numbers by themselves. And a server with the self-service software is called a self-service server.

Once this function is enabled on the switch, users can locate the self-service server through the following operations:

- Select "Change user password" on the 802.1x client.
- After the client opens the default explorer (IE or NetScape), locate the specified URL page used to change the user password on the self-service server.
- Change user password on this page.

Perform the following configuration in ISP domain view.

Table 200 Configure the self-service server URL

Operation	Command
Configure self-service server URL and configure the URL address used to change the user password on the self-service server	self-service-url enable <i>url-string</i>
Remove the configuration of self-service server URL	self-service-url disable

By default, self-service server URL is not configured on the switch.

Note that, if "?" is contained in the URL, you must replace it with "|" when inputting the URL in the command line.

The "Change user password" option is available only when the user passes the authentication; otherwise, this option is in grey and unavailable.

Creating/Deleting a Local User

A local user is a group of users set on NAS. The username is the unique identifier of a user. A supplicant requesting network service may use local authentication only if its corresponding local user has been added onto NAS.

Perform the following configuration in system view.

Table 201 Create/Delete a local user

Operation	Command
Add a local user	local-user { <i>username</i> multicast [domain <i>domain-name</i>] <i>ipaddress</i> password-display-mode { auto cipher-force } }
Delete all the local users	undo local-user all
Delete a local user by specifying its type	undo local-user { <i>username</i> all [service-type { ftp lan-access telnet ppp ssh terminal }] multicast [domain <i>domain-name</i>] <i>ipaddress</i> password-display-mode }

By default, the user database of the system is empty. If the client user wants to access the FTP Server (Switch 8800 Family devices) through FTP, the configuration is required.

Setting the Attributes of a Local User

The attributes of a local user include its password display mode, state, service type and some other settings.

Setting the password display mode

Perform the following configuration in system view.

Table 202 Set the method that a local user uses to display password

Operation	Command
Set the mode that a local user uses to display password	local-user password-display-mode { cipher-force auto }
Cancel the mode that the local user uses to display password	undo local-user password-display-mode

Where, **auto** means that the password display mode will be the one specified by the user at the time of configuring password (see the **password** command in the

following table for reference), and **cipher-force** means that the password display mode of all the accessing users must be in cipher text.

Setting/Removing the attributes of a local user

Perform the following configuration in local user view.

Table 203 Set/Remove the attributes concerned with a specified user

Operation	Command
Set a password for a specified user	password { simple cipher } <i>password</i>
Remove the password set for the specified user	undo password
Set the state of the specified user	state { active block }
Set a service type for the specified user	service-type { ftp [ftp-directory <i>directory</i>] lan-access ppp [call-number <i>call-number</i> callback-nocheck callback-number <i>callback-number</i>] ssh [level <i>level</i>] telnet terminal] telnet [level <i>level</i> ssh terminal] terminal [level <i>level</i> ssh telnet] }
Cancel the service type of the specified user	undo service-type { ftp [ftp-directory <i>directory</i>] lan-access ppp [call-number <i>call-number</i> callback-nocheck callback-number <i>callback-number</i>] ssh [level <i>level</i> telnet terminal] telnet [level <i>level</i> ssh terminal] terminal [level <i>level</i> ssh telnet] }
Set the priority of the specified user	level <i>level</i>
Restore the default priority of the specified user	undo level
Configure the attributes of Lan-access users	attribute { ip <i>ip-address</i> mac <i>mac-address</i> idle-cut <i>second</i> access-limit <i>max-user-number</i> vlan <i>vlanid</i> location { nas-ip <i>ip-address</i> port <i>portnum</i> port <i>portnum</i> } }
Remove the attributes defined for the lan-access users	undo attribute { ip mac idle-cut access-limit vlan location } }

By default, users are not authorized to any service, all their priorities are 0.



When you bind a port to a user, this setting takes effect only when the slot number, the subslot number and the port number exist.

Disconnecting a User by Force

Sometimes it is necessary to disconnect a user or a category of users by force. The system provides the following command to serve for this purpose.

Perform the following configuration in system view.

Table 204 Disconnect a user by force

Operation	Command
Disconnect a user by force	cut connection { all access-type { dot1x gcm mac-authentication } domain <i>domain-name</i> interface <i>interface-type interface-number</i> ip <i>ip-address</i> mac <i>mac-address</i> radius-scheme <i>radius-scheme-name</i> vlan <i>vlanid</i> ucibindex <i>ucib-index</i> user-name <i>user-name</i> }

Configuring Dynamic VLAN Delivering

Dynamic VLAN delivering aims to control the network resources available to a user. With this function enabled, a switch adds the ports connecting to authenticated users to specified VLANs according to the attribute values delivered by the RADIUS server. In actual use, ports are usually set to operate in port-based mode in order to work together with Guest VLAN. A port operating in MAC address-based mode can only have one host connected to it.

Currently, the VLAN IDs delivered by RADIUS servers can be of integer or string type.

- As for a VLAN ID that is of integer type, a switch adds the port to the corresponding VLAN according to the VLAN ID delivered by the RADIUS server. If the VLAN does not exist, the switch creates the VLAN first and then adds ports to the VLAN.
- As for a VLAN ID that is of string type, a switch compares the VLAN ID delivered by the RADIUS server with the names of the VLANs existing on the switch. If a matching entry is found, the switch adds the port to the corresponding VLAN. Otherwise, the delivery fails and the user fails to pass the authentication.



- When configuring a VLAN delivering mode, keep the mode configured on the switch consistent with the mode configured on the Radius Server..
- For the string delivery mode, the value range of the VLAN name supported by the switch is 1-32 characters. If the name configured on the Radius Server exceeds 32 characters, the delivery will fail.
- For the string delivery mode, a string that contains numerals only is first interpreted as a number. That is, if the VLAN name delivered by the RADIUS server contains only numerals (such as "1024"), and the equivalent integer is within the range 1 to 4,094, the switch takes the VLAN name as an integer and add the authenticated port to the VLAN identified by the integer (In this case, the switch will add the port to VLAN 1024). If the equivalent integer is not within the range 1 to 4,094 (such as string "12345"), the RADIUS server fails to deliver the VALN name; if the all-numeral string contains space, such as "12 345", the first block of non-spaced numbers in the string will be converted into its equivalent integer, namely, integer 12 in this example.
- Hybrid ports and Trunk ports do not support VLAN delivering; only Access ports support VLAN delivering.

Dynamic VLAN delivering configuration includes:

- Configuring VLAN delivery mode (integer or string)
- Configuring the name of the delivered VLAN

Configuring VLAN delivery mode

Perform the following configuration in ISP domain view.

Table 205 Configure VLAN delivery mode

Operation	Command
Configure the VLAN delivery mode to be integer	vlan-assignment-mode integer
Configure the VLAN delivery mode to be string	vlan-assignment-mode string

By default, the integer mode is used. That is, the switch supports the RADIUS server delivering VLAN IDs in integer form.

Configuring name of a delivered VLAN

Perform the following configuration in VLAN view.

Table 206 Configure the name of a delivered VLAN

Operation	Command
Configure the name of a delivered VLAN	name <i>string</i>
Remove the configured VLAN name and restore it to the default name	undo name

By default, the delivered VLAN does not have a name.

Configuring RADIUS Protocol

For the 3Com Series Switches, the RADIUS protocol is configured on the per RADIUS scheme basis. In real networking environment, a RADIUS scheme can be an independent RADIUS server or a set of primary/secondary RADIUS servers with the same configuration but two different IP addresses. Accordingly, attributes of every RADIUS scheme include IP addresses of primary and secondary servers, shared key and RADIUS server type etc.

Actually, RADIUS protocol configuration only defines some necessary parameters using for information interaction between NAS and RADIUS Server. To make these parameters take effect on an ISP domain, you must configure the ISP domain to use the RADIUS scheme configured with these parameters in ISP domain view. For more about the configuration commands, refer to the AAA Configuration section above.

The following sections describe RADIUS protocol configuration tasks.

- "Creating/Deleting a RADIUS scheme"
- "Setting IP Address and Port Number of a RADIUS Server"
- "Setting the RADIUS Packet Encryption Key"
- "Configuring VPN of RADIUS Server"
- "Setting the Port State of the Local RADIUS Server"
- "Setting the Maximum Retry Times for RADIUS Request Packets"
- "Setting RADIUS Server Response Timeout Timer"
- "Setting Quiet Time of RADIUS Server"
- "Setting the Retransmission Times of RADIUS Request Packets"
- "Enabling the Selection of Radius Accounting Option"
- "Setting a Real-time Accounting Interval"
- "Setting the Maximum Times of Real-time Accounting Request Failing to be Responded"
- "Enabling/Disabling Stopping Accounting Request Buffer"
- "Setting the Maximum Retransmitting Times of Stopping Accounting Request"
- "Setting the Supported Type of RADIUS Server"
- "Setting RADIUS Server State"

- “Setting the Username Format Transmitted to RADIUS Server”
- “Setting the Unit of Data Flow that Transmitted to RADIUS Server”
- “Configuring the Source Address Used by NAS in RADIUS Packets”
- “Setting the Port State of RADIUS Client”
- “Configuring a Local RADIUS Authentication Server”

Among the above tasks, creating RADIUS scheme and setting IP address of RADIUS server are required, while other tasks are optional and can be performed as your requirements.

Creating/Deleting a RADIUS scheme

As mentioned above, RADIUS protocol configurations are performed on the per RADIUS scheme basis. Therefore, before performing other RADIUS protocol configurations, it is compulsory to create the RADIUS scheme and enter its view.

You can use the following commands to create/delete a RADIUS scheme.

Perform the following configuration in system view.

Table 207 Create/Delete a RADIUS server group

Operation	Command
Create a RADIUS server group and enter its view	radius scheme <i>radius-server-name</i>
Delete a RADIUS server group	undo radius scheme <i>radius-server-name</i>

Several ISP domains can use a RADIUS server group at the same time. You can configure up to 16 RADIUS schemes, including the default server group named as System.

By default, the system has a RADIUS scheme named "system" whose attributes are all default values.

Setting IP Address and Port Number of a RADIUS Server

After creating a RADIUS scheme, you are supposed to set IP addresses and UDP port numbers for the RADIUS servers, including primary/secondary authentication/authorization servers and accounting servers. So you can configure up to 4 groups of IP addresses and UDP port numbers. However, at least you have to set one group of IP address and UDP port number for each pair of primary/secondary servers to ensure the normal AAA operation.

You can use the following commands to configure the IP address and port number for RADIUS schemes.

Perform the following configuration in RADIUS scheme view.

Table 208 Set IP Address and Port Number of RADIUS Server

Operation	Command
Set IP address and port number of primary RADIUS authentication/authorization server.	primary authentication <i>ip-address</i> [<i>port-number</i>]
Restore IP address and port number of primary RADIUS authentication/authorization or server to the default values.	undo primary authentication

Table 208 Set IP Address and Port Number of RADIUS Server

Operation	Command
Set IP address and port number of primary RADIUS accounting server.	primary accounting <i>ip-address</i> [<i>port-number</i>]
Restore IP address and port number of primary RADIUS accounting server or server to the default values.	undo primary accounting
Set IP address and port number of secondary RADIUS authentication/authorization server.	secondary authentication <i>ip-address</i> [<i>port-number</i>]
Restore IP address and port number of secondary RADIUS authentication/authorization or server to the default values.	undo secondary authentication
Set IP address and port number of secondary RADIUS accounting server.	secondary accounting <i>ip-address</i> [<i>port-number</i>]
Restore IP address and port number of secondary RADIUS accounting server or server to the default values.	undo secondary accounting

By default, as for the "system" RADIUS scheme created by the system:

The IP address of the primary authentication server is 127.0.0.1, and the UDP port number is 1645.

The IP address of the secondary authentication server is 0.0.0.0, and the UDP port number is 1812.

The IP address of the primary accounting server is 127.0.0.1, and the UDP port number is 1646

The IP address of the secondary accounting server is 0.0.0.0, and the UDP port number is 1813;

As for the newly created RADIUS scheme:

The IP address of the primary/secondary authentication server is 0.0.0.0, and the UDP port number of this server is 1812;

The IP address of the primary/secondary accounting server is 0.0.0.0, and the UDP port number of this server is 1813;

In real networking environments, the above parameters shall be set according to the specific requirements. For example, you may specify 4 groups of different data to map 4 RADIUS servers, or specify one of the two servers as primary authentication/authorization server and secondary accounting server and the other one as secondary authentication/authorization server and primary accounting server, or you may also set 4 groups of exactly same data so that every server serves as a primary and secondary AAA server.

To guarantee the normal interaction between NAS and RADIUS server, you are supposed to guarantee the normal routes between RADIUS/HWTACACS server and NAS before setting IP address and UDP port of the RADIUS server and IP address and TCP port of the HWTACACS server. In addition, because RADIUS/HWTACACS protocol uses different ports to receive/transmit

authentication/authorization and accounting packets, you shall set two different ports accordingly. Suggested by RFC2138/2139, authentication/authorization port number is 1812 and accounting port number is 1813. However, you may use values other than the suggested ones. (Especially for some earlier RADIUS/HWTACACS Servers, authentication/authorization port number is often set to 1645 and accounting port number is 1646.)

The RADIUS/HWTACACS service port settings on 3Com Series Switches are supposed to be consistent with the port settings on RADIUS server. Normally, RADIUS accounting service port is 1813 and the authentication/authorization service port is 1812.



For a Switch 8800 Family series routing switch, the default RADIUS scheme authentication/authorization port is 1645, the accounting port is 1646. And port 1812 and 1813 are for other schemes.

Setting the RADIUS Packet Encryption Key

RADIUS client (switch system) and RADIUS server use MD5 algorithm to encrypt the exchanged packets. The two ends verify the packet through setting the encryption key. Only when the keys are identical can both ends to accept the packets from each other end and give response.

You can use the following commands to set the encryption key for RADIUS packets.

Perform the following configuration in RADIUS scheme view.

Table 209 Set RADIUS packet encryption key

Operation	Command
Set RADIUS authentication/authorization packet encryption key	key authentication <i>string</i>
Restore the default RADIUS authentication/authorization packet encryption key	undo key authentication
Set RADIUS accounting packet encryption key	key accounting <i>string</i>
Restore the default RADIUS accounting packet encryption key	undo key accounting

By default, the encryption keys of RADIUS authentication/authorization and accounting packets are all "3Com".

Configuring VPN of RADIUS Server

The default address of the RADIUS Server is the address of the public network. If the RADIUS Server is built under a private network, you must specify the VPN to which the RADIUS Server belongs when configuring the RADIUS Server.

Use the following commands to configure the VPN of the RADIUS Server.

Perform the following configuration in RADIUS scheme view.

Table 210 Configure the VPN of the RADIUS Server

Operation	Command
Set the VPN that the RADIUS Server belongs to	vpn-instance <i>vpn-name</i>

Table 210 Configure the VPN of the RADIUS Server

Operation	Command
Restore the VPN attribute of RADIUS Server to the default value	undo vpn-instance

The RADIUS Server does not belong to any VPN by default.

Setting the Port State of the Local RADIUS Server

The local RADIUS server uses the switch itself as the RADIUS server, with port 1645 as authentication port and port 1646 as accounting port. The two ports are enabled in the initial state, without any corresponding command lines to enable/disable them. Considering the policy of maximum security, certain measures are taken to control the ports to eliminate potential security troubles.

Perform the following configuration in system view.

Table 211 Set the port state of the local RADIUS server

Operation	Command
Enable the port of the local RADIUS server	local-server enable
Disable the port of the local RADIUS server	undo local-server

By default, the local RADIUS server is enabled, and port 1645 and port 1646 are enabled.

Setting the Maximum Retry Times for RADIUS Request Packets

Because RADIUS Protocol carries data through UDP packets, its communication process is not reliable. If the RADIUS Server does not respond to the NAS within the time specified by the response timeout timer, it is necessary for the NAS to retry sending the RADIUS request packets to the RADIUS Server. If the number of retry times exceeds maximum retry times while the RADIUS Server still does not respond, the NAS will assume its communication with the current RADIUS Server to have been cut off and will send request packets to another RADIUS Server.

Use the following commands to set the maximum retry times of sending RADIUS request packets.

Perform the following configuration in RADIUS scheme view.

Table 212 Set the maximum retry times of sending RADIUS request packets

Operation	Command
Set the maximum retry times of sending RADIUS request packets	retry <i>retry-times</i>
Restore the maximum retry times of sending RADIUS request packets to the default value	undo retry

By default, the maximum retry times of sending RADIUS request packets is 3.

Setting RADIUS Server Response Timeout Timer

If the NAS fails to receive the response from RADIUS server a certain period of time after it sends a RADIUS request packet (authentication/authorization request or accounting request), it should retransmit the RADIUS request packet to ensure the RADIUS service for the user.

You can use the following command to set the response timeout timer of the RADIUS server.

Perform the following configuration in RADIUS scheme view.

Table 213 Set RADIUS server response timeout timer

Operation	Command
Set the response timeout timer of RADIUS server	timer response-timeout <i>seconds</i>
Restore the default value of the response timeout timer of RADIUS server	undo timer response-timeout

The default value of the response timeout timer of a RADIUS server is 3 seconds.

Setting Quiet Time of RADIUS Server

When the communication between the switch and the RADIUS Server is interrupted, the switch will stop processing request packets from the users, and will send user request packets to the RADIUS Server after it has waited for a certain period of time.

Use the following command to set the quiet time of the RADIUS Server.

Perform the following configuration in RADIUS scheme view.

Table 214 Set quiet time of RADIUS Server

Operation	Command
Set quiet time of RADIUS Server	timer quiet <i>minutes</i>
Restore quiet time of RADIUS Server to the default value	undo timer quiet

By default, the quiet time of the primary server is 5 minutes.

Setting the Retransmission Times of RADIUS Request Packets

Since RADIUS protocol uses UDP packet to carry the data, the communication process is not reliable. If the RADIUS server has not responded NAS before timeout, NAS has to retransmit RADIUS request packet. If it transmits more than the specified *retry-times*, NAS considers the communication with the current RADIUS server has been disconnected, and turn to send request packet to other RADIUS server.

You can use the following command to set retransmission times of RADIUS request packet.

Perform the following configuration in RADIUS scheme view.

Table 215 Set the retransmission times of RADIUS request packets

Operation	Command
Set retransmission times of RADIUS request packet	retry <i>retry-times</i>
Restore the default value of retransmission times	undo retry

By default, RADIUS request packet will be retransmitted up to three times.

Enabling the Selection of Radius Accounting Option

If no RADIUS server is available or if RADIUS accounting server fails when the **accounting optional** is configured, the user can still use the network resource, otherwise, the user will be disconnected.

Perform the following configuration in RADIUS scheme view.

Table 216 Enable the selection of RADIUS accounting option

Operation	Command
Enable the selection of RADIUS accounting option	accounting optional
Disable the selection of RADIUS accounting option	undo accounting optional

By default, selection of RADIUS accounting option is disabled.

Setting a Real-time Accounting Interval

To implement real-time accounting, it is necessary to set a real-time accounting interval. After the attribute is set, NAS will transmit the accounting information of online users to the RADIUS server regularly.

You can use the following command to set a real-time accounting interval.

Perform the following configuration in RADIUS scheme view.

Table 217 Set a real-time accounting interval

Operation	Command
Set a real-time accounting interval	timer realtime-accounting <i>minute</i>
Restore the default value of the interval	undo timer realtime-accounting

minute specifies the real-time accounting interval in minutes. The value shall be a multiple of 3.

The value of *minute* is related to the performance of NAS and RADIUS server. The smaller the value is, the higher the performances of NAS and RADIUS are required. When there are a large amount of users (more than 1000, inclusive), we suggest a larger value. The following table recommends the ratio of *minute* value to the number of users.

Table 218 Recommended real-time accounting intervals for different number of users

Number of users	Real-time accounting interval in minutes
1 to 99	3
100 to 499	6
500 to 999	12
≥1000	≥15

By default, *minute* is set to 12 minutes.

Setting the Maximum Times of Real-time Accounting Request Failing to be Responded

RADIUS server usually checks if a user is online with timeout timer. If the RADIUS server has not received the real-time accounting packet from NAS for long, it will consider that there is device failure and stop accounting. Accordingly, it is necessary to disconnect the user at NAS end and on RADIUS server synchronously when some unpredictable failure exists. 3Com Series Switches support to set maximum times of real-time accounting request failing to be responded. NAS will disconnect the user if it has not received real-time accounting response from RADIUS server for some specified times.

You can use the following command to set the maximum times of real-time accounting request failing to be responded.

Perform the following configuration in RADIUS scheme view.

Table 219 Set the maximum times of real-time accounting request failing to be responded

Operation	Command
Set maximum times of real-time accounting request failing to be responded	retry realtime-accounting <i>retry-times</i>
Restore the maximum times to the default value	undo retry realtime-accounting

How to calculate the value of *retry-times*? Suppose that RADIUS server connection will timeout in T and the real-time accounting interval of NAS is t, then the integer part of the result from dividing T by t is the value of *count*. Therefore, when applied, T is suggested the numbers which can be divided exactly by t.

By default, the real-time accounting request can fail to be responded no more than 5 times.

Enabling/Disabling Stopping Accounting Request Buffer

Because the stopping accounting request concerns account balance and will affect the amount of charge, which is very important for both the subscribers and the ISP, NAS shall make its best effort to send the request to RADIUS accounting server. Accordingly, if the request from 3Com Series Switches to RADIUS accounting server has not been responded, switch shall save it in the local buffer and retransmit it until the server responds or discards the messages after transmitting for specified times. You can use the following command to set whether or not to save the stopping accounting requests.

Perform the following configuration in RADIUS scheme view.

Table 220 Enable/Disable stopping accounting request buffer

Operation	Command
Enable stopping accounting request buffer	stop-accounting-buffer enable
Disable stopping accounting request buffer	undo stop-accounting-buffer enable

By default, the stopping accounting request will be saved in the buffer.

Setting the Maximum Retransmitting Times of Stopping Accounting Request

Because the stopping accounting request concerns account balance and will affect the amount of charge, which is very important for both the subscribers and the ISP, NAS shall make its best effort to send the message to RADIUS accounting server. Accordingly, if the request from 3Com Series Switch to RADIUS accounting server has not been responded, switch shall save it in the local buffer and retransmit it until the server responds or discards the messages after transmitting for specified times. Use the following command to set the maximum retransmission times.

Perform the following configuration in RADIUS scheme view.

Table 221 Set the maximum retransmitting times of stopping accounting request

Operation	Command
Set the maximum retransmitting times of stopping accounting request	retry stop-accounting <i>retry-times</i>
Restore the maximum retransmitting times of stopping accounting request to the default value	undo retry stop-accounting

By default, the stopping accounting request can be retransmitted for up to 500 times.

Setting the Supported Type of RADIUS Server

3Com Series Switches support the standard RADIUS protocol and the extended RADIUS service platforms, such as IP Hotel, 201+ and Portal, independently developed by 3Com.

You can use the following command to set the supported types of RADIUS servers.

Perform the following configuration in RADIUS scheme view.

Table 222 Set the supported type of RADIUS scheme

Operation	Command
Set the Supported Type of RADIUS Server	server-type { 3Com standard }
Restore the Supported Type of RADIUS Server to the default setting	undo server-type

By default, the newly created RADIUS scheme supports the server of **standard** type, while the "system" RADIUS scheme created by the system supports the server of **3Com** type

Setting RADIUS Server State

For the primary and secondary servers (no matter it is an authentication/authorization server or accounting server), if the primary is disconnected to NAS for some fault, NAS will automatically turn to exchange packets with the secondary server. However, after the primary one recovers, NAS will not resume the communication with it at once, instead, it continues communicating with the secondary one. When the secondary one fails to communicate, NAS will turn to the primary one again. The following commands can be used to set the primary server to be **active** manually, in order that NAS can communicate with it right after the troubleshooting.

When both the primary and secondary servers are **active** or **block**, NAS first sends packets to the primary server. If NAS fails to connect the primary server, it sends the packets to the secondary server.

Perform the following configuration in RADIUS scheme view.

Table 223 Set RADIUS server state

Operation	Command
Set the state of primary RADIUS server	state primary { accounting authentication } { block active }

Table 223 Set RADIUS server state

Operation	Command
Set the state of secondary RADIUS sever	state secondary { accounting authentication } { block active }

By default, the state of each server in RADIUS scheme server group is **active**.

Setting the Username Format Transmitted to RADIUS Server

As mentioned above, the supplicants are generally named in `userid@isp-name` format. The part following "@" is the ISP domain name. 3Com Series Switches will put the users into different ISP domains according to the domain names. However, some earlier RADIUS servers reject the username including ISP domain name. In this case, you have to remove the domain name before sending the username to the RADIUS server. The following command of switch decides whether the username to be sent to RADIUS server carries ISP domain name or not.

Perform the following configuration in RADIUS scheme view.

Table 224 Set the username format transmitted to RADIUS server

Operation	Command
Set Username Format Transmitted to RADIUS Server	user-name-format { with-domain without-domain }



If a RADIUS scheme is configured not to allow usernames including ISP domain names, the RADIUS scheme shall not be simultaneously used in more than one ISP domain. Otherwise, the RADIUS server will regard two users in different ISP domains as the same user by mistake, if they have the same username (excluding their respective domain names.)

By default, as for the newly created RADIUS scheme, the username sent to RADIUS servers includes an ISP domain name; as for the "system" RADIUS scheme created by the system, the username sent to RADIUS servers excludes the ISP domain name.

Setting the Unit of Data Flow that Transmitted to RADIUS Server

The following command defines the unit of the data flow sent to RADIUS server.

Perform the following configuration in RADIUS scheme view.

Table 225 Set the unit of data flow transmitted to RADIUS server

Operation	Command
Set the unit of data flow transmitted to RADIUS server	data-flow-format { data { byte giga-byte kilo-byte mega-byte } } { packet { giga-byte kilo-byte mega-byte one-packet } }
Restore the unit to the default setting	undo data-flow-format

By default, the default data unit is byte and the default data packet unit is one packet.

Configuring the Source Address Used by NAS in RADIUS Packets

Perform the following configuration in the corresponding view.

Table 226 Configuring the source address used by the NAS in RADIUS packets

Operation	Command
Configure the source address used by the NAS in RADIUS packets (RADIUS scheme view)	nas-ip <i>ip-address</i>
Cancel the configured source address used by the NAS in RADIUS packets (RADIUS scheme view)	undo nas-ip
Configure the source address used by the NAS in RADIUS packets (System view)	radius nas-ip <i>ip-address</i> [vpn-instance <i>vpn-instance-name</i>]
Cancel the configured source address used by the NAS in RADIUS packets (System view)	undo radius nas-ip [vpn-instance <i>vpn-instance-name</i>]

The effect of the two commands is the same. However, the configuration done in RADIUS scheme view has a higher priority than the configuration done in system view.

By default, no source address is specified, that is to say, the interface from which a packet is sent is regarded as the source address of the packet.

Setting the Port State of RADIUS Client

According to RFC2138/2139 protocol, Radius service generally adopts port 1812 as authentication packet port and port 1813 as accounting packet port. However, the source port of both authentication packets and accounting packets is port 1812 on 3Com Switch 8800 Family series switches. If such packets are sent, the destination port of the response packets is port 1812. So RADIUS service can be controlled on the switch by controlling the inbound UDP packets whose destination port is 1812.

3Com series switches provide the following command to set the state of port 1812 of the RADIUS client.

Perform the following configuration in system view.

Table 227 Set the port state of RADIUS client

Operation	Command
Enable the port 1812 of the RADIUS client	radius client enable
Disable the port 1812 of the RADIUS client	undo radius client

The port 1812 of the RADIUS client is disabled by default.

If the port 1812 is disabled, all the UDP packets whose destination port is port 1812 will be dropped, so the remote RADIUS service cannot be used.

Configuring a Local RADIUS Authentication Server

3Com Switch 8800 Family series switches not only support the traditional RADIUS client service mentioned above, that is, adopting authentication, authorization and accounting servers to authenticate and administrate users, but also provides simple local RADIUS server function (including authentication and authorization), which is also known as local RADIUS authentication server function. A Switch 8800 Family switch supports up to 16 local RADIUS servers.

Perform the following configuration in system view.

Table 228 Create/Delete a local RADIUS authentication server

Operation	Command
Create a local RADIUS authentication server	local-server nas-ip <i>ip-address</i> key <i>password</i>
Delete a local RADIUS authentication server	undo local-server nas-ip <i>ip-address</i>

By default, the IP address of local RADIUS authentication server group is 127.0.0.1 and the password is 3Com.

When using local RADIUS server function, note that,

- 1 The number of UDP port used for authentication/authorization is 1645 and that for accounting is 1646.
- 2 The *password* configured by **local-server** command must be the same as that of the RADIUS authentication/authorization packet configured by the command **key authentication** in radius scheme view.
- 3 Switch 8800 Family series serving as local RADIUS authentication servers currently only support the CHAP and PAP authentication modes; they do not support the MD5-challenge mode.

Configuring HWTACACS Protocol

The following sections describe HWTACACS configuration tasks.

- “Creating a HWTACAS Scheme”
- “Configuring HWTACACS Authentication Servers”
- “Configuring HWTACACS Authorization Servers”
- “Configuring HWTACACS Accounting Servers and the Related Attributes”
- “Configuring the Source Address for HWTACACS Packets Sent by NAS”
- “Setting a Key for Securing the Communication with TACACS Server”
- “Setting the Username Format Acceptable to the TACACS Server”
- “Setting the Unit of Data Flows Destined for the TACACS Server”
- “Setting Timers Regarding TACACS Server”



Pay attention to the following when configuring a TACACS server:

- HWTACACS server does not check whether a scheme is being used by users when changing most of HWTACS attributes, unless you delete the scheme.
- By default, the TACACS server has no key.

In the above configuration tasks, creating HWTACACS scheme and configuring TACACS authentication/authorization server are required; all other tasks are optional and you can determine whether to perform these configurations as needed.

Creating a HWTACAS Scheme

As aforementioned, HWTACACS protocol is configured scheme by scheme. Therefore, you must create a HWTACACS scheme and enter HWTACACS view before you perform other configuration tasks.

Perform the following configuration in system view.

Table 229 Create a HWTACACS scheme

Operation	Command
Create a HWTACACS scheme and enter HWTACACS view	hwtacacs scheme <i>hwtacacs-scheme-name</i>
Delete a HWTACACS scheme	undo hwtacacs scheme <i>hwtacacs-scheme-name</i>

By default, no HWTACACS scheme exists.

If the HWTACACS scheme you specify does not exist, the system creates it and enters HWTACACS view. In HWTACACS view, you can configure the HWTACACS scheme specifically.

The system supports up to 16 HWTACACS schemes. You can only delete the schemes that are not being used.

Configuring HWTACACS Authentication Servers

Perform the following configuration in HWTACACS view.

Table 230 Configure HWTACACS authentication servers

Operation	Command
Configure the HWTACACS primary authentication server	primary authentication <i>ip-address</i> [<i>port-number</i>]
Delete the HWTACACS primary authentication server	undo primary authentication
Configure the HWTACACS secondary authentication server	secondary authentication <i>ip-address</i> [<i>port-number</i>]
Delete the HWTACACS secondary authentication server	undo secondary authentication

The primary and secondary authentication servers cannot use the same IP address. The default port number is 49.

If you execute this command repeatedly, the new settings will replace the old settings.

A TACACS scheme authentication server can be deleted only when no Active TCP connection used to send authentication packets is using the server.

Configuring HWTACACS Authorization Servers

Perform the following configuration in HWTACACS view.

Table 231 Configure HWTACACS authorization servers

Operation	Command
Configure the primary HWTACACS authorization server	primary authorization <i>ip-address</i> [<i>port-number</i>]
Delete the primary HWTACACS authorization server	undo primary authorization
Configure the secondary HWTACACS authorization server	secondary authorization <i>ip-address</i> [<i>port-number</i>]
Delete the secondary HWTACACS authorization server	undo secondary authorization



If only authentication and accounting servers are configured and no authorization server is configured, both authentication and accounting can be performed normally for the FTP, Telnet, and SSH users, but the priority of these users is 0 (that is, the lowest privilege level) by default,

The primary and secondary authorization servers cannot use the same IP address. The default port number is 49.

If you execute this command repeatedly, the new settings will replace the old settings.

Configuring HWTACACS Accounting Servers and the Related Attributes

Configuring HWTACACS accounting servers

Perform the following configuration in HWTACACS view.

Table 232 Configure HWTACACS accounting servers

Operation	Command
Configure the primary TACACS accounting server	primary accounting <i>ip-address</i> [<i>port-number</i>]
Delete the primary TACACS accounting server	undo primary accounting
Configure the secondary TACACS accounting server	secondary accounting <i>ip-address</i> [<i>port-number</i>]
Delete the secondary TACACS accounting server	undo secondary accounting

Do not configure the same IP address for the primary accounting server and the secondary accounting server. Otherwise, an error occurs.

By default, a TACACS accounting server uses an all-zero IP address and port 49.

If you execute the **primary accounting** or **secondary accounting** command repeatedly, the newly configured settings overwrite the corresponding existing settings.

You can delete a TACACS scheme only when no Active TCP connection used to send authentication packets uses the server.

Enabling stop-accounting packet retransmission

Perform the following configuration in HWTACACS view.

Table 233 Configure stop-accounting packet retransmission

Operation	Command
Enable stop-accounting packet retransmission and set the allowed maximum number of transmission attempts	retry stop-accounting <i>retry-times</i>
Disable stop-accounting packet retransmission	undo retry stop-accounting
Clear the stop-accounting request packets that have no response	reset stop-accounting-buffer hwtacacs-scheme <i>hwtacacs-scheme-name</i>

By default, stop-accounting packet retransmission is enabled, and the maximum number of transmission attempts is 300.

Configuring the Source Address for HWTACACS Packets Sent by NAS

Perform the following configuration in the corresponding view.

Table 234 Configure the source address for HWTACACS packets sent by the NAS

Operation	Command
Configure the source address for HWTACACS packets sent from the NAS (HWTACACS view)	nas-ip <i>ip-address</i>
Delete the configured source address for HWTACACS packets sent from the NAS (HWTACACS view)	undo nas-ip
Configure the source address for HWTACACS packets sent from the NAS (System view)	hwtacacs nas-ip <i>ip-address</i>
Cancel the configured source address for HWTACACS packets sent from the NAS (System view)	undo hwtacacs nas-ip

The HWTACACS view takes precedence over the system view when configuring the source address for HWTACACS packets sent from the NAS.

By default, the source address is not specified, and the virtual interface of the VLAN that contains the port to which the server connects for packet sending is used as the source address.

Setting a Key for Securing the Communication with TACACS Server

When using a TACACS server as an AAA server, you can set a key to improve the communication security between the switch and the TACACS server.

Perform the following configuration in HWTACACS view.

Table 235 Set a key for securing the communication with the HWTACACS server

Operation	Command
Configure a key for securing the communication with the accounting, authorization or authentication server	key { accounting authorization authentication } <i>string</i>
Delete the configuration	undo key { accounting authorization authentication }

No key is configured by default.

Setting the Username Format Acceptable to the TACACS Server

Username is usually in the "userid@isp-name" format, with the domain name following "@".

If a TACACS server does not accept the username with domain name, you can remove the domain name and resend it to the TACACS server.

Perform the following configuration in HWTACACS view.

Table 236 Set the username format acceptable to the TACACS server

Operation	Command
Send username with domain name	user-name-format with-domain
Send username without domain name	user-name-format without-domain

By default, each username sent to a TACACS server contains a domain name.

Setting the Unit of Data Flows Destined for the TACACS Server

Perform the following configuration in HWTACACS view.

Table 237 Set the unit of data flows destined for the TACACS server

Operation	Command
Set the unit of data flows destined for the TACACS server	data-flow-format data { byte giga-byte kilo-byte mega-byte }
	data-flow-format packet { giga-packet kilo-packet mega-packet one-packet }
Restore the default unit of data flows destined for the TACACS server	undo data-flow-format { data packet }

The default data flow unit is byte.

Setting Timers Regarding TACACS Server

Setting the response timeout timer

Since HWTACACS is implemented on the basis of TCP, server response timeout or TCP timeout may terminate the connection to the TACACS server.

Perform the following configuration in HWTACACS view.

Table 238 Set the response timeout timer

Operation	Command
Set the response timeout time	timer response-timeout <i>seconds</i>
Restore the default setting	undo timer response-timeout

The default response timeout timer is set to 5 seconds.

Setting the quiet timer for the primary TACACS server

Perform the following configuration in HWTACACS view.

Table 239 Set the quiet timer for the primary TACACS server

Operation	Command
Set the quiet timer for the primary TACACS server	timer quiet <i>minutes</i>
Restore the default setting	undo timer quiet

The **timer quiet** command is used to make the switch ignore users' requests for server within the time configured in this command in case the communication between the switch and the server is terminated. In that case, the switch can send users' requests to the server only after it has waited a time no less than the time configured with this command for the communication to be resumed.

By default, the primary TACACS server must wait five minutes before it can resume the active state. The time ranges from 1 to 255.

Setting a realtime accounting interval

The setting of real-time accounting interval is necessary to real-time accounting. After an interval value is set, the NAS transmits the accounting information of online users to the TACACS accounting server periodically.

Perform the following configuration in HWTACACS view.

Table 240 Set a real-time accounting interval

Operation	Command
Set a real-time accounting interval	timer realtime-accounting <i>minute</i>
Restore the default real-time accounting interval	undo timer realtime-accounting

The interval is in minutes and must be a multiple of 3.

The setting of real-time accounting interval somewhat depends on the performance of the NAS and the TACACS server: a shorter interval requires higher device performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table lists the numbers of users and the recommended intervals.

Table 241 Numbers of users and the recommended intervals

Number of users	Real-time accounting interval (in minutes)
1 to 99	3
100 to 499	6
500 to 999	12
≥1000	15

The real-time accounting interval defaults to 12 minutes.

Displaying and Debugging AAA and RADIUS Protocol

After the above configuration, execute **display** command in any view to display the running of the AAA and RADIUS/HWTACACS configuration, and to verify the effect of the configuration. Execute **reset** command in user view to reset AAA and RADIUS/HWTACACS statistics, etc. Execute **debugging** command in user view to debug AAA and RADIUS/HWTACACS.

Table 242 Display and debug AAA and RADIUS/HWTACACS protocol

Operation	Command
Display the configuration information of the specified or all the ISP domains	display domain [<i>isp-name</i>]
Display related information of user's connection	display connection { access-type { dot1x gcm } domain <i>isp-name</i> hwtacacs-scheme <i>hwtacacs-scheme-name</i> interface <i>interface-type interface-number</i> ip <i>ip-address</i> mac <i>mac-address</i> radius-scheme <i>radius-scheme-name</i> vlan <i>vlanid</i> ucibindex <i>ucib-index</i> user-name <i>user-name</i> }
Display related information of the local user	display local-user [domain <i>isp-name</i> idle-cut { disable enable } service-type { ftp lan-access ppp ssh telnet terminal } state { active block } user-name <i>user-name</i> vlan <i>vlanid</i>]
Display the statistics of local RADIUS server group	display local-server { statistics nas-ip }
Display the configuration information of all the RADIUS server groups or a specified one	display radius [<i>radius-server-name</i>]

Table 242 Display and debug AAA and RADIUS/HWTACACS protocol

Operation	Command
Display all global NAS-IP information configured in system view	display radius nas-ip
Display the statistics of RADIUS packets	display radius statistics
Display the stop-accounting requests saved in buffer without response	display stop-accounting-buffer { radius-scheme <i>radius-scheme-name</i> session-id <i>session-id</i> time-range <i>start-time stop-time</i> user-name <i>user-name</i> }
Reset the statistics of RADIUS server	reset radius statistics
Display the specified or all the HWTACACS schemes	display hwtacacs [<i>hwtacacs-server-name</i>]
Display the HWTACACS stop-accounting requests saved in buffer without response	display stop-accounting-buffer hwtacacs-scheme <i>hwtacacs-scheme-name</i>
Delete the stop-accounting requests saved in buffer without response	reset stop-accounting-buffer { radius-scheme <i>radius-scheme-name</i> session-id <i>session-id</i> time-range <i>start-time stop-time</i> user-name <i>user-name</i> }
Delete the HWTACACS stop-accounting requests saved in buffer without response	reset stop-accounting-buffer hwtacacs-scheme <i>hwtacacs-scheme-name</i>
Reset the statistics of HWTACACS server	reset hwtacacs statistics { accounting authentication authorization all }
Enable RADIUS packet debugging	debugging radius packet
Disable RADIUS packet debugging	undo debugging radius packet
Enable debugging of local RADIUS authentication server	debugging local-server { all error event packet }
Disable debugging of local RADIUS authentication server	undo debugging local-server { all error event packet }
Enable HWTACACS debugging	debugging hwtacacs { all error event message receive-packet send-packet }
Disable HWTACACS debugging	undo debugging hwtacacs { all error event message receive-packet send-packet }

AAA and RADIUS/HWTACACS Protocol Configuration Examples

For the hybrid configuration example of AAA/RADIUS/HWTACACS protocol and 802.1x protocol, refer to the part "802.1x".

Perform the following configuration in system view.

Table 243 Enable/disable the anti-attack function of packets

Operation	Command
Enable/disable the anti-attack function of packets	anti-attack { arp dot1x ip } { disable enable }

The anti-attack function of IP packets is enabled while the anti-attack function of ARP packets and dot1x packets are disabled by default.

Configuring Authentication at Remote RADIUS Server



Configuring Telnet user authentication at the remote server is similar to configuring FTP users. The following description is based on Telnet users.

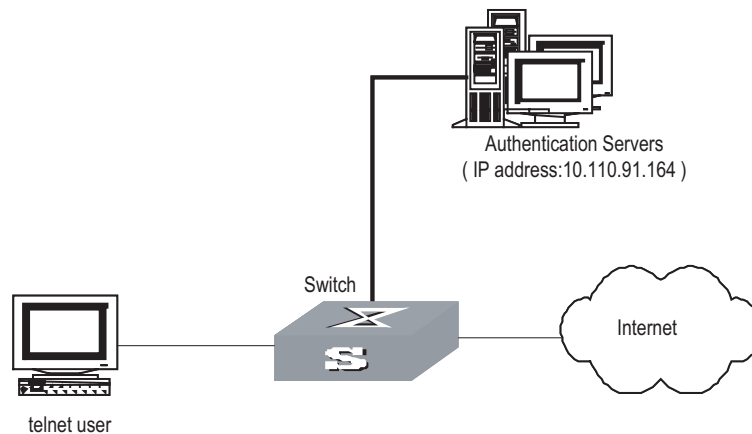
Network Requirements

In the environment as illustrated in the following figure, it is required to achieve through proper configuration that the RADIUS server authenticates the Telnet users to be registered.

One RADIUS server (as authentication server) is connected to the switch and the server IP address is 10.110.91.146. The password for exchanging messages between the switch and the authentication server is "expert". The switch cuts off domain name from username and sends the left part to the RADIUS server.

Network Topology

Figure 63 Network diagram for the remote RADIUS authentication of Telnet users



Configuration procedure

Add a Telnet user.

Omitted



For details about configuring FTP and Telnet users, refer to User Interface Configuration of Getting Started Operation part in Switch 8800 Family Series Routing Switches Operation Manual.

Configure remote authentication mode for the Telnet user, i.e. Scheme mode.

```
[3Com-ui-vty0-4] authentication-mode scheme
```

Configure RADIUS scheme.

```
[SW8800] radius scheme cams
[3Com-radius-cams] primary authentication 10.110.91.146 1812
[3Com-radius-cams] key authentication expert
[3Com-radius-cams] server-type 3Com
[3Com-radius-cams] user-name-format without-domain
```

```
# Associate the domain with RADIUS.
```

```
[3Com-radius-cams] quit
[SW8800] domain cams
[3Com-isp-cams] radius-scheme cams
```

Configuring Authentication at Local RADIUS Authentication Server

Local RADIUS authentication of Telnet/FTP users is similar to the remote RADIUS authentication described in section “Configuring Authentication at Remote RADIUS Server” . But you should modify the server IP address in Figure 63 of section “Configuring Authentication at Remote RADIUS Server” to 127.0.0.1, authentication password to 3Com, the UDP port number of the authentication server to 1645.



For details about local RADIUS authentication of Telnet/FTP users, refer to the section “Setting the Port State of RADIUS Client” “Setting the Port State of RADIUS Client”.

Configuring Authentication at Remote TACACS Server

Network requirements

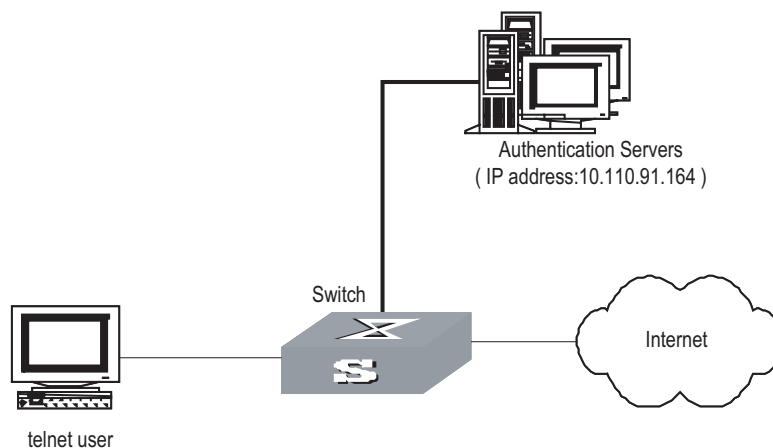
Configure the switch to use a TACACS server to provide authentication and authorization services to login users (see the following figure).

Connect the switch to one TACACS server (which acting as a AAA server) with the IP address 10.110.91.164. On the switch, set the shared key for AAA packet encryption to "expert" . Configure the switch to send usernames to the TACACS server with *isp-name* removed.

On the TACACS server, set the shared key for encrypting the packets exchanged with the switch to "expert" .

Network diagram

Figure 64 Network diagram for TACACS authentication



Configuration procedure

```
# Configure the Telnet user.
```

Here it is omitted.



The configuration of the FTP and Telnet users can refer to *User Interface Configuration of Getting Started Operation part in Switch 8800 Family Series Routing Switches Operation Manual*.

Configure a HWTACACS scheme.

```
[SW8800] hwtacacs scheme hwtac
[3Com-hwtacacs-hwtac] primary authentication 10.110.91.164
[3Com-hwtacacs-hwtac] primary authorization 10.110.91.164
[3Com-hwtacacs-hwtac] key authentication expert
[3Com-hwtacacs-hwtac] key authorization expert
[3Com-hwtacacs-hwtac] user-name-format without-domain
[3Com-hwtacacs-hwtac] quit
```

Associate the Domain with the HWTACACS scheme.

```
[SW8800] domain hwtacacs
[3Com-isp-hwtacacs] scheme hwtacacs-scheme hwtac
```

Troubleshooting AAA and RADIUS/HWTACACS

RADIUS/HWTACACS protocol is located on the application layer of TCP/IP protocol suite. It mainly specifies how to exchange user information between NAS and RADIUS/HWTACACS server of ISP. So it is very likely to be invalid.

Symptom: User authentication/authorization always fails

Solution:

- The username may not be in the `userid@isp-name` format or NAS has not been configured with a default ISP domain. Please use the username in proper format and configure the default ISP domain on NAS.
- The user may have not been configured in the RADIUS/HWTACACS server database. Check the database and make sure that the configuration information of the user does exist in the database.
- The user may have input a wrong password. So please make sure that the supplicant inputs the correct password.
- The encryption keys of RADIUS/HWTACACS server and NAS may be different. Please check carefully and make sure that they are identical.
- There might be some communication fault between NAS and RADIUS/HWTACACS server, which can be discovered through pinging RADIUS/HWTACACS server from NAS. So please ensure the normal communication between NAS and RADIUS/HWTACACS server.

Symptom: RADIUS/HWTACACS packet cannot be transmitted to RADIUS/HWTACACS server.

Solution:

- The communication lines (on physical layer or link layer) connecting NAS and RADIUS/HWTACACS server may not work well. So please ensure the lines work well.
- The IP address of the corresponding RADIUS/HWTACACS server may not have been set on NAS. Please set a proper IP address for RADIUS/HWTACACS server.

- Ports of authentication/authorization and accounting services may not be set properly. So make sure they are consistent with the ports provided by RADIUS/HWTACACS server.

Symptom: After being authenticated and authorized, the user cannot send charging bill to the RADIUS/HWTACACS server.

Solution:

- The accounting port number may be set improperly. Please set a proper number.
- The accounting service and authentication/authorization service are provided on different servers, but NAS requires the services to be provided on one server (by specifying the same IP address). So please make sure the settings of servers are consistent with the actual conditions.

27

PORTAL CONFIGURATION

Portal Overview

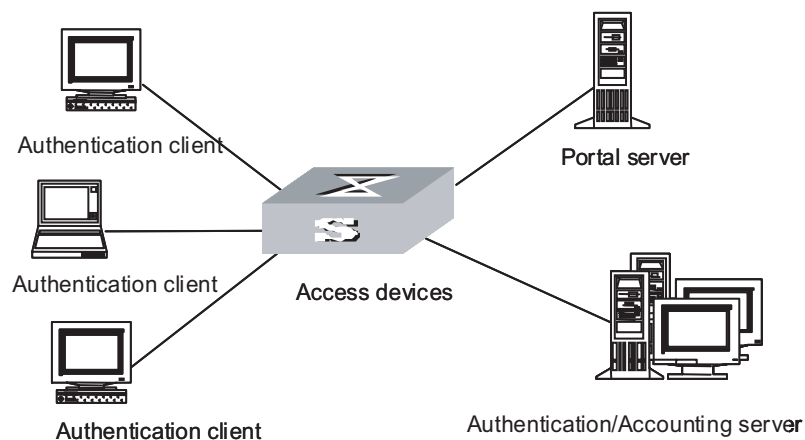
Introduction Portal is also known as portal website, and Portal authentication is also known as the Web authentication. Its major advantages are:

- Users need not install any client software;
- It is powerful in its ability to support new services. With the help of Portal authentication, the operators can provide services such as information query, online shopping based on Portal.

The principle of Portal is: Unauthenticated users can access only specified website servers, and any other access is redirected to the Portal server unconditionally. Users can access the Internet only after they are successfully authenticated.

Portal Structure The basic network diagram of Portal is shown in Figure 65. It is composed of four elements: authentication client, access device, Portal server, and authentication/accounting server.

Figure 65 Portal structure



- Authentication client is the Internet Web Browser where the HTTP/HTTPS protocols run. All the HTTP requests are submitted to the Portal server before the user passes the authentication.
- Access device unconditionally forces the HTTP requests of authentication client to the Portal server before the user passes the authentication. The access device interacts with the authentication/accounting server to implement the authentication and accounting function. Access devices refer to 3Com Switch 8800 Family series switches in this book.

- Portal server is a Web server. Users can access it by using standard WWW browsers. The portal server provides free portal service and Web-authentication-based interface. The access device exchanges the authentication information of the authentication client with the Portal server. Internet content provider (ICP) can provide related information about its own website to users through this website.
- Authentication/accounting server implements the authentication and accounting function for the users. The access device interacts with the authentication/accounting server through the RADIUS protocol.

Portal Authentication Procedure

Portal authentication procedure on 3Com series switches is:

- When the switch receives the login user's HTTP packets for the first time, it will judge whether this user is Portal user at first. For Portal users, the switch allows the user to access only the contents of the specified website servers (the Portal server and the authentication-free addresses).
- For the HTTP packets of the Portal user to access other websites, the switch will redirect them to the Portal server in the way of TCP cheat.
- The Portal server provides a Web interface for users to input usernames and passwords. The input usernames and passwords are forwarded to the switch through the Portal server.
- The switch sends the usernames and passwords to the authentication server for authentication. The switch allows a user to access Internet only after he passes the authentication, and then the switch will not redirect HTTP packets of this user.



CAUTION: *Portal and 802.1x cannot be enabled on the same switch at the same time.*

Running Methods of Portal

In 3Com series switches, Portal runs in one of the following three methods: Direct authentication method, ReDHCP authentication method and Layer 3 authentication method.

- Direct authentication method: In this method, the user gets a public address directly. Before passing authentication, the user can access only the Portal server and the set authentication-free addresses. The user can access Internet after passing authentication.
- ReDHCP authentication method: In this method, the user gets a private address through DHCP before passing authentication. Before passing authentication, the user can access only the Portal server and the set authentication-free addresses. The user can apply for a public address and access Internet after passing authentication.
- Layer 3 Portal authentication method: This method expands the Direct authentication method. In this method, the user can access the Portal-enabled switch across network segments.



- Considering security problems, both the Direct authentication method and the ReDHCP authentication method require checking MAC addresses of the user. So Portal can be enabled only on the first Layer 3 interface that the user

accesses. That is to say, Layer-3-protocol-enabled network devices cannot exist between the user and the access devices.

- The Layer 3 Portal authentication method does not check MAC addresses of the user, so the security performance is reduced. . You are not recommended to use the Layer 3 Portal authentication method in occasions requiring high security performance.

Portal Authentication-free Users and Free IP Addresses

Authentication-free users

Authentication-free users are users that can access Internet without Portal authentication. In the network practice, you can configure network devices attached to the switch or several servers as authentication-free users, so that they can access Internet without authentication.

The information about authentication-free users includes IP addresses, MAC addresses, and the connected switch ports and VLANs. Only the users who match all the information can access Internet without authentication.

Free IP addresses

Free IP addresses are IP addresses that the user can access unrestrictedly. Free IP addresses can be the IP addresses of DNS servers or the IP addresses that ISP provides to access free websites. All users can access these free IP addresses unrestrictedly.

ARP Packet Handshake between the User PC and the Switch

When authentications are performed in the Direct method or ReDHCP method, the switch handshakes with the user PC through ARP packets after the user has passed Portal authentication. If the switch finds the handshake abnormal, it will cut the connection with the user actively and notice the Portal server about this case.



CAUTION:

- When the Portal user is online, DHCP Relay Security Check cannot be configured.
- If you want to configure DHCP Relay Security Check, you must enable it when configuring Portal.

Portal Rate Limit Function

The Portal rate limit function is used together with the bandwidth limit service that the CAMS server provides. The bandwidth limit service is that you can specify the bandwidth for each user when you are configuring the service for each user on the CAMS server.

The principle of Portal rate limit is as follows: when the switch receives the bandwidth limit rules for Portal users from the CAMS server, the switch will limit the traffic on the specified upload interface, that is to say, the switch will perform bandwidth control for the upload rates of Portal users.



- An upload interface is the interface to connect the switch with the upstream network devices.
- The system supports only one upload interface for rate limit.

Basic Portal Configuration

Configuration Prerequisites

- A valid IP address has been configured for this portal-enabled VLAN interface.
- 802.1x is not enabled on the switch.
- The Portal server has been installed and configured. Refer to *CAMS Portal Service Components User's Guide* for details about installation and configuration.



- Refer to the "Network Protocol" section in *3Com Switch 8800 Family Series Routing Switches-Operation Manual* for DHCP configuration.
- Refer to Chapter 2 AAA&RADIUS Protocol Configuration for AAA&RADIUS configuration.

Basic Portal Configuration Procedure

The following table describes the basic Portal configuration procedure.

Table 244 Basic Portal configuration procedure

Operation	Command	Description
Enter system view	system-view	-
Configure the Portal server	portal server <i>server-name</i> { ip <i>ip-address</i> key <i>key-string</i> port <i>port</i> url <i>url-string</i> } *	Required No Portal server is configured by default. When a Portal server is configured, the <i>key-string</i> is 3Com, the port is 50100 and the <i>url-string</i> is the string format of <i>ip-address</i> by default.
Configure the running method of Portal	portal method { direct layer3 redhcp }	Optional The direct authentication method is adopted in Portal authentication by default.
Configure the authentication network segment	portal auth-network <i>network-address net-mask</i> vlan <i>vlan-id</i>	This command must be configured if the Layer 3 authentication method is adopted in Portal authentication. This procedure is omitted in other methods. Optional
Configure the interval of handshakes with user PCs and the maximum retry times	portal arp-handshake { interval <i>interval</i> retry-times <i>retry-times</i> } *	Optional This task is effective only for the Direct authentication method and the ReDHCP authentication method. By default, the interval of ARP handshakes is 60 seconds, and the maximum retry times is five times.
Enter VLAN interface view	interface vlan-interface <i>vlan-id</i>	The following displayed information in VLAN interface view is corresponding to the input <i>vlan-id</i>

Table 244 Basic Portal configuration procedure

Operation	Command	Description
Enable Portal authentication on a VLAN interface	portal <i>server-name</i>	Required
Display the statistics about the state machines about authentication, connection and management	display portal { acm server tcp-cheat } statistics	-
Display the information about Portal authentication network segment	display portal [auth-network [<i>auth-vlan-id</i>]] free-ip free-user server [<i>server-name</i>] vlan [<i>vlan-id</i>]]	-
Display the information about the Portal users	display portal user [ip <i>ipaddress</i> interface <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-id</i>]	-
Clear the statistics about Portal	reset portal { acm server tcp-cheat } statistics	-

**CAUTION:**

- When a Portal server is first configured, you must configure the IP address for it.
- If a Portal server has been enabled on a VLAN interface, you must disable this Portal server on the VLAN interface before modifying its parameters.
- When Portal authentication is enabled, 802.1x protocol must be disabled globally.
- The name of the specified Portal server must exist.
- When the Layer 3 authentication method is adopted, a default route must be configured on the layer 3 device between Portal users and the Portal-enabled switch.
- When the ReDHCP authentication method is adopted, the Portal-enabled switches can only be configured as DHCP Relay instead of DHCP Server.
- When Portal is enabled on a VLAN interface, it is forbidden to configure any more ACL rules related with this network segment on this VLAN interface (and the corresponding ports). Otherwise, the Portal function may be caused abnormal.

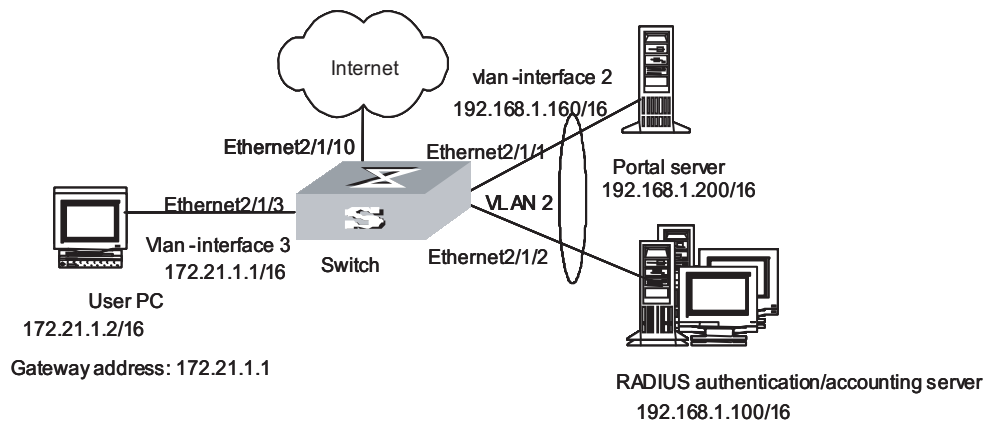
Portal Direct Authentication Method Configuration Example

Network requirements

- Portal is enabled on the switch and Portal runs in the Direct authentication method.
- The switch uses a RADIUS server to implement authentication and accounting.
- Users can access only the Portal server before passing Portal authentication.
- Users can access external networks after passing Portal authentication.

Network diagram

Figure 66 Network diagram for Portal Direct authentication method



Configuration procedure



Only the configurations on switches are listed below. Configurations on the Portal servers and RADIUS authentication/accounting servers are not described here.

1 Configure the RADIUS scheme

Create a RADIUS scheme named portal

```
[SW8800] radius scheme portal
```

Set the server type of this RADIUS scheme as Portal

```
[3Com-radius-portal] server-type portal
```

Set the primary authentication and accounting servers of this RADIUS scheme and their communication keys

```
[3Com-radius-portal] primary authentication 192.168.1.100
[3Com-radius-portal] primary accounting 192.168.1.100
[3Com-radius-portal] key accounting hello
[3Com-radius-portal] key authentication hello
[3Com-radius-portal] user-name-format without-domain
[3Com-radius-portal] quit
```

2 Configure ISP domain

Create an ISP domain named portal

```
[SW8800] domain portal
```

This ISP domain uses the RADIUS scheme named portal

```
[3Com-isp-portal] radius-scheme portal
[3Com-isp-portal] quit
```

Set portal as the default ISP domain of the system (optional)

```
[SW8800] domain default enable portal
```


3 Configure Portal authentication

Configure the portal server. Its name is newp, IP address is 192.168.1.200, key is 3Com, port is 50100, and URL is http://192.168.1.200:81/portal/index_page.jsp

```
[SW8800] portal server newp ip 192.168.1.200 key 3Com port 50100 url
http://192.168.1.200/portal/index_default.jsp
```

Set the Portal to run in the Direct authentication method

```
[SW8800] portal method direct
```

4 Enable Portal authentication on the VLAN interface connected with the user PC

Configure VLAN 2

```
[SW8800] vlan 2
[3Com-vlan2] port ethernet 2/1/1 ethernet 2/1/2
[SW8800] interface vlan-interface 2
[3Com-Vlan-interface2] ip address 192.168.1.160 255.255.0.0
[3Com-Vlan-interface2] quit
```

Configure VLAN 3

```
[SW8800] vlan 3
[3Com-vlan3] port ethernet 2/1/3
[3Com-vlan3] quit
[SW8800] interface vlan-interface 3
[3Com-Vlan-interface3] ip address 172.21.1.1 255.255.0.0
```

Enable Portal authentication on VLAN interface 3

```
[3Com-Vlan-interface3] portal newp
```

Portal ReDHCP Authentication Method Configuration Example

Network requirements

- Portal is enabled on the switch and Portal runs in the ReDHCP authentication method.
- Configure address pools on the DHCP server: 172.21.0.0/16 for public networks and 18.21.0.0/16 for private networks.
- The user was assigned a private address before passing Portal authentication. The user can access the external networks only after the user applies for a public address after passing Portal authentication.

Network diagram

Refer to Figure 66.

Configuration procedure



- Only the configurations related to the Portal ReDHCP authentication method are listed below. Refer to “Portal Direct Authentication Method Configuration Example” for the configurations on RADIUS schemes, ISP domains and Portal servers.

- When the Portal ReDHCP authentication method is adopted, the switch must be configured as DHCP Relay instead of DHCP Server. Additionally, the master IP address (public address) and the slave IP address (private IP address) must be configured on the Portal-enabled VLAN interface.

Set the Portal to run in the ReDHCP authentication method.

```
[SW8800] portal method redhcp
```

Configure the DHCP server.

```
[SW8800] dhcp server ip-pool dhcp_ip
[3Com-dhcp-dhcp_ip] network 172.21.0.0 mask 255.255.0.0
[3Com-dhcp-dhcp_ip] gateway-list 172.21.1.1
[3Com-dhcp-dhcp_ip] quit
[SW8800] dhcp server ip-pool dhcp_ip2
[3Com-dhcp-dhcp_ip2] network 18.21.0.0 mask 255.255.0.0
[3Com-dhcp-dhcp_ip2] gateway-list 18.21.1.1
[3Com-dhcp-dhcp_ip2] quit
```

Configure VLAN 3

```
[SW8800] vlan 3
[3Com-vlan3] port ethernet 2/1/3
[SW8800] interface vlan-interface 3
[3Com-Vlan-interface3] ip address 172.21.1.1 255.255.0.0
[3Com-Vlan-interface3] ip address 18.21.1.1 255.255.0.0 sub
```

Configure the DHCP Relay address check (ip relay address must be specified as a VLAN interface in Up state).

```
[3Com-Vlan-interface3] ip relay address 9.0.0.1
[3Com-Vlan-interface3] dhcp select relay
[3Com-Vlan-interface3] dhcp relay security address-check enable
```

Enable Portal authentication function on VLAN-interface 3. The name of the Portal server is newp. Refer to "Portal Direct Authentication Method Configuration Example" for related configurations.

```
[3Com-Vlan-interface3] portal newp
```

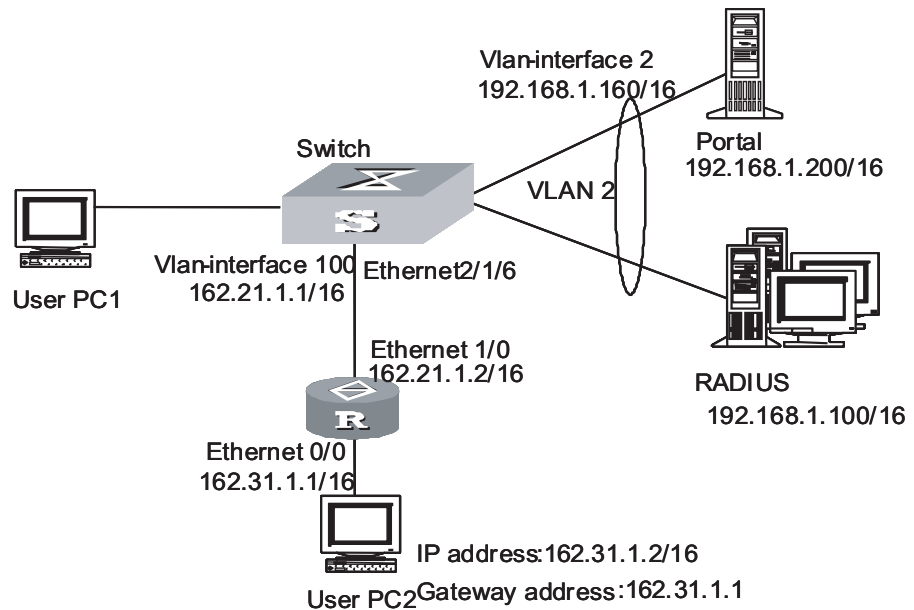
Layer 3 Portal Authentication Method Configuration Example

Network requirements

- The user PC2 accesses the switch through a router. Layer 3 Portal authentication method is enabled on the switch. User PC2 can access external networks after passing Portal authentication.

Network diagram

Figure 67 Network diagram for Layer 3 Portal authentication method



Configuration procedure



Only the configurations related to the Layer 3 Portal authentication method are listed below. Refer to “Portal Direct Authentication Method Configuration Example” for the configurations on RADIUS schemes, ISP domains and Portal servers.

Configure the authentication network segment

```
[SW8800] portal auth-network 162.31.0.0 255.255.0.0 vlan 100
```

Set the Portal to run in the Layer 3 Portal authentication method

```
[SW8800] portal method layer3
```

Configure VLAN 100

```
[SW8800] vlan 100
[3Com-vlan100] port ethernet 2/1/6
[3Com-vlan100] quit
[SW8800] interface vlan-interface 100
[3Com-Vlan-interface100] ip address 162.21.1.1 255.255.0.0
```

Enable Portal authentication function on VLAN-interface 100. The name of the Portal server is newp. Refer to section “Portal Direct Authentication Method Configuration Example” “Portal Direct Authentication Method Configuration Example” for related configurations.

```
[3Com-Vlan-interface100] portal newp
```

Portal Authentication-free User and Free IP Address Configuration

Configuration Prerequisites

The prerequisite of Portal authentication-free user and free IP address configuration-the basic Portal configuration has been finished.

Portal Authentication-free User and Free IP Address Configuration Procedure

Portal authentication-free user and free IP address configuration is optional. The following table describes its configuration procedure:

Table 245 Portal authentication-free user and free IP address configuration procedure

Operation	Command	Description
Enter system view	system-view	-
Configure free IP addresses	portal free-ip <i>ip-address [mask mask-length]</i>	Up to eight free IP addresses can be configured. The Portal server will use one free IP address automatically
Configure authentication-free users	In system view portal free-user mac <i>mac-address ip ip-address vlan-id interface interface-type interface-num</i> In port view. portal free-user mac <i>mac-address ip ip-address vlan-id</i>	Up to 32 authentication-free users can be configured; The current port is used when this command is configured on a port. You need not specify the interface keyword
Display the information about Portal authentication-free user and free IP address configuration	display portal [free-ip free-user]	-



CAUTION:

- The ReDHCP authentication method requires that the IP address of an authentication-free user and the master IP address of the interface belong to the same network segment. The Direct authentication method requires that the IP address of an authentication-free user and that of the VLAN interface belong to the same network segment.
- This configuration takes effect after Portal is enabled in the VLAN that the authentication-free users belongs to.
- The Layer 3 Portal authentication method does not support the authentication-free user configuration.

Authentication-free User and Free IP Address Configuration Example

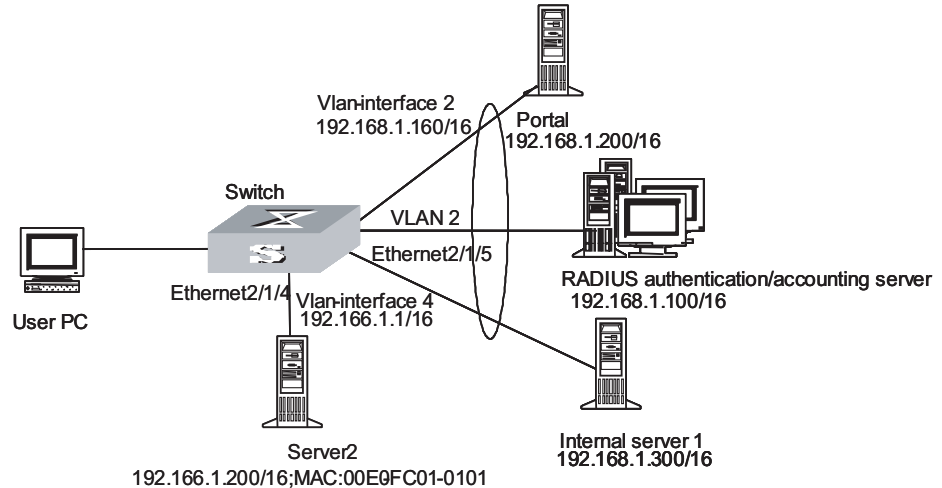
Network requirements

- Portal is enabled on the switch and Portal runs in the Direct authentication method.
- The user can access the internal server Server1 before passing Portal authentication.

- Server2 can access Internet without passing the authentication.

Network diagram

Figure 68 Network diagram for authentication-free user and free IP address configuration



Configuration procedure



The following configurations are based on configurations in section “Portal Direct Authentication Method Configuration Example” “Portal Direct Authentication Method Configuration Example” and the same configurations are not listed below.

1 Configure authentication-free users

Configure VLAN4 and enable Portal on the VLAN interface 4

```
[SW8800] vlan 4
[3Com-vlan4] port ethernet 2/1/4
[3Com-vlan4] quit
[SW8800] interface vlan-interface 4
[3Com-Vlan-interface4] ip address 192.166.1.1 255.255.0.0
[3Com-Vlan-interface4] portal newp
[3Com-Vlan-interface4] quit
```

Configure Server1 as an authentication user

```
[SW8800] portal free-user mac 00E0-FC01-0101 ip 192.166.1.200 vlan
4 interface ethernet 2/1/4
```

2 Configure free IP addresses

Add Ethernet2/1/5 into the VLAN2 configured in “Portal Direct Authentication Method Configuration Example”

```
[SW8800] vlan 2
[3Com-vlan2] port ethernet 2/1/5
[3Com-vlan2] quit
```

Configure Server1 as a free IP address

```
[SW8800] portal free-ip 192.168.1.300
```

Portal Rate Limit Function Configuration

Portal Rate Limit Function Configuration Procedure

Table 246 Portal rate limit function configuration procedure

Operation	Command	Description
Enter system view	system-view	-
Enter interface view	interface Ethernet X/X/X	-
Configure the Portal rate limit function on upload interfaces	portal upload interface	By default, the Portal rate limit function is disabled.

Portal Rate Limit Function Configuration Example

Network requirements

- The upload interface for Portal rate limit is specified.

Network diagram

Refer to Figure 66.

Configuration procedure

Specify Ethernet2/1/10 as the upload interface for Portal rate limit.

```
[3Com-Ethernet2/1/10]portal upload-interface
```

Portal User Deletion

Portal User Deletion Procedure

Table 247 Portal user deletion procedure

Operation	Command	Description
Enter system view	system-view	-
Delete the Portal user using the specified IP address	portal delete-user ip-address	-

Portal User Deletion Configuration Procedure

Network requirements

- Delete the Portal user using the IP address 172.31.1.2.

Configuration procedure

Delete the user using the IP address 172.31.1.2

```
[SW8800] portal delete-user 172.31.1.2
```

28

IP ROUTING PROTOCOL OVERVIEW



A router that is referred to in the following or its icon represents a generalized router or an Switch 8800 Family series routing switch running routing protocols. To improve readability, this will not be described in the other parts of the manual.

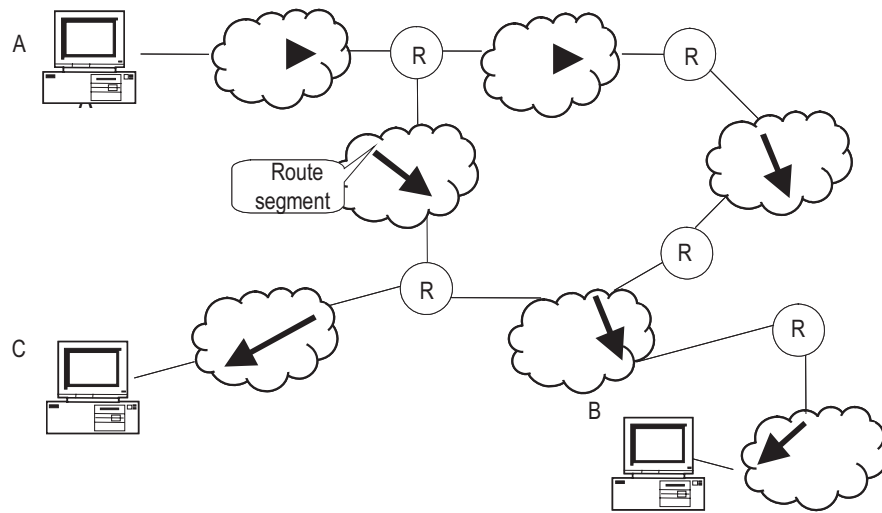
For the configuration of VPN instance, refer to the MPLS module in *3Com Switch 8800 Family Series Routing Switches Operation Manual*.

Introduction to IP Route and Routing Table

IP Route and Route Segment

Routers are implemented for route selection in the Internet. A router works in the following way: The router selects an appropriate path (through a network) according to the destination address of the packet it receives and forwards the packet to the next router. The last router in the path is responsible for submitting the packet to the destination host.

In Figure 69, R stands for a router. A packet sent from Host A to Host C should go through two routers and the packet is transmitted through two hops. Therefore, when a node (router) is connected to another node through a network, they are in the same route segment and are deemed as adjacent in the Internet. That is, the adjacent routers refer to two routers connected to the same network. The number of route segments between a router and hosts in the same network counted as zero. In Figure 69, the bold arrows represent these route segments. Which physical links comprise which route segment is not a concern of a router however.

Figure 69 The concept of route segment

As the networks may have different sizes, the segment lengths connected between two different pairs of routers are also different. The number of route segments multiplies a weighted coefficient can serve as a weighted measurement for the actual length of the signal transmission path.

If a router in a network is regarded as a node and a route segment in the Internet is regarded as a link, message routing in the Internet works in a similar way as the message routing in a conventional network. Message routed through the shortest route may not always be the optimal route. For example, routing through three high-speed LAN route segments may be much faster than that through two low-speed WAN route segments.

Route Selection through the Routing Table

The key for a router to forward packets is the routing table. Each router saves a routing table in its memory, and each entry of this table specifies the physical port of the router through which the packet is sent to a subnet or a host. Therefore, it can reach the next router via a particular path or reach a destination host via a directly connected network.

A routing table has the following key entries:

- **Destination address:** It is used to identify the destination IP address or the destination network of an IP packet.
- **Network mask:** Combined with the destination address, it is used to identify the network address of the destination host or router. If the destination address is ANDed with the network mask, you will get the address of the network segment where the destination host or router is located. For example, if the destination address is 129.102.8.10, the address of the network where the host or the router with the mask 255.255.0.0 is located will be 129.102.0.0. It is made up of several consecutive "1"s, which can also be expressed in the dotted decimal format.
- **Output interface:** It indicates an interface through which an IP packet should be forwarded.

- Next hop address: It indicates the IP address of the next router that an IP packet will pass through.
- Priority added to the IP routing table for a route: There may be different next hops to the same destination. These routes may be discovered by different routing protocols, or they can just be the static routes configured manually. The one with the highest priority (the smallest numerical value) is selected as the current optimal route.
- Path cost: Cost to forward data over the route.

According to different destinations, the routes can be divided into:

- Subnet route: The destination is a subnet.
- Host route: The destination is a host

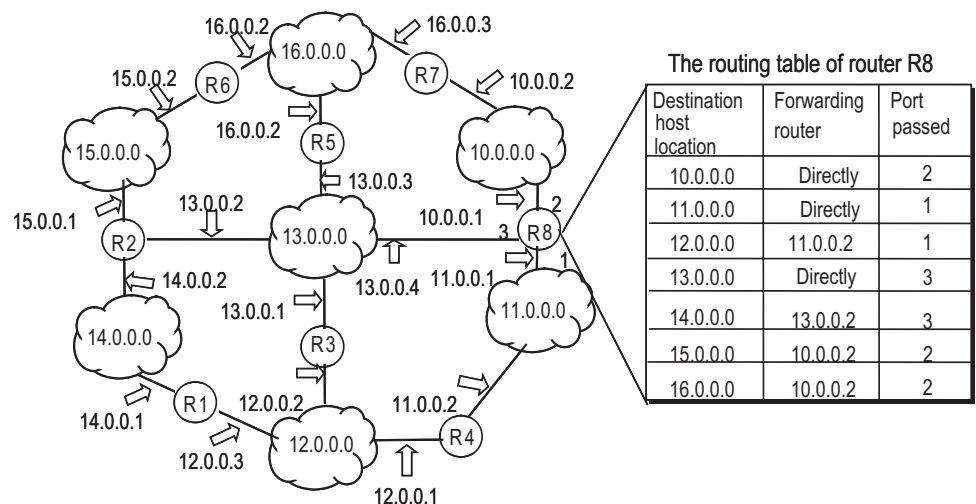
In addition, according to whether the network of the destination host is directly connected to the router, there are the following types of routes:

- Direct route: The router is directly connected to the network where the destination resides.
- Indirect route: The router is not directly connected to the network where the destination resides.

In order to limit the size of the routing table, an option is available to set a default route. All the packets that fail to find the suitable entry will be forwarded through this default route.

In a complicated Internet as shown in Figure 70, the number in each network is the network address, and R stands for a router. The router R8 is directly connected with three networks, so it has three IP addresses and three physical ports, and its routing table is shown in the diagram below:

Figure 70 The routing table



The 3Com Switch 8800 Family Series Routing Switches (hereinafter referred to as Switch 8800 Family series) support the configuration of a series of dynamic routing protocols such as RIP, OSPF, IS-IS and BGP, as well as the static routes. In

addition, the running switch will automatically obtain some direct routes according to the port state and user configuration.

Routing Management Policy

For Switch 8800 Family series, you can configure manually the static route to a specific destination, and configure dynamic routing protocol to interact with other routers on the network. The routing algorithm can also be used to discover routes. For the configured static routes and dynamic routes discovered by the routing protocol, the Switch 8800 Family series implement unified management. That is, the static routes configured by the user are managed together with the dynamic routes discovered by the routing protocol. The static routes and the routes learned or configured by different routing protocols can also be shared with each other.

Routing Protocols and the Preferences of the Corresponding Routes

Different routing protocols (as well as the static configuration) may generate different routes to the same destination, but not all these routes are optimal. In fact, at a certain moment, only one routing protocol can determine a current route to a specific destination. Thus, each of these routing protocols (including the static configuration) is set with a preference, and when there are multiple routing information sources, the route discovered by the routing protocol with the highest preference will become the current route. Routing protocols and the default preferences (the smaller the value is, the higher the preference is) of the routes learned by them are shown in Table 248.

In the table, 0 indicates a direct route. 255 indicates any route from unreliable sources.

Table 248 Routing protocols and the default preferences for the routes learned by them

Routing protocol or route type	The preference of the corresponding route
DIRECT	0
OSPF	10
IS-IS	15
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
IBGP	256
EBGP	256
UNKNOWN	255

Apart from direct routing, IBGP and EBGP, the preferences of various dynamic routing protocols can be manually configured to meet the user requirements. In addition, the preferences for individual static routes can be different.

Supporting Load Sharing and Route Backup

Load sharing

The Switch 8800 Family series support static equivalent route, permitting to configure multiple routes that reach the same destination and use the same precedence. After you configured static equivalent routes, a packet can reach the same destination through multiple different paths, whose precedence levels are equal. When there is no route that can reach the same destination with a higher

precedence, the multiple routes will be adopted. Thus, the router will forward the packets to the destination through these paths according to a certain algorithm so as to implement load sharing.

For the same destination, a specified routing protocol may find multiple different routes with the same precedence and different next hops. If the routing protocol has the highest precedence among all active routing protocols, these multiple routes will be regarded as currently valid routes. Thus, load sharing of IP traffic is ensured in terms of routing protocols.

By far, Switch 8800 Family series support eight routes to implement load sharing.

Route backup

The Switch 8800 Family series support route backup. When the main route fails, the system will automatically switch to a backup route to improve the network reliability.

In order to achieve static route backup, the user can configure multiple routes to the same destination according to actual situations. One of the routes has the highest precedence and is called as main route. The other routes have descending precedence levels and are called as backup routes. Normally, the router sends data via main route. When the line fails, the main route will hide itself and the router will choose one from the left routes as a backup route whose precedence is higher than others' to send data. In this way, the switchover from the main route to the backup route is implemented. When the main route recovers, the router will restore it and re-select route. As the main route has the highest precedence, the router still chooses the main route to send data. This process is the automatic switchover from the backup route to the main route.

Routes Shared Between Routing Protocols

As the algorithms of various routing protocols are different, different protocols may generate different routes, thus bringing about the problem of how to resolve the differences when different routes are generated by different routing protocols. The Switch 8800 Family series support the import of routes discovered by one routing protocol into another. Each protocol has its own route importing mechanism. For details, refer to the description about "Importing an External Route" in the operation manual of the corresponding routing protocol.

29

STATIC ROUTE CONFIGURATION

Introduction to Static Route

Static Route A static route is a special route configured manually by an administrator. You can set up an interconnecting network with the static route configuration. The problem for such configuration is when a fault occurs to the network, the static route cannot change automatically to steer away from the node causing the fault, if without the help of an administrator.

In a relatively simple network, you only need to configure the static routes to make the router work normally. The proper configuration and usage of the static route can improve the network performance and ensure the bandwidth of the important applications.

All the following routes are static routes:

- Reachable route: A normal route is of this type. That is, the IP packet is sent to the next hop via the route marked by the destination. It is a common type of static routes.
- Unreachable route: When a static route to a destination has the "**reject**" attribute, all the IP packets to this destination will be discarded, and the source host will be informed that the destination is unreachable.
- Blackhole route: If a static route to a destination has the "**blackhole**" attribute, the outgoing interface of this route is the Null 0 interface regardless of the next hop address, and any IP packets addressed to this destination are dropped without notifying the source host.

The attributes "**reject**" and "**blackhole**" are usually used to control the range of reachable destinations of this router, and help troubleshooting the network.

Default Route A default route is a special route. You can configure a default route using a static route. Some dynamic routing protocols can also generate default routes, such as OSPF and IS-IS.

In brief, a default route is used only when no suitable routing table entry is matched. That is, when no proper route is found, the default route is used. In a routing table, the default route is in the form of the route to the network 0.0.0.0 (with the mask 0.0.0.0). You can see whether the default route has been set by executing the **display ip routing-table** command. If the destination address of a packet fails in matching any entry of the routing table, the router will select the default route to forward this packet. If there is no default route and the destination address of the packet fails in matching any entry in the routing table,

this packet will be discarded, and an internet control message protocol (ICMP) packet will be sent to the originating host to inform that the destination host or network is unreachable.

Configuring Static Route

Static Route Configuration includes:

- “Configuring a Static Route”
- “Configuring a Default Route”
- “Deleting All the Static Routes”

Configuring a Static Route

Perform the following configurations in system view.

Table 249 Configure a static route

Operation	Command
Add a static route	ip route-static [vpn-instance <i>vpn-instance-name-list</i>] <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-type</i> <i>interface-number</i> } [vpn-instance <i>vpn-instance-name</i>] <i>gateway-address</i> } [preference <i>preference-value</i>] [reject blackhole]
Delete a static route	undo ip route-static [vpn-instance <i>vpn-instance-name-list</i>] <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-type</i> <i>interface-number</i> } [vpn-instance <i>vpn-instance-name</i>] <i>gateway-address</i> } [preference <i>preference-value</i>] [reject blackhole]

The parameters are explained as follows:

- IP address and mask

The IP address and mask are in a dotted decimal format. As "1"s in the 32-bit mask is required to be consecutive, the dotted decimal mask can also be replaced by the *mask-length* (which refers to the digits of the consecutive "1"s in the mask).

- Next hop address and NULL interface

When configuring a static route, you can specify the *gateway-address* to decide the next hop address, depending on the actual conditions.

In fact, for all the routing entries, the next hop address must be specified. When IP layer transmits an IP packet, it will first search the matching route in the routing table according to the destination address of the packet. Only when the next hop address of the route is specified can the link layer find the corresponding link layer address, and then forward the packet according to this address.

The packets sent to NULL interface, a kind of virtual interface, will be discarded at once. This can decrease the system load.

- Preference

Depending on the configuration of preference, you can achieve different route management policies. For example, to implement load sharing, you can specify the same preference for multiple routes to the same destination network. To implement route backup, you can specify different preferences for them.

- Other parameters

The attributes **reject** and **blackhole** respectively indicate the unreachable route and the blackhole route.

Configuring a Default Route

Perform the following configurations in system view.

Table 250 Configure a default route

Operation	Command
Configure a default route	ip route-static 0.0.0.0 { 0.0.0.0 0 } { <i>interface-type</i> <i>interface-number</i> <i>gateway-address</i> } [preference <i>value</i>] [reject blackhole]
Delete a default route	undo ip route-static 0.0.0.0 { 0.0.0.0 0 } [<i>interface-type</i> <i>interface-number</i> <i>gateway-address</i>] [preference <i>value</i>]

The meanings of parameters in the command are the same as those of the static route.

Deleting All the Static Routes

You can use the **undo ip route-static** command to delete one static route. The Switch 8800 Family series also provide the following command for you to delete all static routes at one time, including the default routes.

Perform the following configuration in system view.

Table 251 Delete all static routes

Operation	Command
Delete all static routes	delete static-routes all
Delete all static routes of the VPN	delete vpn-instance <i>vpn-instance-name</i> static-routes all

Displaying and Debugging Static Route

After the above configuration, execute the **display** command in any view to display the running of the static route configuration, and to verify the effect of the configuration.

Table 252 Display and debug the routing table

Operation	Command
Display routing table summary	display ip routing-table
Display routing table details	display ip routing-table verbose
Display the detailed information of a specific route	display ip routing-table <i>ip-address</i> [<i>mask</i>] [longer-match] [verbose]
Display the route information in the specified address range	display ip routing-table <i>ip-address1</i> <i>mask1</i> <i>ip-address2</i> <i>mask2</i> [verbose]
Display the route filtered through the specified basic access control list (ACL)	display ip routing-table acl { <i>acl-number</i> <i>acl-name</i> } [verbose]
Display the route information that is filtered through the specified ip prefix list	display ip routing-table ip-prefix <i>ip-prefix-number</i> [verbose]
Display the routing information discovered by the specified protocol	display ip routing-table protocol <i>protocol</i> [inactive verbose]
Display the tree routing table	display ip routing-table radix

Table 252 Display and debug the routing table

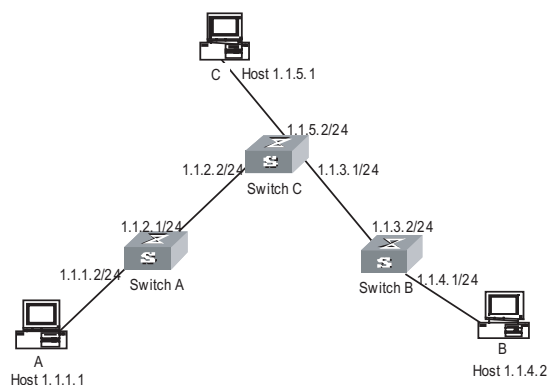
Operation	Command
Display the statistics of the routing table	display ip routing-table statistics
Display the routing information about the VPN instance	display ip routing-table vpn-instance <i>vpn-instance-name</i>

Typical Static Route Configuration Example

Network requirements

As shown in Figure 71, the masks of all the IP addresses are 255.255.255.0. It is required that all the hosts or Switch 8800 Family series routing switches can be interconnected in pairs by static route configuration.

Network diagram

Figure 71 Network diagram for the static route configuration example

Configuration procedure

Configure the static route for Switch A

```
[Switch A] ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[Switch A] ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
[Switch A] ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

Configure the static route for Switch B

```
[Switch B] ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
[Switch B] ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
[Switch B] ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

Configure the static route for Switch C

```
[Switch C] ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
[Switch C] ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

Configure the default gateway of the Host A to be 1.1.1.2

Configure the default gateway of the Host B to be 1.1.4.1

Configure the default gateway of the Host C to be 1.1.5.2

Then, all the hosts or switches in the figure can be interconnected in pairs.

Troubleshooting Static Route Faults**Symptom:**

The switch is configured with the static routing protocol and both the physical status and the link layer protocol status of the interface is Up, but the IP packets cannot be forwarded normally.

Solution:

- Use the **display ip routing-table protocol static** command to view whether the configured static route is correct and in effect.

30

RIP CONFIGURATION

Introduction to RIP

Routing Information Protocol (RIP) is a relatively simple interior gateway protocol (IGP), which is mainly applied to small scale networks.

It is easy to implement RIP. You can configure and maintain RIP more easily than OSPF and IS-IS, so RIP still has a wide application in actual networking.

RIP Operation Mechanism

RIP basic concepts

RIP is a kind of Distance-Vector (D-V) algorithm-based protocol and exchanges routing information via UDP packets.

It employs Hop Count to measure the distance to the destination host, which is called Routing Cost. In RIP, the hop count from a router to its directly connected network is 0, and that to a network which can be reached through another router is 1, and so on. To restrict the time to converge, RIP prescribes that the cost value is an integer ranging from 0 to 15. The hop count equal to or exceeding 16 is defined as infinite, that is, the destination network or the host is unreachable.

To improve the performance and avoid route loop, RIP supports Split Horizon and allows importing the routes discovered by other routing protocols.

RIP route database

Each router running RIP manages a route database, which contains routing entries to all the reachable destinations in the network. These routing entries contain the following information:

- Destination address: IP address of a host or a network.
- Next hop address: The interface address of the next router that an IP packet will pass through for reaching the destination.
- Output interface: The interface through which the IP packet should be forwarded.
- Cost: The cost for the router to reach the destination, which should be an integer in the range of 0 to 16.
- Timer: Duration from the last time that the routing entry is modified till now. The timer is reset to 0 whenever a routing entry is modified.

RIP timer

In RFC1058, RIP is controlled by the following timers: Period update, Timeout and Garbage-Collection.

- Period Update is triggered periodically to send all RIP routes to all neighbors.

- If the RIP route is not updated (a router receives the update packets from the neighbor) when the Timeout timer expires, this route is regarded as unreachable. The cost is set to 16.
- If the Garbage-Collection timer expires, and the unreachable route receives no update packet from the same neighbor, the route will be completely deleted from the routing table.
- By default, the values of Period Update and Timeout timers are 30 seconds and 180 seconds respectively. The value of Garbage-collection timer is four times that of Period Update timer: 120 seconds.

RIP Enabling and Running

The following section describes the procedure:

- If RIP is enabled on a router for the first time, the router will broadcast or multicast the request packet to the adjacent routers. Upon receiving the request packet, the RIP on each adjacent router responds with a packet conveying its local routing table.
- After receiving the response packets, the router, which has sent the request, will modify its own routing table. At the same time, the router sends trigger modification packets to its adjacent routers running RIP and broadcasts modification information, following split horizon mechanism. After receiving trigger modification packets, the adjacent routers send trigger modification packets to their respective adjacent routers. As a result, each router can obtain and maintain the latest routing information.
- RIP broadcasts its routing table to the adjacent routers every 30 seconds. The adjacent routers will maintain their own routing table after receiving the packets and will select an optimal route, and then advertise the modification information to their respective adjacent network so as to make the updated route globally known. Furthermore, RIP uses the timeout mechanism to handle the out-timed routes so as to ensure the real-timeliness and validity of the routes.

RIP has become one of the actual standards of transmitting router and host routes by far. It can be used in most of the campus networks and the regional networks that are simple yet extensive. For larger and more complicated networks, RIP is not recommended.

Configuring RIP

1 RIP basic configuration

RIP basic configuration includes:

- Enabling RIP
- Enabling RIP on specified network

If the link, which does not support broadcast or multicast packets, runs RIP, you need to configure RIP to send any packet to the specified destination, establishing RIP neighbors correctly.

2 RIP route management

You can make the following configurations for RIP to advertise and receive routing information:

- Setting additional routing metric
 - Configuring RIP to import routers of other protocols
 - Configuring RIP route filtering
 - Enabling/disabling host route receiving by the router
 - Configuring RIP-2 route summary
- 3** RIP configuration
- Configuring the RIP precedence
 - Configuring RIP timers
 - Configuring zero field check for RIP-1 packets
 - Specifying RIP version of the interface
- 4** Configuration related to security

You can select the following configurations to improve RIP security during exchanging routing information, or control the area to transmit RIP packets.

- Setting RIP-2 packet authentication
- Specifying the operating state of the interface

Enabling RIP and Entering RIP View

Perform the following configurations in system view.

Table 253 Enable RIP and enter RIP view

Operation	Command
Enable RIP and enter the RIP view	rip
Disable RIP	undo rip

By default, RIP is not enabled.

Enabling RIP on the Specified Network Segment

To flexibly control RIP operation, you can enable RIP on the specified network segment so that the corresponding ports can receive and send RIP packets.

Perform the following configurations in RIP view.

Table 254 Enable RIP Interface

Operation	Command
Enable RIP on the specified network	network <i>network-address</i>
Disable RIP on the specified network	undo network <i>network-address</i>

Note that after the RIP task is enabled, you should also specify its operating network segment, for RIP only operates on the interface on the specified network segment. For an interface that is not on the specified network segment, RIP does not receive or send routes on it, nor forwards its interface route, as if this interface does not exist at all. *network-address* is the address of the enabled or disabled network, and it can also be configured as the IP network address of respective interfaces.

When a command **network** is used for an address, you can enable the network address of the port, which also includes the subnet addresses. For example, for **network** 129.102.1.1, you can see **network** 129.102.0.0 either using **display current-configuration** or using **display rip** command.

By default, RIP is disabled on all the interfaces after it is started up.

Configuring Unicast of the Packets

Usually, RIP sends packets using broadcast or multicast addresses. It exchanges routing information with non-broadcasting networks in unicast mode.

Perform the following configuration in RIP view.

Table 255 Configure unicast of the packets

Operation	Command
Configure unicast of the packets	peer <i>ip-address</i>
Cancel unicast of the packets	undo peer <i>ip-address</i>

By default, RIP does not send any packets to any unicast addresses.

It should be noted that a peer should also be restricted by **rip work**, **rip output**, **rip input** and **network** when transmitting packets.

Configuring Split Horizon

Split horizon means that the route received via an interface will not be sent via this interface again. To some extent, the split horizon is necessary for reducing routing loop.

Perform the following configuration in interface view.

Table 256 Configure Split Horizon

Operation	Command
Enable split horizon	rip split-horizon
Disable split horizon	undo rip split-horizon

By default, split horizon of the interface is enabled.

Setting Additional Routing Metric

Additional routing metric is the input or output routing metric added to an RIP route. It does not change the metric value of the route in the routing table, but adds a specified metric value when the interface receives or sends a route.

Perform the following configuration in interface view.

Table 257 Set additional routing metric

Operation	Command
Set the additional routing metric of the route when the interface receives an RIP packet	rip metricin <i>value</i>
Disable the additional routing metric of the route when the interface receives an RIP packet	undo rip metricin
Set the additional routing metric of the route when the interface sends an RIP packet	rip metricout <i>value</i>

Table 257 Set additional routing metric

Operation	Command
Disable the additional routing metric of the route when the interface sends an RIP packet	undo rip metricout

By default, the additional routing metric added to the route when RIP sends a packet is 1. The additional routing metric when RIP receives the packet is 0 by default.



The metricout configuration takes effect only on the RIP routes learnt by the router and RIP routes generated by the router itself. That is, it has no effect on the routes imported to RIP by other routing protocols.

Configuring RIP to Import Routes of Other Protocols

RIP allows users to import the route information of other protocols into the RIP routing table.

RIP can import the routes of Direct, Static, OSPF, IS-IS and BGP, etc.

Perform the following configuration in RIP view.

Table 258 Configure RIP to import routes of other protocols

Operation	Command
Configure RIP to import routes of other protocols	import-route <i>protocol</i> [cost <i>value</i> route-policy <i>route-policy-name</i>]*
Cancel the imported routing information of other protocols	undo import-route <i>protocol</i>
Set the default routing metric	default cost <i>value</i>
Restore the default routing metric	undo default cost

By default, RIP does not import the route information of other protocols.

If you do not specify the routing metric when importing a route, the default routing metric 1 is used.

Configuring Route Filtering

The router provides the route filtering function. You can configure the filter policy rules through specifying the ACL and IP-prefix for route import and advertisement. Besides, to import a route, the RIP packet of a specific router can also be received by designating a neighbor router.

Perform the following configuration in RIP view.

Configuring RIP to filter the received routes

Table 259 Configure RIP to filter the received routes

Operation	Command
Configure RIP to filter the received routing information advertised by the specified address	filter-policy gateway <i>ip-prefix-name</i> import
Cancel filtering the received routing information advertised by the specified address	undo filter-policy gateway <i>ip-prefix-name</i> import

Table 259 Configure RIP to filter the received routes

Operation	Command
Configure RIP to filter the received global routing information	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } import
Cancel filtering the received global routing information	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } import

Configuring RIP to filter the routes advertised by RIP

Table 260 Configure RIP to filter the advertised routes

Operation	Command
Configure RIP to filter the advertised routing information	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>routing-protocol</i>]
Cancel filtering the advertised routing information	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>routing-protocol</i>]

By default, RIP does not filter the received and advertised routing information.



- The **filter-policy import** command filters the RIP routes received from its neighbors, and the routes that fail to pass the filter will not be added to the routing table, and will not be advertised to the neighbors.
- The **filter-policy export** command filters all the advertised routes, including routes imported by the **import-route** command, and RIP routes learned from the neighbors.
- If the **filter-policy export** command does not specify which route to be filtered, then all the routes imported by the **import-route** command and the advertised RIP routes will be filtered.

Disabling RIP to Receive Host Route

In some special cases, the router can receive a lot of host routes, and these routes are of little help in route addressing but consume a lot of network resources. Routers can be configured to reject host routes by using the **undo host-route** command.

Perform the following configuration in RIP view.

Table 261 Enable/disable host route receiving

Operation	Command
Enable the route to receive host route	host-route
Disable the router from receiving host route	undo host-route

By default, the router receives the host route.

Configuring RIP-2 Route summary Function

The so-called route summary means that different subnet routes in the same natural network can be aggregated into one natural mask route for transmission when they are sent to the outside (i.e. other network). Route summary can be performed to reduce the routing traffic on the network as well as to reduce the size of the routing table.

RIP-1 only sends the route with natural mask, that is, it always sends routes in the route summary form. RIP-2 supports subnet mask and classless interdomain routing. To advertise all the subnet routes, the route summary function of RIP-2 can be disabled.

Perform the following configuration in RIP view.

Table 262 Enable/disable RIP-2 route summary function

Operation	Command
Enable the route summary function of RIP-2	summary
Disable the route summary function of RIP-2	undo summary

By default, RIP-2 route summary is enabled.

Setting the RIP Preference

Each kind of routing protocol has its own preference, by which the routing policy will select the optimal one from the routes of different protocols. The greater the preference value is, the lower the preference becomes. The preference of RIP can be set manually.

Perform the following configuration in RIP view.

Table 263 Set the RIP Preference

Operation	Command
Set the RIP Preference	preference <i>value</i>
Restore the default value of RIP preference	undo preference

By default, the preference of RIP is 100.

Specifying RIP Version of the Interface

RIP has two versions, RIP-1 and RIP-2. You can specify the version of the RIP packets processed by the interface.

RIP-1 broadcasts the packets. RIP-2 can transmit packets by both broadcast and multicast. By default, multicast is adopted for transmitting packets. In RIP-2, the multicast address is 224.0.0.9. The advantage of transmitting packets in the multicast mode is that the hosts not operating RIP in the same network can avoid receiving RIP broadcast packets. In addition, this mode can also make the hosts running RIP-1 avoid incorrectly receiving and processing the routes with subnet mask in RIP-2. When an interface is running in RIP-2 broadcast mode, the RIP-1 packets can also be received.

Perform the following configuration in interface view:

Table 264 Specify RIP version of the interface

Operation	Command
Specify the RIP version as RIP-1 for the interface	rip version 1
Specify the RIP version as RIP-2 for the interface	rip version 2 [broadcast multicast]
Restore the default RIP version running on the interface	undo rip version

By default, the interface receives and sends the RIP-1 packets. It will transmit packets in multicast mode when the interface RIP version is set to RIP-2.

Configuring RIP Timers

As mentioned previously, RIP has three timers: Period update, Timeout and Garbage-collection. Modification of these timers affects RIP convergence speed.

Perform the following configuration in RIP view.

Table 265 Configure RIP timers

Operation	Command
Configure RIP timers	timers { update <i>update-timer-length</i> timeout <i>timeout-timer-length</i> } *
Restore the default settings of RIP timers	undo timers { update timeout } *

The modification of RIP timers is validated immediately.

By default, the values of Period Update and Timeout timers are 30 seconds and 180 seconds respectively. The value of Garbage-collection timer is four times that of Period Update timer: 120 seconds.

In fact, you may find that the timeout time of Garbage-collection timer is not fixed. If Period Update timer is set to 30 seconds, Garbage-collection timer might range from 90 to 120 seconds.

Before RIP completely deletes an unreachable route from the routing table, it advertises the route by sending four Period Update packets with route metric of 16, so as to acknowledge all the neighbors that the route is unreachable. As routes cannot always become unreachable at the point when a new period starts, the actual value of Garbage-collection timer is three to four times that of Period Update timer.



You must consider network performance when adjusting RIP timers, and configure all the routers that are running RIP, so as to avoid unnecessary traffic or network jitter.

Configuring RIP-1 Zero Field Check of the Interface Packet

According to the RFC 1058, some fields in the RIP-1 packet must be 0, and they are called zero fields. Therefore, when an interface version is set as RIP-1, the zero field check should be performed on the packet. But if the value in the zero field is not zero, processing will be refused. As there is no zero field in the RIP-2 packet, this configuration is invalid for RIP-2.

Perform the following configuration in RIP view.

Table 266 Configure zero field check of the interface packet

Operation	Command
Configure zero field check on the RIP-1 packet	checkzero
Disable zero field check on the RIP-1 packet	undo checkzero

By default, RIP-1 performs zero field check on the packet.

Specifying the Operating State of the Interface

In interface view, you can specify the operating state of RIP on the interface. For example, whether RIP operates on the interface, namely, whether RIP update packets are sent and received on the interface. In addition, whether an interface sends or receives RIP update packets can be specified separately.

Perform the following configuration in interface view.

Table 267 Specify the operating state of the interface

Operation	Command
Enable the interface to run RIP	rip work
Disable the interface to run RIP	undo rip work
Enable the interface to receive RIP update packet	rip input
Disable the interface to receive RIP update packet	undo rip input
Enable the interface to send RIP update packet	rip output
Disable the interface to send RIP update packet	undo rip output

The **undo rip work** command and the **undo network** command have similar but not all the same functions. Neither of the two commands configures an interface to receive or send RIP route. The difference also exists. RIP still advertises the routes of the interface applying the **undo rip work** command. However, other interfaces will not forward the routes of the interface applying the **undo network** command. It seems that the interface is removed.

In addition, **rip work** is functionally equivalent to both **rip input** and **rip output** commands.

By default, all interfaces except loopback interfaces both receive and transmit RIP update packets.

Setting RIP-2 Packet Authentication

RIP-1 does not support packet authentication. But when the interface operates RIP-2, the packet authentication can be configured.

RIP-2 supports two authentication modes: Simple authentication and MD5 authentication. MD5 authentication uses two packet formats: One follows RFC1723 and the other follows the RFC2082.

The simple authentication does not ensure security. The authentication key not encrypted is sent together with the packet, so the simple authentication cannot be applied to the case with high security requirements.

Perform the following configuration in Interface view:

Table 268 Set RIP-2 packet authentication

Operation	Command
Configure RIP-2 simple authentication key	rip authentication-mode simple <i>password-string</i>
Perform usual MD5 authentication on RIP-2 packets	rip authentication-mode md5 usual <i>key-string</i>
Perform nonstandard-compatible MD5 authentication on RIP-2 packets	rip authentication-mode md5 nonstandard <i>key-string key-id</i>

Table 268 Set RIP-2 packet authentication

Operation	Command
Disable RIP-2 packet authentication	undo rip authentication-mode

Before configuring MD5 authentication, you must configure MD5 type. The **usual** packet format follows RFC1723 and the **nonstandard** follows RFC2082.

Displaying and Debugging RIP

After the above configuration, execute the **display** command in any view to display the running of the RIP configuration, and to verify the effect of the configuration. Execute the **debugging** command in user view to debug the RIP module. Execute the **reset** command in RIP view to reset the system configuration parameters of RIP.

Table 269 Display and debug RIP

Operation	Command
Display the current RIP running state and configuration information.	display rip
Enable the RIP packet debugging information	debugging rip packet
Disable the RIP packet debugging information	undo debugging rip packet
Enable the debugging of RIP receiving packets	debugging rip receive
Disable the debugging of RIP receiving packets	undo debugging rip receive
Enable the debugging of RIP sending packet	debugging rip send
Disable the debugging of RIP sending packet	undo debugging rip send
Reset the system configuration parameters of RIP	reset

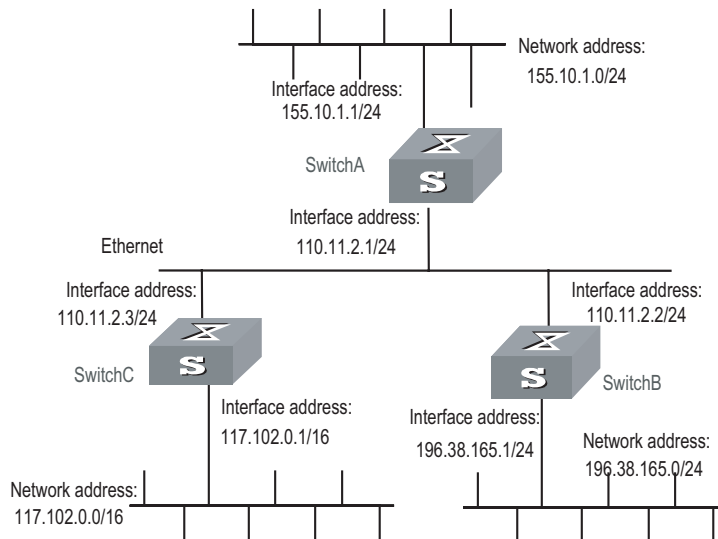
Typical RIP Configuration Example

Network requirements

As shown in Figure 72, the Switch 8800 Family series routing switch C connects to the subnet 117.102.0.0 through the Ethernet port. The Ethernet ports of the Switch 8800 Family series routing switches A and Switch B are respectively connected to the network 155.10.1.0 and 196.38.165.0. Switch C, Switch A and Switch B are connected via Ethernet 110.11.2.0. Correctly configure RIP to ensure that Switch C, Switch A and Switch B can interconnect with each other.

Network diagram

Figure 72 Network diagram for RIP configuration



Configuration procedure



The following configuration only shows the operations related to RIP. Before performing the following configuration, make sure the Ethernet link layer can work normally.

1 Configure Switch A

Configure RIP

```
[Switch A] rip
[Switch A-rip] network 110.11.2.0
[Switch A-rip] network 155.10.1.0
```

2 Configure Switch B

Configure RIP

```
[Switch B] rip
[Switch B-rip] network 196.38.165.0
[Switch B-rip] network 110.11.2.0
```

3 Configure Switch C

Configure RIP

```
[Switch C] rip
[Switch C-rip] network 117.102.0.0
[Switch C-rip] network 110.11.2.0
```

Solution: RIP does not operate on the corresponding interface (for example, the **undo rip work** command is executed) or this interface is not enabled through the **network** command. The peer routing device is configured to be in the multicast mode (for example, the **rip version 2 multicast** command is executed) but the multicast mode has not been configured on the corresponding interface of the local switch.

OSPF Overview

Introduction to OSPF

Open Shortest Path First (OSPF) is an Interior Gateway Protocol based on the link state developed by IETF. At present, OSPF version 2 (RFC2328) is used, which is available with the following features:

- **Applicable scope:** It can support networks in various sizes and can support several hundreds of routers at maximum.
- **Fast convergence:** It can transmit the update packets instantly after the network topology changes so that the change is synchronized in the AS.
- **Loop-free:** Since the OSPF calculates routes with the shortest path tree algorithm according to the collected link states, it is guaranteed that no loop routes will be generated from the algorithm itself.
- **Area partition:** It allows the network of AS to be divided into different areas for the convenience of management so that the routing information transmitted between the areas is abstracted further, hence to reduce the network bandwidth consumption.
- **Equal-cost multi-route:** Support multiple equal-cost routes to a destination.
- **Routing hierarchy:** OSPF has a four-level routing hierarchy. It prioritizes the routes to be intra-area, inter-area, external type-1, and external type-2 routes.
- **Authentication:** It supports the interface-based packet authentication so as to guarantee the security of the route calculation.
- **Multicast transmission:** Support multicast address to receive and send packets.

Process of OSPF Route Calculation

The routing calculation process of the OSPF protocol is as follows:

- Each OSPF-capable router maintains a Link State Database (LSDB), which describes the topology of the whole AS. According to the network topology around itself, each router generates a Link State Advertisement (LSA). The routers on the network transmit the LSAs among them by transmitting the protocol packets to each others. Thus, each router receives the LSAs of other routers and all these LSAs compose its LSDB.
- LSA describes the network topology around a router, so the LSDB describes the network topology of the whole network. Routers can easily transform the LSDB to a weighted directed graph, which actually reflects the topology architecture of the whole network. Obviously, all the routers get a graph exactly the same.
- A router uses the SPF algorithm to calculate the shortest path tree with itself as the root, which shows the routes to the nodes in the autonomous system. The external routing information is the leave node. A router, which advertises the routes, also tags them and records the additional information of the

autonomous system. Obviously, the routing tables obtained by different routers are different.

Furthermore, to enable individual routers to broadcast their local state information to the entire AS, any two routers in the environment should establish adjacency between them. In this case, however, the changes that any router takes will result in multiple transmissions, which are not only unnecessary but also waste the precious bandwidth resources. To solve this problem, "Designated Router" (DR) is defined in the OSPF. Thus, all the routers only send information to the DR for broadcasting the network link states in the network. Thereby, the number of router adjacent relations on the multi-access network is reduced.

OSPF supports interface-based packet authentication to guarantee the security of route calculation. Also, it transmits and receives packets by IP multicast (224.0.0.5 and 224.0.0.6).

OSPF Packets OSPF uses five types of packets:

- Hello Packet:

It is the commonest packet, which is periodically sent by a router to its neighbor. It contains the values of some timers, DR, BDR and the known neighbor.

- Database Description (DD) Packet:

When two routers synchronize their databases, they use the DD packets to describe their own LSDBs, including the digest of each LSA. The digest refers to the HEAD of LSA, which uniquely identifies the LSA. This reduces the traffic size transmitted between the routers, since the HEAD of a LSA only occupies a small portion of the overall LSA traffic. With the HEAD, the peer router can judge whether it already has had the LSA.

- Link State Request (LSR) Packet:

After exchanging the DD packets, the two routers know which LSAs of the peer routers are lacked in the local LSDBs. In this case, they will send LSR packets requesting for the needed LSAs to the peers. The packets contain the digests of the needed LSAs.

- Link State Update (LSU) Packet:

The packet is used to transmit the needed LSAs to the peer router. It contains a collection of multiple LSAs (complete contents).

- Link State Acknowledgment (LSAck) Packet

The packet is used for acknowledging the received LSU packets. It contains the HEAD(s) of LSA(s) requiring acknowledgement.

LSA Type Five basic LSA types

As mentioned previously, OSPF calculates and maintains routing information from LSAs. RFC2328 defines five LSA types as follows:

- Router-LSAs: Type-1. Each router generates Router-LSAs, which describe the link state and cost of the local router. Router-LSAs are broadcast within the area where the router is located.
- Network-LSAs: Type-2. DRs on the broadcast network generate Network-LSAs, which describe the link state of the local network. Network-LSAs are broadcast within the area where a DR is located.
- Summary-LSAs: Include Type-3 and Type-4. Area border routers (ABRs) generate Summary-LSAs. Summary-LSAs are broadcast within the area related to the LSA. Each Summary-LSA describes a route (inter-area route) to a certain destination in other areas of this AS. Type-3 Summary-LSAs describe the routes to networks (the destination is network). Type-4 Summary-LSAs describe the routes to autonomous system border routers (ASBRs).
- AS-external-LSAs: or ASE LSA, the Type-5. ASBRs generate AS-external-LSAs, which describe the routes to other ASs. AS-external-LSA packets are transmitted to the whole AS (except Stub areas). AS-external-LSAs can also describe the default route of an AS.

Type-7 LSA

RFC 1587 (OSPF NSSA Option) adds a new LSA type: Type-7 LSAs.

According to RFC 1587, Type-7 LSAs differ from Type-5 LSAs as follows:

- Type-7 LSAs are generated and released within a Not-So-Stubby Area (NSSA). Type-5 LSAs cannot be generated or released within a NSSA.
- Type-7 LSAs can only be released within an NSSA. When Type-7 LSAs reach an ABR, the ABR can convert part routing information of Type-7 LSAs into Type-5 LSAs and releases the information. Type-7 LSAs cannot be directly released to other areas or backbone areas.

Basic Concepts Related to OSPF

Router ID

To run OSPF, a router must have a router ID. If no ID is configured, the system will automatically pick an IP address from the IP addresses of the current interfaces as the Router ID. The following introduces how to choose a router ID. If loopback interface addresses exist, the system chooses the Loopback address with the greatest IP address value as the router ID. If no Loopback interface configured, then the address of the physical interface with the greatest IP address value will be the router ID.

DR and BDR

- Designated Router (DR)

In multi-access networks, if any two routers establish adjacencies, the same LSA will be transmitted repeatedly, wasting bandwidth resources. To solve this problem, the OSPF protocol regulates that a DR must be elected in a multi-access network and only the DR (and the BDR) can establish adjacencies with other routers in this network. Two non-DR routers or non-BDR routers cannot establish adjacencies and exchange routing information.

You cannot specify the DR in the segment. Instead, DR is elected by all the routers in the segment.

- Backup Designated Router (BDR)

If the DR fails for some faults, a new DR must be elected and synchronized with other routers on the segment. This process will take a relatively long time, during which, the route calculation is incorrect. To shorten the process, BDR is brought forth in OSPF. In fact, BDR is a backup for DR. DR and BDR are elected in the meantime. The adjacencies are also established between the BDR and all the routers on the segment, and routing information is also exchanged between them. After the existing DR fails, the BDR will become a DR immediately.

Area

The network size grows increasingly larger. If all the routers on a huge network are running OSPF, the large number of routers will result in an enormous LSDB, which will consume an enormous storage space, complicate the SPF algorithm, and add the CPU load as well. Furthermore, as a network grows larger, the topology becomes more likely to take changes. Hence, the network will always be in "turbulence", and a great deal of OSPF packets will be generated and transmitted in the network. This will lower the network bandwidth utility. In addition, each change will cause all the routes on the network to recompute the route.

OSPF solves the above problem by partition an AS into different areas. Areas are logical groups of routers. The borders of areas are formed by routers. Thus, some routers may belong to different areas. A router connects the backbone area and a non-backbone area is called Area Border Router (ABR). An ABR can connect to the backbone area physically or logically.

Backbone area and virtual link

- Backbone Area

After the area partition of OSPF, not all the areas are equal. In which, an area is different from all the other areas. Its area-id is 0 and it is usually called the backbone area.

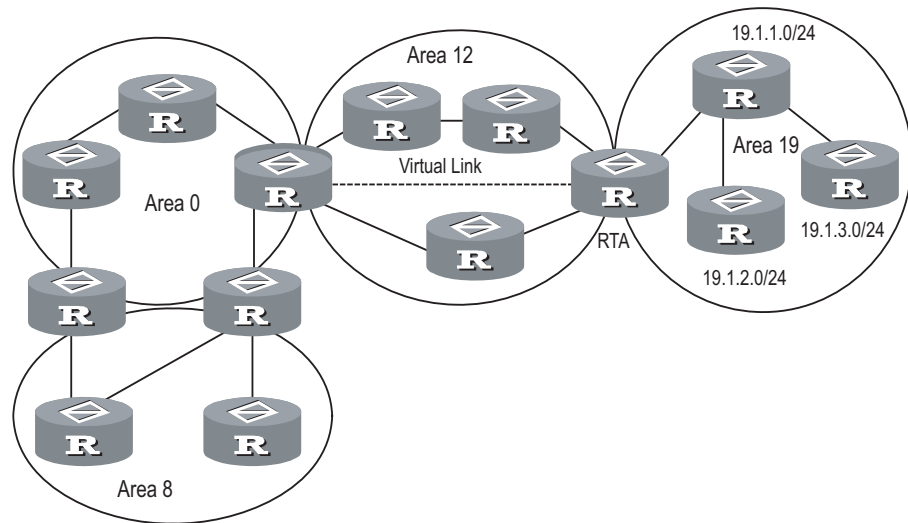
- Virtual link

Since all the areas should be connected to the backbone area, virtual link is adopted so that the physically separated areas can still maintain the logic connectivity to the backbone area.

Route summary

An AS is divided into different areas that are interconnected via OSPF ABRs. The routing information between areas can be reduced through route summary. Thus, the size of routing table can be reduced and the calculation speed of the router can be improved. After calculating an intra-area route of an area, the ABR summarizes multiple OSPF routes into an LSA and sends it outside the area according to the configuration of summary.

For example, as shown in Figure 73, the Area 19 has three area intra-area routes: 19.1.1.0/24, 19.1.2.0/24 and 19.1.3.0/24. The three routes are summarized into one route 19.1.0.0/16 after you configured route summary. The RTA only generates an LSA, describing the summarized route.

Figure 73 Area and route summary

OSPF Features Supported by Switch 8800 Family Series

The Switch 8800 Family series support the following OSPF features:

- Support stub areas: OSPF defines stub areas to decrease the overhead when the routers within the area receive ASE routes.
- Support NSSA: OSPF defines NSSA areas, surmounting the restriction of stub areas on topology. NSSA is the abbreviation of Not-So-Stubby Area.
- Support OSPF Multi-Process: A router runs multiple OSPF processes.
- Share the discovered routing information with other dynamic routing protocols: OSPF currently can import static routes and routes of other dynamic routing protocols such as RIP into the autonomous system of the router, or advertise the routing information discovered by OSPF to other routing protocols.
- Authenticator: OSPF provides clear text authenticator and MD5 encryption authenticator to authenticate packets transmitted between neighboring routers in the same area.
- Flexible configuration for the router port parameter: On the router port, you can configure the following OSPF parameters: output cost, Hello packet interval, retransmission interval, port transmission delay, route precedence, invalid time for adjacent routers, packet authentication mode, packet authenticator, and others.
- Virtual connection: Creates and configures virtual connections.
- Abundant debugging information: OSPF provides abundant debugging information, consequently helping users to diagnose failure

OSPF GR Overview

Open Shortest Path First (OSPF) is an internal gateway protocol. It is developed by IETF based on link state algorithm. OSPF version 2 (RFC2328) is now commonly used.

Graceful Restart (GR) is designed to keep the OSPF routing data normal when abnormal switchover occurs on the switch, so that critical services will not be interrupted.

Working Mechanism of OSPF GR

1. Implementation standard of OSPF GR

RFC3623:Graceful OSPF Restart

IETF drafts:

draft-nguyen-ospf-lls-05;

draft-nguyen-ospf-oob-resync-05;

draft-nguyen-ospf-restart-05;

Work mechanism of RFC3623

RFC3623 defines two main principles for GR: the network topology must remain stable and the forwarding tables can be kept when a router is being restarted.

During the GR process, the behaviors of restarters and helpers are defined. A GR process is started with the restarter's sending a Grace LSA advertisement.

The restarter device does not generate LSAs during the GR process. When it receives a self-generated LSA, it will accept and mark this LSA. Route items are not delivered to the forwarding table. The restarter device finds out its state before restart through hello packets on the snooping interface. When all the neighbor relationships are rebuilt or the GR period timeouts, the Restarter devices will exit GR.

The Restarter device will perform standard OSPF reflooding and routing operation after exiting GR, no matter whether it has finished GR.

The Helper device judges its relationship with the Restarter device when it receives Grace LSA from the Restarter device. When its neighbor state machine is full, and it is not in the GR state, it will enter Helper mode and keep the received Grace LSAs. The Helper routes help the Restarter routes to regain the LSDB information before restart.

When Grace LSAs in the Helper device are updated or when the Helper device exits the Helper mode when a GR period is finished, the Helper device will calculate DR routers of this network, generate class 1 LSAs and calculate routes.

3. Work mechanism of IETF drafts

Two primary concepts are defined in the drafts: Link-local Signaling (LLS) which is used to negotiate about OOB capabilities and trigger GR processes and Out-of-band LSDB resynchronization (OOB) which is used to synchronize LSDB.

The L_bit set in a HELLO packet can negotiate about LLS capabilities and notify the peer about its own LLS data. The LR_bit set in the EO_TLV of the LLS data is used to negotiate about the OOB capabilities.

When a protocol is restarted, the protocol will notify the peer that it will be restarted and let the peer keep the neighbor relationship through the RS_bit set in the EO_TLV of a HELLO packet. The R_bit set in a DD packet indicates that this is an OOB process.

The neighbor will keep the neighbor relationship and set the Restartstat-flag after receiving HELLO packets of the RS_bit set.

When both neighbors exit from the OOB process, the standard OSPF algorithm is performed.



The GR method on both OSPF neighbors must be the same. Different GR methods cannot perform the GR process successfully. A OSPF process can use only one GR method.

Packet Format of OSPF GR

Format of Grace LSA

This LSA is an Opaque-LSA generated by the Restarter. For this LSA, the LS-type is 9, Opaque type is 3 and Opaque ID is 0.

Figure 74 Format of Grace LSA

LS age		Options	9
3	0		
Advertising Router			
LS sequence number			
LS checksum		Length	
TLVs			
.....			

Format of TLV

Figure 75 Format of TLV

Type	Length
Vlaue	

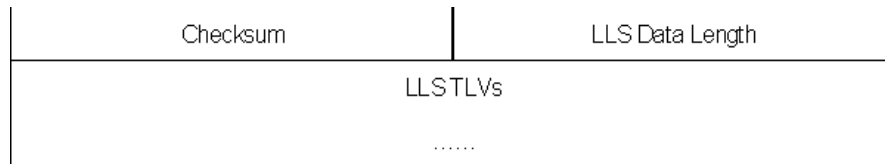
2. Option fields extended by LLS

Figure 76 Option fields with L-bit

*	*	DC	L	N/P	MC	E	*
---	---	----	---	-----	----	---	---

3. Format of LLS data

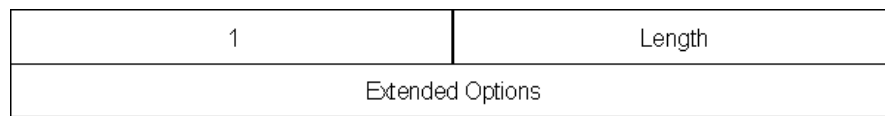
Figure 77 Format of LLS data



TLV structure: EO_TLV and CA_TLV

1 Format of EO_TLV

Figure 78 Format of EO_TLV



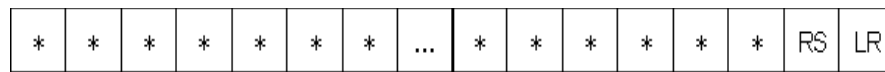
The meaning of each field in EO_TLV:

The type field refers to the type of TLV, and the type of EO_TLV is 1;

The Length field refers to the length of TLV, and the length of EO_TLV is 4;

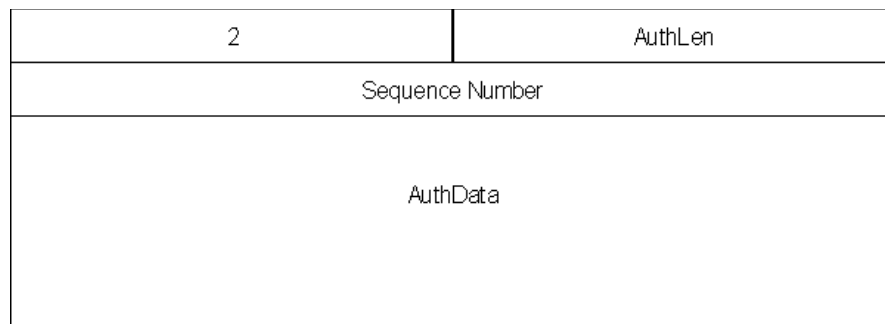
The Extend Options field is the extend options of OSPF. RS_bit and LR_bit are set in this Option field in OSPF GR. The following figure describes the detailed format:

Figure 79 Format of Extend Option



Format of CA_TLV

Figure 80 Format of CA_TLV



The meaning of each field in the CA_TLV:

The type field refers to the type of CA_TLV, and the type of CA_TLV is 2;

The AuthLen field refers to the length of CA_TLV, and the length of CA_TLV is 20;

The Sequence number and AuthData fields are determined by the OSPF check information.



LLS data can be included in only HELLO packets and DD packets. Only one LLS data can be included in a packet. EO_TLV must be included in LLS data. Additionally, CA_TLV must be included in LLS data if OSPF is configured with MD5 check.

Format of DD Packets of Extended OOB

The R_bit set in a DD packet indicates that this is an OOB process.

Figure 81 Format of DD Packets of the R-bit set

Version #	2	Packet Length										
Router ID												
Area ID												
Checksum					AuType							
Authentication												
Authentication												
Interface MTU					Options							
					0	0	0	0	R	I	M	MS
DD Sequence number												
An LSA Header												

OSPF GR Features Supported by Comware

The two GR methods above are supported in the implementation of Comware.

Configuring OSPF

OSPF configuration needs cooperation among routers: intra-area, area boundary, and AS boundary. If none of OSPF parameters is configured, their default settings apply. In this case, sent and received packets are not authenticated, and an individual interface does not belong to the area of any AS. When reconfiguring a default parameter on one router, make sure that the same change is made on all other involved routers.

In various configurations, you must first enable OSPF, specify the interface and area ID before configuring other functions. But the configuration of the functions related to the interface is not restricted by whether the OSPF is enabled or not. It should be noted that after OSPF is disabled, the OSPF-related interface parameters also become invalid.

OSPF configuration includes:

- 1 OSPF basic configuration
 - “Configuring Router ID”
 - “Enabling OSPF”
 - “Entering OSPF Area View”
 - “Specifying an Interface to Run OSPF”
- 2 Configuration related to OSPF route
 - “Configuring OSPF to Import Routes of Other Protocols”
 - “Configuring OSPF to Import Default Routes”
 - “Configuring OSPF Route Filtering”
 - “Configuring the Route Summary of OSPF”
- 3 Some OSPF configurations
 - “Setting OSPF Route Preference”
 - “Setting the Interface Priority for DR Election”
 - “Configuring OSPF Timers”
 - “Configuring an Interval Required for Sending LSU Packets”
 - “Configuring the Cost for Sending Packets on an Interface”
 - “Configuring the Network Type of the OSPF Interface”
 - “Configuring to Fill the MTU Field When an Interface Transmits DD Packets”
 - “Setting a Shortest Path First (SPF) Calculation Interval for OSPF”
- 4 Configurations related to OSPF networking
 - “Configuring OSPF Authentication”
 - “Disabling the Interface to Send OSPF Packets”
 - “Configuring OSPF Virtual Link”
 - “Configuring Stub Area of OSPF”
 - “Configuring NSSA Area of OSPF”
 - “Setting the Switch for Adjacency State Output”
- 5 Configuration related to specific applications
 - “Configuring OSPF and Network Management System”
 - “Configuring OSPF GR”
- 6 Others
 - “Resetting the OSPF Process”

Configuring Router ID Router ID is a 32-bit unsigned integer in IP address format that uniquely identifies a router within an AS. Router ID can be configured manually. If router ID is not configured, the system will select the IP address of an interface automatically. When you do that manually, you must guarantee that the IDs of any two routers in the AS are unique. A common undertaking is to set the router ID to be the IP address of an interface on the router.

Perform the following configuration in system view.

Table 270 Configure router ID

Operation	Command
Configure router ID	router id <i>router-id</i>
Remove the router ID	undo router id

To ensure stability of OSPF, the user should determine the division of router IDs and manually configure them when planning the network.

Enabling OSPF Perform the following configuration in system view.

Table 271 Enable/Disable OSPF

Operation	Command
Enable OSPF and enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i> vpn-instance <i>vpn-instance-name</i>]]
Disable one or all OSPF processes	undo ospf [<i>process-id</i>]

By default, OSPF is disabled.

When enabling OSPF, pay attention to the following points:

- The default OSPF process ID is 1. If no process ID is specified in the command, the default one is adopted.
- If a router is running multiple OSPF processes, you are recommended to use **router-id** in the command to specify different router IDs for different processes.

Entering OSPF Area View

OSPF divides an AS into different areas or logical groups of routers.

Perform the following configuration in OSPF view.

Table 272 Enter OSPF area view

Operation	Command
Enter OSPF area view	area <i>area-id</i>
Delete an OSPF area	undo area <i>area-id</i>

The *area-id* parameter identifies an area. It can be a decimal integer in the range of 0 to 4,294,967,295, or in the format of IP address. Regardless of how it is specified, it is displayed in the format of IP address.

Note that when you configure OSPF routers in the same area, you should apply most configuration data to the whole area. Otherwise, the neighboring routers cannot exchange information. This may even block routing information or create routing loops.

Specifying an Interface to Run OSPF

After using the **ospf** command to enable OSPF in system view, you must specify the network to run OSPF. An ABR router can be in different areas, while a network segment can only belong to an area. That is, you must specify a specific area for each port running OSPF.

Perform the following configuration in OSPF area view.

Table 273 Specifying an interface to run OSPF

Operation	Command
Specify an interface to run OSPF	network <i>ip-address ip-mask</i>
Disable OSPF on the interface	undo network <i>ip-address ip-mask</i>

The *ip-mask* argument is IP address wildcard shielded text (similar to the complement of the IP address mask).

Configuring OSPF to Import Routes of Other Protocols

The dynamic routing protocols on the router can share the routing information. As far as OSPF is concerned, the routes discovered by other routing protocols are always processed as the external routes of AS. In the **import-route** commands, you can specify the route cost type, cost value and tag to overwrite the default route receipt parameters (refer to “Configuring parameters for OSPF to import external routes”).

The OSPF uses the following four types of routes (ordered by priority):

- Intra-area route
- Inter-area route
- External route type 1
- External route type 2

Intra-area and inter-area routes describe the internal AS topology whereas the external routes describe how to select the route to the destinations beyond the AS.

The external routes type-1 refers to the imported IGP routes (such as static route and RIP). Since these routes are more reliable, the calculated cost of the external routes is the same as the cost of routes within the AS. Also, such route cost and the route cost of the OSPF itself are comparable. That is, cost to reach the external route type 1 = cost to reach the corresponding ASBR from the local router + cost to reach the destination address of the route from the ASBR.

The external routes type-2 refers to the imported EGP routes. Since these routes have lower credibility, OSPF assumes that the cost spent from the ASBR to reach the destinations beyond the AS is greatly higher than that spent from within the AS to the ASBR. So in route cost calculation, the former is mainly considered, that is, the cost spent to reach the external route type 2 = cost spent to the destination address of the route from the ASBR. If the two values are equal, then the cost of the router to the corresponding ASBR will be considered.

Configuring OSPF to import external routes

Perform the following configuration in OSPF view.

Table 274 Configure OSPF to import external routes

Operation	Command
Configure OSPF to import routes of other protocols	import-route <i>protocol</i> [cost <i>value</i> type <i>value</i> tag <i>value</i> route-policy <i>route-policy-name</i>]*
Cancel importing routing information of other protocols	undo import-route <i>protocol</i>

By default, OSPF will not import the routing information of other protocols. For an imported route, type is 2, cost is 1, and tag is 1 by default.

The routes that can be imported include Direct, Static, rip, is-is, and bgp. In addition, the routes of other OSPF processes can also be imported.



- It is recommended to configure the imported route type, cost and tag for the **import-route** command simultaneously. Otherwise, the later configuration will overwrite the former configuration.
- After you configured the **import-route** command on the OSPF router to import external routing information, this OSPF router becomes an ASBR.

Configuring the maximum number of imported exterior routes

Perform the following configuration in OSPF view.

Table 275 Configure the maximum number of imported exterior routes

Operation	Command
Configure the maximum number of imported exterior routes	import-route-limit <i>num</i>
Restore the default value of the maximum number of imported exterior routes	undo import-route-limit

By default, the maximum number of imported exterior routes is 20K.

Configuring parameters for OSPF to import external routes

When the OSPF imports the routing information discovered by other routing protocols in the autonomous system, some additional parameters need configuring, such as default route cost and default tag of route distribution. Route tag can be used to identify the protocol-related information. For example, OSPF can use it to identify the AS number when receiving BGP.

Perform the following configuration in OSPF view.

Table 276 Configure parameters for OSPF to import external routes

Operation	Command
Configure the default cost for the OSPF to import external routes	default cost <i>value</i>
Restore the default cost for the OSPF to import external routes	undo default cost
Configure the default tag for the OSPF to import external routes	default tag <i>tag</i>

Table 276 Configure parameters for OSPF to import external routes

Operation	Command
Restore the default tag for the OSPF to import external routes	undo default tag
Configure the default type of external routes that OSPF will import	default type { 1 2 }
Restore the default type of the external routes imported by OSPF	undo default type

By default, the type of imported route is type-2, the cost is 1 and the tag is 1 for a imported route.

Configuring the default interval and number for OSPF to import external routes

OSPF can import the external routing information and broadcast it to the entire autonomous system. Importing routes too often and importing too many external routes at one time will greatly affect the performance of the device. Therefore it is necessary to specify the default interval and number for the protocol to import external routes.

Perform the following configuration in OSPF view.

Table 277 Configure the default interval and number for OSPF to import external routes

Operation	Command
Configure the default interval for OSPF to import external routes	default interval <i>seconds</i>
Restore the default interval for OSPF to import external routes	undo default interval
Configure the upper limit to the routes that OSPF imports at a time	default limit <i>routes</i>
Restore the default upper limit to the external routes that can be imported at a time	undo default limit

By default, the interval for importing external routes is 1 second. The upper limit to the external routes imported is 1000 at a time.

Configuring OSPF to Import Default Routes

By default, there are no default routes in a common OSPF area (either a backbone area or a non-backbone area). Besides, the **import-route** command cannot be used to import the default route.

Use the **default-route-advertise** command to generate and advertise a default route in an OSPF route area. Note the following when you use this command:

- If you use the **default-route-advertise** command on an ASBR or ABR of a common OSPF area, the system generates a Type-5 LSA, advertising the default route in the OSPF route area.
- If you use the **default-route-advertise** command on an ASBR or ABR of an NSSA, the system generates a Type-7 LSA, advertising the default route in the NSSA.
- This command is invalid for a stub area or a totally stub area.

- For an ASBR, the system generates the corresponding Type-5 LSA or Type-7 LSA by default when a default route existed in the routing table.
- For an ABR, the system will generate a Type-5 LSA or Type-7 LSA no matter whether there is a default route in the routing table.
- The broadcasting scope of Type-5 LSA or Type-7 LSA advertising the default route is the same as that of the common Type-5 LSA or Type-7 LSA.

Perform the following configuration in OSPF view.

Table 278 Configure OSPF to import the default route

Operation	Command
Import the default route to OSPF	default-route-advertise [always cost <i>value</i> type <i>type-value</i> route-policy <i>route-policy-name</i>]*
Remove the imported default route	undo default-route-advertise [always cost type route-policy]*

By default, OSPF does not import the default route.

If you use the **always** keyword of this command, the system will generate a Type-5 or Type-7 LSA no matter whether there is default route in the routing table. Be cautious that the **always** keyword is only valid for an ASBR.

Because OSPF does not calculate the LSAs it generated during SPF calculation, there is no default route in the OSPF route on this router. To ensure the correct routing information, you should configure to import the default route on the router only connected to the external network.



- After the **default-route-advertise** command is configured on the OSPF router, this router becomes an ASBR. For the OSPF router, the **default-route-advertise** and **import-route** commands have the similar effect.
- For the ABR or ASBR in the NSSA area, the **default-route-advertise** and **nssa default-route-advertise** commands have the same effect.

Configuring OSPF Route Filtering

Perform the following configuration in OSPF view.

Configuring OSPF to filter the received routes

Table 279 Enable OSPF to filter the received routes

Operation	Command
Disable filtering the received global routing information	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> gateway <i>ip-prefix-name</i> } import
Cancel filtering the received global routing information	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> gateway <i>ip-prefix-name</i> } import

By default, OSPF will not filter the received routing information.

Configuring filtering the routes imported to OSPF

Use the **filter-policy export** command to configure the ASBR router to filter the external routes imported to OSPF. This command is only valid for the ASBR router.

Table 280 Enable OSPF to filter the imported routes of other routing protocols

Operation	Command
Enable OSPF to filter the routes advertised by other routing protocols	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>routing-protocol</i>]
Disable OSPF to filter the advertised routes by other routing protocols	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>routing-protocol</i>]

By default, OSPF does not receive the routes advertised by other routing protocols.



- The **filter-policy import** command only filters the OSPF routes of this process received from the neighbors, and routes that cannot pass the filter will not be added to the routing table. This command only takes effect on ABR.
- The **filter-policy export** command only takes effect on the routes imported by the **import-route** command. If you configure the switch with only the **filter-policy export** command, but without configuring the **import-route** command to import other external routes (including OSPF routes of different process), then the **filter-policy export** command does not take effect.
- If the **filter-policy export** command does not specify which type of route is to be filtered, it takes effect on all routes imported by the local device using the **import-route** command.

Configuring filtering of received Type-3 LSAs

Use the following command to configure route filtering between OSPF areas.

Table 281 Configure filtering of received Type-3 LSAs

Operation	Command
Enable an OSPF area to filter received Type-3 LSAs	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } import
Disable an OSPF area from filtering received Type-3 LSAs	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } import

By default, the OSPF area does not filter received Type-3 LSAs.

Configuring filtering of Type-3 LSAs advertised to other areas

Table 282 Configure filtering of Type-3 LSAs advertised to other areas

Operation	Command
Enable an OSPF area to filter Type-3 LSAs advertised to other areas	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export
Disable an OSPF area from filtering Type-3 LSAs advertised to other areas	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export

By default, an OSPF area does not filter Type-3 LSAs advertised to other areas.



*The **filter-policy import/export** command filters only locally originated Type-3 LSAs, and does not filter Type-3 LSAs received from neighbors. This command is valid on ABR only.*

Configuring the Route Summary of OSPF

Configuring the route summary of OSPF area

Route summary means that ABR can aggregate information of the routes of the same prefix and advertise only one route to other areas. An area can be configured with multiple aggregate segments, thereby OSPF can summarize them. When the ABR transmits routing information to other areas, it will generate Sum_net_Lsa (type-3 LSA) per network. If some continuous networks exist in this area, you can use the **abr-summary** command to summarize these segments into one segment. Thus, the ABR only needs to send an aggregated LSA, and all the LSAs in the range of the aggregate segment specified by the command will not be transmitted separately. This can reduce the LSDB size in other areas.

Once the aggregated segment of a certain network is added to the area, all the internal routes of the IP addresses in the range of the aggregated segment will no longer be separately advertised to other areas. Only the route summary of the whole aggregated network will be advertised. But if the range of the segment is restricted by the keyword **not-advertise**, the route summary of this segment will not be advertised. This segment is represented by IP address and mask.

Route summary can take effect only when it is configured on ABRs.

Perform the following configuration in OSPF area view.

Table 283 Configure the route summary of OSPF area

Operation	Command
Configure route summary of OSPF area	abr-summary <i>ip-address mask</i> [advertise not-advertise]
Cancel route summary of OSPF area	undo abr-summary <i>ip-address mask</i>

By default, route summary is disabled on ABRs.

Configuring summarization of imported routes by OSPF

OSPF of the Switch 8800 Family series supports route summary of imported routes.

Perform the following configurations in OSPF view.

Table 284 Configure summarization of imported routes by OSPF

Operation	Command
Configure summarization of imported routes by OSPF	asbr-summary <i>ip-address mask</i> [not-advertise tag value]
Remove summarization of routes imported into OSPF	undo asbr-summary <i>ip-address mask</i>

By default, summarization of imported routes is disabled.

After the summarization of imported routes is configured, if the local router is an autonomous system border router (ASBR), this command summarizes the imported Type-5 LSAs in the summary address range. When NSSA is configured, this command will also summarize the imported Type-7 LSA in the summary address range.

If the local router works as an area border router (ABR) and a router in the NSSA, this command summarizes Type-5 LSAs transformed from Type-7 LSAs. If the router is not the router in the NSSA, the summarization is disabled.

Setting OSPF Route Preference

Since maybe multiple dynamic routing protocols are running on one router concurrently, the problem of route sharing and selection between various routing protocols occurs. The system sets a preference for each routing protocol, which will be used in tie-breaking in case different protocols discover the same route.

Perform the following configuration in OSPF view.

Table 285 Set OSPF route preference

Operation	Command
Configure a preference for OSPF for comparing with the other routing protocols	preference [ase] preference
Restore the default protocol preference	undo preference [ase]

By default, the OSPF preference is 10, and that of the imported external routing protocol is 150.

Configuring OSPF Timers

Setting the interval for Hello packet transmission

Hello packets are a kind of most frequently used packets, which are periodically sent to the adjacent router for discovering and maintaining the adjacency, and for electing DR and BDR. The user can set the Hello timer.

According to RFC2328, the consistency of Hello intervals between network neighbors should be kept. The Hello interval value is in inverse proportion to the route convergence rate and network load.

Perform the following configuration in interface view.

Table 286 Set the Hello interval

Operation	Command
Set the hello interval of the interface	ospf timer hello seconds
Restore the default hello interval of the interface	undo ospf timer hello
Restore the default poll interval	undo ospf timer poll

By default, p2p and broadcast interfaces send Hello packets every 10 seconds, and p2mp interfaces send Hello packets every 30 seconds.

Setting a dead timer for the neighboring routers

The dead timer of neighboring routers refers to the interval in which a router will regard the neighboring router as dead if no Hello packet is received from it. The user can set a dead timer for the neighboring routers.

Perform the following configuration in interface view.

Table 287 Set a dead timer for the neighboring routers

Operation	Command
Configure a dead timer for the neighboring routers	ospf timer dead <i>seconds</i>
Restore the default dead interval of the neighboring routers	undo ospf timer dead

By default, the dead interval for the neighboring routers of p2p or broadcast interfaces is 40 seconds and that for the neighboring routers of p2mp interfaces is 120 seconds.

Note that both hello and dead timer will restore to the default values after the user modify the network type.

Setting an interval for LSA retransmission between neighboring routers

If a router transmits a Link State Advertisements (LSA) to the peer, it requires the acknowledgement packet from the peer. If it does not receive the acknowledgement packet within the retransmit time, it will retransmit this LSA to the neighbor. The value of retransmit is user-configurable.

Perform the following configuration in interface view.

Table 288 Set an interval for LSA retransmission between neighboring routers

Operation	Command
Configure the interval of LSA retransmission for the neighboring routers	ospf timer retransmit <i>interval</i>
Restore the default LSA retransmission interval for the neighboring routers	undo ospf timer retransmit

By default, the interval for neighboring routers to retransmit LSAs is 5 seconds.

The value of *interval* should be bigger than the roundtrip value of a packet.

Note that you should not set the LSA retransmission interval too small. Otherwise, unnecessary retransmission will be caused.

Configuring the Network Type of the OSPF Interface

The route calculation of OSPF is based upon the topology of the adjacent network of the local router. Each router describes the topology of its adjacent network and transmits it to all the other routers.

OSPF divides networks into four types by link layer protocol, but due to ethernet media type, 3Com supports the Broadcast domain only. OSPF uses the network type, **broadcast**.

Perform the following configuration in interface view.

Table 289 Configure a network type for an OSPF interface

Operation	Command
Configure the network type on the interface	ospf network-type { broadcast nbma p2mp p2p }
Restore the default network type of the OSPF interface	undo ospf network-type

Note: 3Com supports the broadcast domain only.

By default, OSPF determines the network type based on the link layer type. After the interface has been configured with a new network type, the original network type of the interface is removed automatically.

Setting the Interface Priority for DR Election

On a broadcast network, a designated router (DR) and a backup designated router (BDR) must be elected.

The priority of a router interface determines the qualification of the interface in DR election. The router with the priority of 0 cannot be elected as the DR or BDR.

DR is not designated manually. Instead, it is elected by all the routers on the segment. Routers with the priorities larger than 0 in the network are eligible "candidates". Votes are hello packets. Each router writes the expected DR in the packet and sends it to all the other routers on the segment. If two routers attached to the same segment concurrently declare themselves to be the DR, choose the one with higher priority. If the priorities are the same, choose the one with greater router ID. If the priority of a router is 0, it will not be elected as DR or BDR.

If DR fails due to some faults, the routers on the network must elect a new DR and synchronize with the new DR. The process will take a relatively long time, during which, the route calculation is incorrect. In order to speed up this process, OSPF puts forward the concept of BDR. In fact, BDR is a backup for DR. DR and BDR are elected in the meantime. The adjacencies are also established between the BDR and all the routers on the segment, and routing information is also exchanged between them. When the DR fails, the BDR will become the DR instantly. Since no re-election is needed and the adjacencies have already been established, the process is very short. But in this case, a new BDR should be elected. Although it will also take a quite long period of time, it will not exert any influence upon the route calculation.

Note the following:

- The DR on the network is not necessarily the router with the highest priority. Likewise, the BDR is not necessarily the router with the second highest priority. If a new router is added after DR and BDR election, it is impossible for the router to become the DR even if it has the highest priority.
- DR is based on the router interface in a certain segment. Maybe a router is a DR on one interface, but can be a BDR or DROther on another interface.
- DR election is only required for the broadcast interfaces.

Perform the following configuration in interface view.

Table 290 Set the interface priority for DR election

Operation	Command
Configure the interface with a priority for DR election	ospf dr-priority <i>priority-num</i>
Restore the default interface priority	undo ospf dr-priority

By default, the priority of the interface is 1 in the DR election.

Use the **ospf dr-priority** and **peer** commands to set priorities with different usages:

- Use the **ospf dr-priority** command to set priority for DR selection.
- The priority you use the **peer** command to set indicates whether the adjacent router is eligible for election. If you specify the priority as 0 during neighbor configuration, the local router considers that this neighbor is not eligible for election, thus sending no Hello packets to this neighbor. This configuration can reduce the Hello packets on the network during DR and BDR selection. However, if the local router is DR or BDR, this router can also send Hello packets to the neighbor with priority 0 to establish adjacency relations.

Configuring an Interval Required for Sending LSU Packets

Trans-delay seconds should be added to the aging time of the LSA in an LSU packet. Setting the parameter like this mainly considers the time duration that the interface requires for transmitting a packet.

The user can configure the interval of sending LSU message. Obviously, more attention should be paid to this item over low speed networks.

Perform the following configuration in interface view.

Table 291 Configure an interval required for sending LSU packets

Operation	Command
Configure an interval for sending LSU packets	ospf trans-delay <i>seconds</i>
Restore the default interval for sending LSU packets	undo ospf trans-delay

By default, the LSU packets are transmitted per second.

Configuring the Cost for Sending Packets on an Interface

The user can control the network traffic by configuring different packet sending costs for different interfaces.

Perform the following configuration in interface view.

Table 292 Configure the cost for sending packets on an interface

Operation	Command
Configure the cost for sending packets on an interface	ospf cost <i>value</i>
Restore the default cost for packet transmission on the interface	undo ospf cost

For Switch 8800 Family series, the default cost for running OSPF on the VLAN interface is 10.

Configuring to Fill the MTU Field When an Interface Transmits DD Packets

OSPF-running routers use Database Description (DD) packets to describe their own LSDBs during LSDB synchronization.

You can manually specify an interface to fill in the MTU field in a DD packet when it transmits the packet. The MTU should be set to the real MTU on the interface.

Perform the following configuration in interface view.

Table 293 Configure whether the MTU field will be filled in when an interface transmits DD packets

Operation	Command
Enable an interface to fill in the MTU field when transmitting DD packets	ospf mtu-enable
Disable the interface to fill the MTU field when transmitting DD packets	undo ospf mtu-enable

By default, the interface does not fill in the MTU field when transmitting DD packets. In other words, MTU in the DD packets is 0.

Setting a Shortest Path First (SPF) Calculation Interval for OSPF

Whenever the LSDB of OSPF takes changes, the shortest path requires recalculation. Calculating the shortest path upon change will consume enormous resources as well as affect the operation efficiency of the router. Adjusting the SPF calculation interval, however, can restrain the resource consumption due to frequent network changes.

Perform the following configuration in OSPF view.

Table 294 Set the SPF calculation interval

Operation	Command
Set the SPF calculation interval	spf-schedule-interval <i>seconds</i>
Restore the SPF calculation interval	undo spf-schedule-interval <i>seconds</i>

By default, the interval of SPF recalculation is five seconds.

Disabling the Interface to Send OSPF Packets

To prevent OSPF routing information from being acquired by the routers on a certain network, use the **silent-interface** command to disable the interface to transmit OSPF packets.

Perform the following configuration in OSPF view.

Table 295 Enable/disable OSPF packet transmission

Operation	Command
Disable the interface to send OSPF packets	silent-interface { default Vlan-interface <i>Vlan-interface-number</i> }
Enable the interface from sending OSPF packets	undo silent-interface { default Vlan-interface <i>Vlan-interface-number</i> }

By default, all interfaces are allowed to transmit and receive OSPF packets.

After an OSPF interface is set to be in silent status, the interface can still advertise its direct route. However, the OSPF hello packets of the interface will be blocked, and no neighboring relationship can be established on the interface. Thereby, the capability for OSPF to adapt to the networking can be enhanced, which will hence reduce the consumption of system resources. On a switch, this command can disable/enable the specified VLAN interface to send OSPF packets.

Configuring OSPF Authentication

Configuring the OSPF Area to Support Packet Authentication

All the routers in one area must use the same authentication mode (no authentication, simple text authentication or MD5 cipher text authentication). If the mode of supporting authentication is configured, all routers on the same segment must use the same authentication key. To configure a simple text authentication key, use the **authentication-mode simple** command. Use the **authentication-mode md5** command to configure the MD5 cipher text authentication key if the area is configured to support MD5 cipher text authentication mode.

Perform the following configuration in OSPF area view.

Table 296 Configure the OSPF area to support packet authentication

Operation	Command
Configure the area to support authentication type	authentication-mode { simple md5 }
Cancel the configured authentication mode	undo authentication-mode

By default, the area does not support packet authentication.

Configuring OSPF packet authentication

OSPF supports simple authentication or MD5 authentication between neighboring routers.

Perform the following configuration in interface view.

Table 297 Configure OSPF packet authentication

Operation	Command
Specify a password for OSPF simple text authentication on the interface	ospf authentication-mode simple password
Cancel simple authentication on the interface	undo ospf authentication-mode simple
Specify the interface to use MD5 authentication	ospf authentication-mode md5 key-id key
Disable the interface to use MD5 authentication	undo ospf authentication-mode md5

By default, the interface is not configured with either simple authentication or MD5 authentication.

Configuring OSPF Virtual Link

According to RFC2328, after the area partition of OSPF, not all the areas are equal. In which, an area is different from all the other areas. Its Area-id is 0.0.0.0 and it is usually called the backbone Area. The OSPF routes between non-backbone areas are updated with the help of the backbone area. OSPF stipulates that all the non-backbone areas should maintain the connectivity with the backbone area. That is, at least one interface on the ABR should fall into the area 0.0.0.0. If an area does not have a direct physical link with the backbone area 0.0.0.0, a virtual link must be created.

If the physical connectivity cannot be ensured due to the network topology restriction, a virtual link can satisfy this requirement. The virtual link refers to a logic channel set up through the area of a non-backbone internal route between

two ABRs. Both ends of the logic channel should be ABRs and the connection can take effect only when both ends are configured. The virtual link is identified by the ID of the remote router. The area, which provides the ends of the virtual link with a non-backbone area internal route, is called the transit area. The ID of the transit area should be specified during configuration.

The virtual link is activated after the route passing through the transit area is calculated, which is equivalent to a **p2p** connection between two ends. Therefore, similar to the physical interfaces, you can also configure various interface parameters on this link, such as hello timer.

The "logic channel" means that the routers running OSPF between two ABRs only take the role of packet forwarding (the destination addresses of the protocol packets are not these routers, so these packets are transparent to them and the routers forward them as common IP packets). The routing information is directly transmitted between the two ABRs. The routing information herein refers to the Type-3 LSAs generated by the ABRs, for which the synchronization mode of the routers in the area will not be changed.

Perform the following configuration in OSPF area view.

Table 298 Configure an OSPF virtual link

Operation	Command
Create and configure a virtual link	vlink-peer <i>router-id</i> [hello <i>seconds</i> retransmit <i>seconds</i> trans-delay <i>seconds</i> dead <i>seconds</i> simple <i>password</i> md5 <i>keyid</i> <i>key</i>]*
Remove the created virtual link	undo vlink-peer <i>router-id</i>

By default, the value of *hello seconds* is 10 seconds, the value of *retransmit seconds* is 5 seconds, the value of *trans-delay seconds* is 1 second, and the value of *dead seconds* is 40 seconds.

Configuring Stub Area of OSPF

Stub areas are some special areas, in which the ABRs do not propagate the learned external routes of the AS.

The stub area is an optional configuration attribute, but not every area conforms to the configuration condition. Generally, stub areas, located at the AS boundaries, are those non-backbone areas with only one ABR. Even if this area has multiple ABRs, no virtual links are established between these ABRs.

To ensure that the routes to the destinations outside the AS are still reachable, the ABR in this area will generate a default route (0.0.0.0) and advertise it to the non-ABR routers in the area.

Pay attention to the following items when configuring a stub area:

- The backbone area cannot be configured to be the stub area and the virtual link cannot pass through the stub area.
- If you want to configure an area to be the stub area, then all the routers in this area should be configured with this attribute.

- No ASBR can exist in a stub area. In other words, the external routes of the AS cannot be propagated in the stub area.

Perform the following configuration in OSPF area view.

Table 299 Configure stub area of OSPF

Operation	Command
Configure an area to be the stub area	stub [no-summary]
Remove the configured stub area	undo stub
Configure the cost of the default route transmitted by OSPF to the stub area	default-cost value
Remove the cost of the default route to the stub area	undo default-cost

By default, the stub area is not configured, and the cost of the default route to the stub area is 1.

Configuring NSSA Area of OSPF

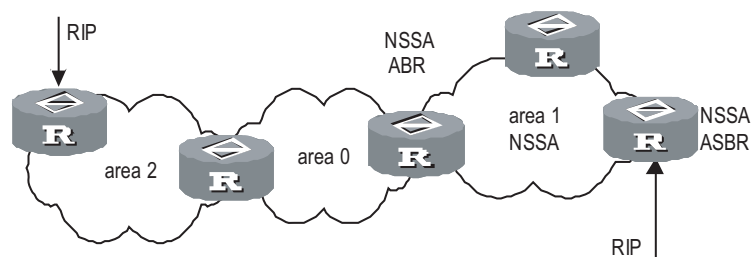
RFC1587 introduced a new type of area called NSSA area, and a new type of LSA called NSSA LSA (or Type-7 LSA).

NSSA areas are virtually variations of Stub areas. They are similar in many ways. Neither of them generates or imports AS-External-LSA (namely Type-5 LSA), and both of them can generate and import Type-7 LSA. Type-7 LSA is generated by ASBR of NSSA area, which can only be advertised in NSSA area. When Type-7 LSA reaches ABR of NSSA, ABR will select whether to transform Type-7 LSA into AS-External-LSA so as to advertise to other areas.

For example, in the network below, the AS running OSPF comprises three areas: Area 1, Area 2 and Area 0. Among them, Area 0 is the backbone area. Also, there are other two ASs respectively running RIP. Area 1 is defined as an NSSA area. After RIP routes of the Area 1 are propagated to the NSSA ASBR, the NSSA ASBR will generate type-7 LSAs which will be propagated in Area 1. When the type-7 LSAs reach the NSSA ABR, the NSSA ABR will transform it into type-5 LSA, which will be propagated to Area 0 and Area 2. On the other hand, RIP routes of the AS running RIP will be transformed into type-5 LSAs that will be propagated in the OSPF AS. However, the type-5 LSAs will not reach Area 1 because Area 1 is an NSSA. NSSAs and stub areas have the same approach in this aspect.

Similar to a stub area, the NSSA cannot be configured with virtual links.

Figure 82 NSSA area



Perform the following configuration in OSPF area view.

Table 300 Configure NSSA of OSPF

Operation	Command
Configure an area to be the NSSA area	nssa [default-route-advertise no-import-route no-summary]*
Cancel the configured NSSA	undo nssa
Configure the default cost value of the route to the NSSA	default-cost <i>cost</i>
Restore the default cost value of the route to the NSSA area	undo default-cost

All the routers connected to the NSSA should use the **nssa** command to configure the area with the NSSA attribute.

The keyword **default-route-advertise** is used to generate default type-7 LSAs. When **default-route-advertise** is configured, a default type-7 LSA route will be generated on the ABR, even though no default route 0.0.0.0 is in the routing table. On an ASBR, however, a default type-7 LSA route can be generated only if the default route 0.0.0.0 is in the routing table.

Executing the keyword **no-import-route** on the ASBR will prevent the external routes that OSPF imported through the **import-route** command from being advertised to the NSSA. Generally, if an NSSA router is both ASBR and ABR, this keyword will be used.

The keyword **default-cost** is used on the ABR attached to the NSSA. Using this command, you can configure the default route cost on the ABR to NSSA.

By default, the NSSA is not configured, and the cost of the default route to the NSSA is 1.

Setting the Switch for Adjacency State Output

When the switch for adjacency state output is enabled, the OSPF adjacency state changes will be output to the configuration terminal until the switch for adjacency state output is disabled.

Perform the following configuration in OSPF view.

Table 301 Set the switch for adjacency state output

Operation	Command	Description
Enter system view	system-view	-
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i> vpn-instance <i>vpn-instance-name</i>]]	Required
Set the switch for adjacency state output	log-peer-change	Required The OSPF adjacency state changes are not reported by default

Configuring OSPF and Network Management System

Configuring OSPF MIB binding

After multiple OSPF processes are enabled, you can configure to which OSPF process MIB is bound.

Perform the following configuration in system view.

Table 302 Configure OSPF MIB binding

Operation	Command
Configure OSPF MIB binding	ospf mib-binding <i>process-id</i>
Restore the default OSPF MIB binding	undo ospf mib-binding

By default, MIB is bound to the first enabled OSPF process.

Configuring OSPF TRAP

The OSPF Trap function enables the switch to send multiple types of SNMP Trap packets in case of OSPF process exceptions. In addition, you can specify an OSPF process ID so that this functions works only on that process. If no process ID is specified, this function works on all OSPF processes.

Perform the following configuration in system view.

Table 303 Enable/Disable OSPF TRAP function

Operation	Command
Enable OSPF TRAP function	snmp-agent trap enable ospf [<i>process-id</i>] [ifstatechange virifstatechange nbrstatechange virnbrstatechange ifcfgerror virifcfgerror ifauthfail virifauthfail ifrxbadpkt virifrxbadpkt iftxretransmit viriftxretransmit originatelsa maxagelsa lsdboverflow lsdbapproachoverflow]
Disable OSPF TRAP function	undo snmp-agent trap enable ospf [<i>process-id</i>] [ifstatechange virifstatechange nbrstatechange virnbrstatechange ifcfgerror virifcfgerror ifauthfail virifauthfail ifrxbadpkt virifrxbadpkt iftxretransmit viriftxretransmit originatelsa maxagelsa lsdboverflow lsdbapproachoverflow]

By default, OSPF TRAP function is disabled. That is, the switch does not send TRAP packets when any OSPF process is abnormal.

For detailed configuration of SNMP TRAP, refer to the module "System Management" in this manual.

Configuring OSPF GR **Configuring GR method as RFC3623**

Table 304 Configure OSPF GR

Operation	Command	Description
Enter system view	system-view	-
Enter OSPF view	ospf [<i>process-id</i>] [router-id <i>router-id</i>] vpn-instance <i>vpn-instance-name</i>]	-
Configure GR	graceful-restart [<i>value</i>]	Required The time is 120 s by default

Configuring GR method as IETF drafts

Table 305 Configure OSPF GR

Operation	Command	Description
Enter system view	system-view	-
Enter OSPF view	ospf [<i>process-id</i> [[router-id <i>router-id</i>] vpn-instance <i>vpn-instance-name</i>]]	-
Configure GR	graceful-restart compatible	Required

Resetting the OSPF Process

If the **undo ospf** command is executed on a router and then the **ospf** command is used to restart the OSPF process, the previous OSPF configuration will lose. With the **reset ospf** command, you can restart the OSPF process without losing the previous OSPF configuration.

Perform the following configuration in user view.

Table 306 Reset OSPF processes

Operation	Command
Reset one or all OSPF processes	reset ospf [statistics] { all <i>process-id</i> }

Resetting the OSPF process can immediately clear invalid LSAs, and make the modified router ID effective or the DR and BDR are re-elected.

Displaying and Debugging OSPF

After the above configuration, execute the **display** command in any view to display the running of the OSPF configuration, and to verify the effect of the configuration. Execute the **debugging** command in user view to debug the OSPF module.

Table 307 Display and debug OSPF

Operation	Command
Display the brief information of the OSPF routing process	display ospf [<i>process-id</i>] brief
Display OSPF statistics	display ospf [<i>process-id</i>] cumulative
Display LSDB information of OSPF	display ospf [<i>process-id</i>] [<i>area-id</i>] lsdb [brief [asbr ase network nssa router summary [verbose]] [<i>ip-address</i>] [originate-router <i>ip-address</i> self-originate [verbose]]
Display OSPF peer information	display ospf [<i>process-id</i>] peer [brief]
Display OSPF next hop information	display ospf [<i>process-id</i>] nexthop
Display OSPF routing table	display ospf [<i>process-id</i>] routing
Display OSPF virtual links	display ospf [<i>process-id</i>] vlink
Display OSPF request list	display ospf [<i>process-id</i>] request-queue
Display OSPF retransmission list	display ospf [<i>process-id</i>] retrans-queue
Display the information of OSPF ABR and ASBR	display ospf [<i>process-id</i>] abr-asbr

Table 307 Display and debug OSPF

Operation	Command
View OSPF inter-area route summarization information	display ospf [process-id] abr-summary
Display the summary information of OSPF imported routes	display ospf [process-id] asbr-summary [ip-address mask]
Display OSPF interface information	display ospf [process-id] interface
Display OSPF errors	display ospf [process-id] error
Display OSPF Graceful Restart information	display ospf [process-id] graceful-restart status
Display the state of the global OSPF debugging switches and the state of the debugging switches for each process	display debugging ospf
Enable OSPF packet debugging	debugging ospf packet [ack dd hello interface interface-type interface-number request update]
Disable OSPF packet debugging	undo debugging ospf packet [ack dd hello interface interface-type interface-number request update]
Enable OSPF event debugging	debugging ospf event
Disable OSPF event debugging	undo debugging ospf event
Enable OSPF LSA packet debugging	debugging ospf lsa-originate
Disable OSPF LSA packet debugging	undo debugging ospf lsa-originate
Enable SPF debugging of OSPF	debugging ospf spf
Disable SPF debugging of OSPF	undo debugging ospf spf

Typical OSPF Configuration Example

Configuring DR Election Based on OSPF Priority

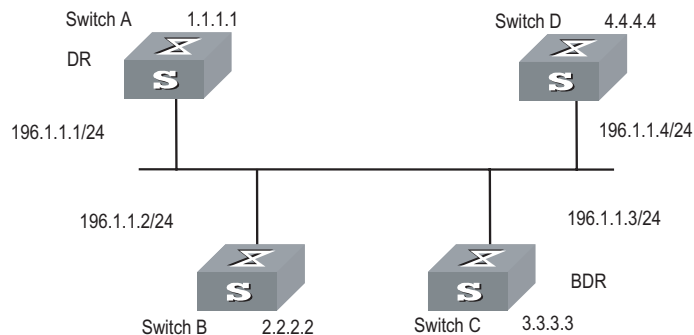
Network requirements

Four Switch 8800 Family series, Switch A, Switch B, Switch C and Switch D, which can perform the router functions and run OSPF, are located on the same segment, as shown in the following figure.

Configure Switch A and Switch C as DR and BDR respectively. The priority of Switch A is 100, which is the highest on the network, so it is elected as the DR. Switch C has the second highest priority, that is, 2, so it is elected as the BDR. The priority of Switch B is 0, which means that it cannot be elected as the DR. Switch D does not have a priority, which takes 1 by default.

Network diagram

Figure 83 Network diagram for configuring DR election based on OSPF priority



Configuration procedure

Configure Switch A

```
[Switch A] interface Vlan-interface 1
[Switch A-Vlan-interface1] ip address 196.1.1.1 255.255.255.0
[Switch A-Vlan-interface1] ospf dr-priority 100
[Switch A] router id 1.1.1.1
[Switch A] ospf
[Switch A-ospf-1] area 0
[Switch A-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

Configure Switch B.

```
[Switch B] interface Vlan-interface 1
[Switch B-Vlan-interface1] ip address 196.1.1.2 255.255.255.0
[Switch B-Vlan-interface1] ospf dr-priority 0
[Switch B] router id 2.2.2.2
[Switch B] ospf
[Switch B-ospf-1] area 0
[Switch B-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

Configure Switch C.

```
[Switch C] interface Vlan-interface 1
[Switch C-Vlan-interface1] ip address 196.1.1.3 255.255.255.0
[Switch C-Vlan-interface1] ospf dr-priority 2
[Switch C] router id 3.3.3.3
[Switch C] ospf
[Switch C-ospf-1] area 0
[Switch C-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

Configure Switch D.

```
[Switch D] interface Vlan-interface 1
[Switch D-Vlan-interface1] ip address 196.1.1.4 255.255.255.0
[Switch D] router id 4.4.4.4
[Switch D] ospf
[Switch D-ospf-1] area 0
[Switch D-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

On Switch A, execute the **display ospf peer** command to display the OSPF peers. Note that Switch A has three peers.

The state of each peer is full, which means that adjacency is set up between Switch A and each peer. (Switch A and Switch C should set up adjacencies with all the routers on the network for them to be DR and BDR on the network respectively.) Switch A is DR, while Switch C is BDR on the network. And all the other neighbors are DR others (which means that they are neither DRs nor BDRs).

Change the priority of Switch B to 200

```
[Switch B-Vlan-interface2000] ospf dr-priority 200
```

On Switch A, execute the **display ospf peer** command to show its OSPF neighbors. Note the priority of Switch B has changed to 200, but it is still not the DR.

Only when the current DR is offline, will the DR be changed. Shut down Switch A, and execute the **display ospf peer** command on Switch D to display its neighbors. Note that the original BDR (Switch C) becomes the DR, and Switch B is BDR now.

If all Switches on the network are removed and added back again, Switch B will be elected as the DR (with the priority of 200), and Switch A becomes the BDR (with a priority of 100). To switch off and restart all of the switches will bring about a new round of DR/BDR selection.

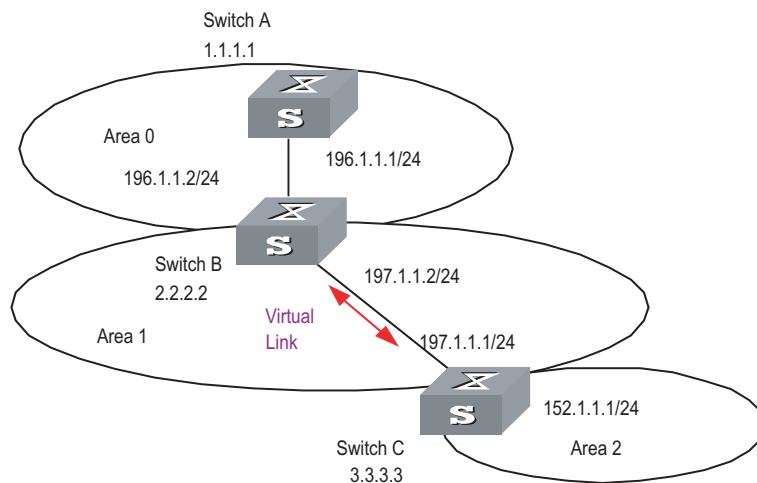
Configuring OSPF Virtual Link

Network requirements

In Figure 84, Area 2 and Area 0 are not directly connected. Area 1 is required to be taken as a transit area for connecting Area 2 and Area 0. Configure a virtual link between Switch B and Switch C in Area 1.

Network diagram

Figure 84 Network diagram for OSPF virtual link configuration



Configuration procedure**# Configure Switch A**

```
[Switch A] interface Vlan-interface 1
[Switch A-Vlan-interface1] ip address 196.1.1.1 255.255.255.0
[Switch A] router id 1.1.1.1
[Switch A] ospf
[Switch A-ospf-1] area 0
[Switch A-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

Configure Switch B

```
[Switch B] interface vlan-interface 7
[Switch B-Vlan-interface7] ip address 196.1.1.2 255.255.255.0
[Switch B] interface vlan-interface 8
[Switch B-Vlan-interface8] ip address 197.1.1.2 255.255.255.0
[Switch B] router id 2.2.2.2
[Switch B] ospf
[Switch B-ospf-1] area 0
[Switch B-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.0] quit
[Switch B-ospf-1] area 1
[Switch B-ospf-1-area-0.0.0.1] network 197.1.1.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3
```

Configure Switch C

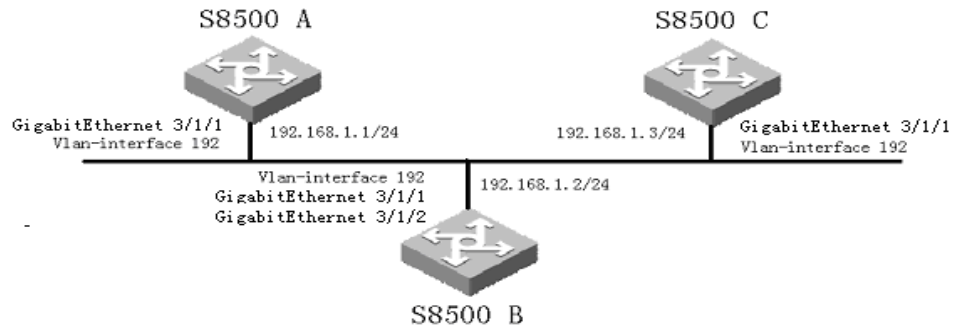
```
[Switch C] interface Vlan-interface 1
[Switch C-Vlan-interface1] ip address 152.1.1.1 255.255.255.0
[Switch C] interface Vlan-interface 2
[Switch C-Vlan-interface2] ip address 197.1.1.1 255.255.255.0
[Switch C] router id 3.3.3.3
[Switch C] ospf
[Switch C-ospf-1] area 1
[Switch C-ospf-1-area-0.0.0.1] network 197.1.1.0 0.0.0.255
[Switch C-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[Switch C-ospf-1-area-0.0.0.1] quit
[Switch C-ospf-1] area 2
[Switch C-ospf-1-area-0.0.0.2] network 152.1.1.0 0.0.0.255
```

OSPF GR Configuration Example**Network requirements**

- For the GR-enabled switch, the GR method must be configured in the view of the corresponding process. Additionally, the Neighbor State Machine (NSM) must be in the FULL state.
- Three switches Switch 8800 FamilyA, Switch 8800 FamilyB and Switch 8800 FamilyC are connected adjacently with each other. Switch 8800 FamilyA serves as the Restarter, and Switch 8800 FamilyB and S8 500C serve as the Helper.

Network diagram

Figure 85 Network diagram



Configuration procedure

Configure the switch Switch 8800 FamilyA

```
<Switch 8800 FamilyA> system-view
[Switch 8800 FamilyA] vlan 192
[Switch 8800 FamilyA-vlan192] port GigabitEthernet 3/1/1
[Switch 8800 FamilyA-vlan192] interface vlan 192
[Switch 8800 FamilyA-Vlan-interface192] ip address 192.168.1.1 24
[Switch 8800 FamilyA-Vlan-interface192] quit
[Switch 8800 FamilyA] ospf 1
[Switch 8800 FamilyA-ospf-1] graceful-restart 180
[Switch 8800 FamilyA-ospf-1] area 0
[Switch 8800 FamilyA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
```

Configure the switch Switch 8800 FamilyB

```
<Switch 8800 FamilyB> system-view
[Switch 8800 FamilyB] vlan 192
[Switch 8800 FamilyB-vlan192] port GigabitEthernet 3/1/1
[Switch 8800 FamilyB-vlan192] interface vlan 192
[Switch 8800 FamilyB-Vlan-interface192] ip address 192.168.1.2 24
[Switch 8800 FamilyB-Vlan-interface192] quit
[Switch 8800 FamilyB] interface GigabitEthernet 3/1/2
[Switch 8800 FamilyB-GigabitEthernet3/1/2] port access vlan 192
[Switch 8800 FamilyB-GigabitEthernet3/1/2] quit
[Switch 8800 FamilyB] ospf 1
[Switch 8800 FamilyB-ospf-1] graceful-restart 180
[Switch 8800 FamilyB-ospf-1] area 0
[Switch 8800 FamilyB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
```

Configure the switch Switch 8800 FamilyC

```
<Switch 8800 FamilyC> system-view
[Switch 8800 FamilyC] vlan 192
[Switch 8800 FamilyC-vlan192] port GigabitEthernet 3/1/1
[Switch 8800 FamilyC-vlan192] interface vlan 192
[Switch 8800 FamilyC-Vlan-interface192] ip address 192.168.1.3 24
[Switch 8800 FamilyC-Vlan-interface192] quit
[Switch 8800 FamilyC] ospf 1
[Switch 8800 FamilyC-ospf-1] graceful-restart 180
[Switch 8800 FamilyC-ospf-1] area 0
[Switch 8800 FamilyC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
```

Troubleshooting OSPF Faults

Symptom 1: OSPF has been configured in accordance with the earlier-mentioned steps, but OSPF on the router cannot run normally.

Solution: Check according to the following procedure.

Local troubleshooting: Check whether the protocol between two directly connected routers is in normal operation. The normal sign is the peer state machine between the two routers reaches the FULL state. (Note: On a broadcast network, if the interfaces for two routers are in DROther state, the peer state machines for the two routers are in 2-way state, instead of FULL state. The peer state machine between DR/BDR and all the other routers is in FULL state.

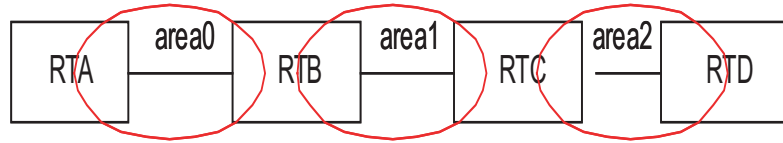
- Execute the **display ospf peer** command to view peers.
- Execute the **display ospf interface** command to view OSPF information on the interface.
- Check whether the physical connections and the lower layer protocol operate normally. You can execute the **ping** command to test. If the local router cannot ping the peer router, it indicates that faults have occurred to the physical link and the lower layer protocol.
- If the physical link and the lower layer protocol are normal, check the OSPF parameters configured on the interface. The parameters should be the same parameters configured on the router adjacent to the interface. The same area ID should be used, and the networks and the masks should also be consistent. (The **p2p** or virtually linked segment can have different segments and masks.)
- Ensure that the dead timer on the same interface is at least four times the value of the Hello timer.
- If the network type is broadcast, there must be at least one interface with a priority greater than zero.
- If an area is set as the stub area, to which the routers are connected. The area on these routers must be also set as the stub area.
- The same interface type should be adopted for the neighboring routers.
- If more than two areas are configured, at least one area should be configured as the backbone area (that is to say, the area ID is 0).
- Ensure that the backbone area is connected to all other areas.
- The virtual links do not pass through the stub area.

Global troubleshooting: If OSPF cannot discover the remote routes yet in the case that the above steps are correctly performed, proceed to check the following configurations.

- If more than two areas are configured on a router, at least one area should be configured as the backbone area.

As shown in Figure 86: RTA and RTD are configured to belong to only one area, whereas RTB (Area0 and Area1) and RTC (Area1 and Area 2) are configured to belong to two areas. In which, RTB also belongs to area0, which is compliant with the requirement. However, none of the areas to which RTC belongs is Area0. Therefore, a virtual link should be set up between RTC and RTB. Ensure that Area2 and Area0 (backbone area) is connected.

Figure 86 OSPF areas



- The backbone area (Area 0) cannot be configured as the stub area and the virtual link cannot pass through the stub area. That is, if a virtual link has been set up between RTB and RTC, neither Area1 nor Area0 can be configured as a stub area. In the figure above, only Area 2 can be configured as the stub area.
- Routers in the stub area cannot receive external routes.
- The backbone area must guarantee the connectivity of all nodes.

Introduction to Integrated IS-IS

Intermediate System-to-Intermediate System (IS-IS) intra-domain routing information exchange protocol is designed by the international organization for standardization (ISO) for connection-less network protocol (CLNP). This protocol is a dynamic routing protocol. To let this protocol support IP routing, IETF expands and modifies IS-IS in RFC1195, applying the protocol to TCP/IP and OSI. The modified IS-IS is called Integrated IS-IS or Dual IS-IS.

IS-IS is a link state protocol, which uses shortest path first (SPF) algorithm. IS-IS and the OSPF protocol are similar in many aspects. As an interior gateway protocol (IGP), IS-IS is applied inside an AS.

Terms of IS-IS Routing Protocol**Terms of IS-IS routing protocol**

- Intermediate System (IS). IS equals a router of TCP/IP. It is the basic unit in IS-IS protocol used for propagating routing information and generating routes. In the following text, the IS shares the same meaning with the router.
- End System (ES). It equals the host system of TCP/IP. ES does not process the IS-IS routing protocol, and therefore it can be ignored in the IS-IS protocol.
- Routing Domain (RD). A group of ISs exchange routing information with the same routing protocol in a routing domain.
- Area. Area is the division unit in the routing domain.
- Link State DataBase (LSDB). All the link states in the network form the LSDB. In an IS, at least one LSDB is available. The IS uses the SPF algorithm and the LSDB to generate its own routes.
- Link State Protocol Data Unit (LSPDU). In the IS-IS, each IS will generate an LSP which contains all the link state information of the IS. Each IS collects all the LSPs in the local area to generate its own LSDB.
- Network Protocol Data Unit (NPDU). It is the network layer packets of OSI and equals the IP packet of TCP/IP.
- Designated IS (DIS). It is the elected router on the broadcast network.
- Network Service Access Point (NSAP) is the network layer address of OSI. It identifies an abstract network service access point and describes the very network address structure for the OSI model.

Link types IS-IS routing protocol is applied to

IS-IS routing protocol can run on point to point Links, such as PPP, HDLC and others. IS-IS routing protocol can also run on broadcast links, such as Ethernet, Token-Ring and others.

Two-level Structure of IS-IS Routing Protocol

Two-level structure of IS-IS routing protocol

Two-level structure of IS-IS routing protocol is adopted in a route area to support large scale route network. A large route area can be divided into one or multiple areas. A Level-1 router manages the intra-area routes. A Level-2 router manages the inter-area routes.

Level-1 and Level-2

- Level-1 router

The Level-1 router is responsible for intra-area route. The Level-1 router and the Level-1 router or Level-1-2 router in the same area are neighbors. The Level-1 router maintains a Level-1 LSDB. This LSDB contains intra-area routing information. The packets sent to other areas are forwarded to the closest Level-2 router.

- Level-2 router

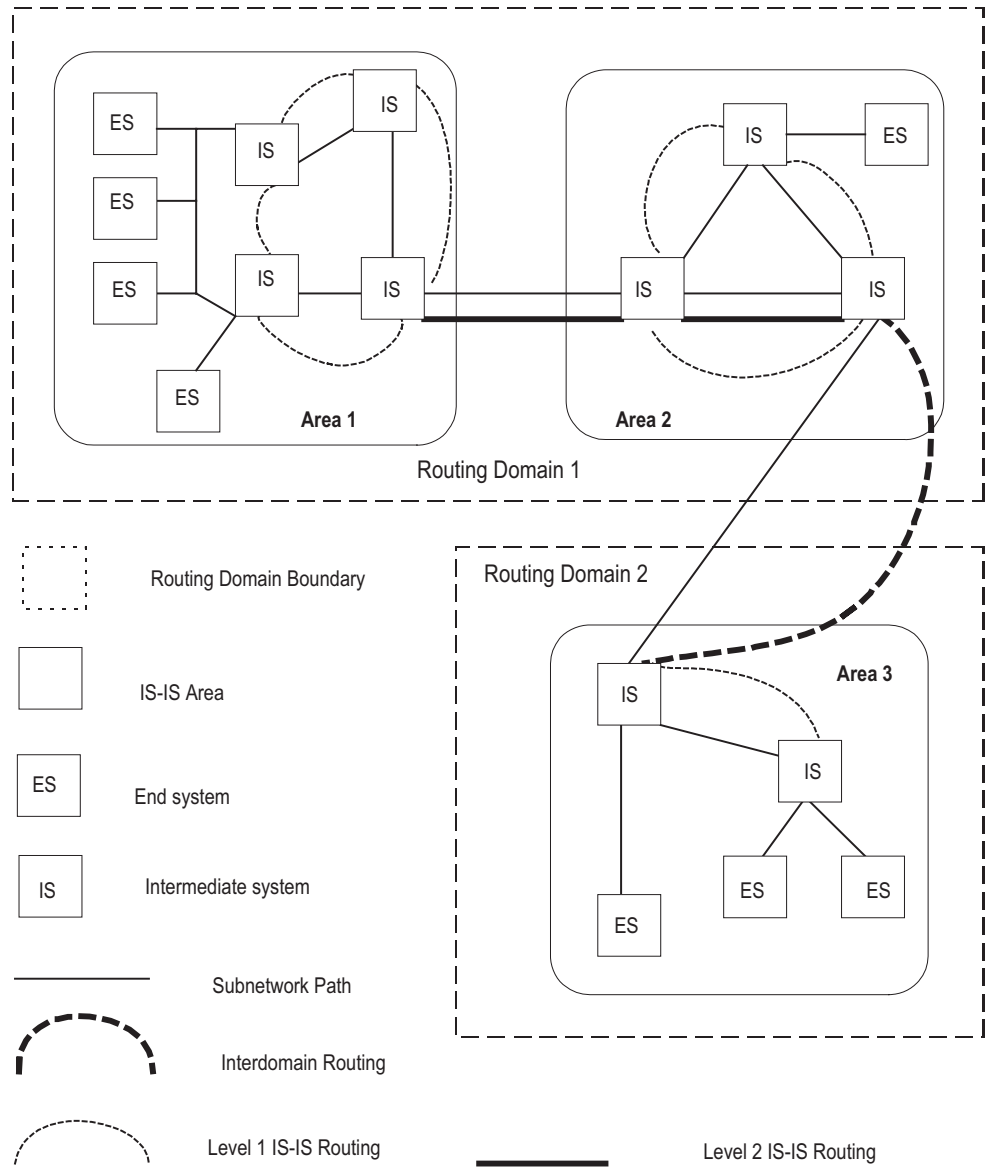
The Level-2 router is responsible for inter-area route. The Level-2 router and Level-2 routers or Level-1-2 routers in other areas are neighbors. The Level-2 router maintains a Level-2 LSDB. This LSDB contains inter-area routing information. The backbone (which is made up of all Level-2 routers) of a route area is responsible for inter-area communications. The Level-2 routers in the route area must be continuous to ensure the backbone continuity.

- Level-1-2 router

A Level-1-2 router is both a Level-1 router and a Level-2 router. At least one Level-1-2 router in each area connects the area to the backbone network. A Level-1-2 router maintains two LSDBs: the Level-1 LSDB for intra- area route and Level-2 LSDB for inter-area route.

Figure 87 illustrates a network running IS-IS routing protocol and composed of Routing Domain 1 and Routing Domain 2. Routing Domain 1 includes two areas, Area 1 and Area 2, and Routing Domain 2 only has Area 3. In Routing Domain 1, the three ISs connected by bold lines compose the area backbone. They are all Level-2 routers. The other 4 ISs not connected by bold line are Level-1-2 routers.

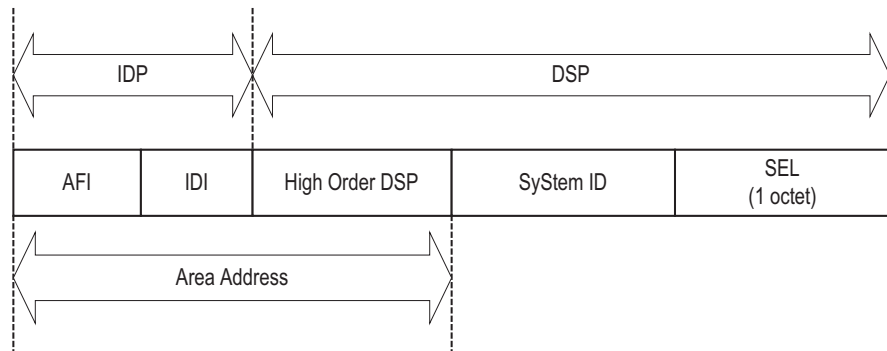
Figure 87 IS-IS topology



NSAP Structure of IS-IS Routing Protocol

Address structure

Figure 88 NSAP structure



OSI adopts the address structure as shown in Figure 88. NSAP includes initial domain part (IDP) and domain specific part (DSP). The IDP is defined by ISO; it consists of authority responsible for assigning the rest of the address and address format. The DSP is allocated by the authority specified in IDP. IDP and DSP are length-variable with a total length of 20 bytes.

- Area Address

IDP includes authority and format identifier (AFI) and initial domain identifier (IDI). AFI defines the format of IDI. DSP has several bytes. The combination of IDP and HO-DSP can identify a route area and an area of the route area, so the combination is called an area address.

In general, you only need to configure an area address for a router. The area addresses of all nodes are the same in an area. To support the seamless combination, segmentation and conversion, Switch 8800 Family series support up to three area addresses.

- System ID

System ID uniquely identifies terminal system or router in a route area. You can select length for it. For Switch 8800 Family series, System ID length is 48 bits (6 bytes). In general, you can obtain System ID according to Router_ID.

If the IP address 168.10.1.1 of the interface LoopBack0 serves as a router_ID for the router, you can use the following method to obtain the System ID:

Turn each part of the IP address 168.10.1.1 into three digits. Add 0 to the front of the part less than three digits.

Divide the expanded address 168.010.001.001 into three parts. Each part contains four digits.

You get the System ID 1680.1000.1001.

You can specify a System ID using different methods. However, you should ensure a System ID can uniquely identify a terminal system or a router.

- SEL

NSAP selector (SEL or N-SEL) functions as the protocol identifier of an IP address. Different transmission protocols correspond to different identifiers. All the SELs of IP are 00.

Because the address structure defines clearly an area, a Level-1 router can easily identify the packets not sent to the area where it is located. The Level-1 router forwards the packets to a Level-2 router.

The Level-1 router performs routing within areas by System IDs. If it detects the destination address of a packet does not belong to the area where it is located, it forwards the packet to its closest Level-1-2 router.

The Level-2 router performs intra-area routing according to the area address (IDP + HO-DSP).

NET

Network Entity Title (NET) indicates the network layer information, which contains no transfer layer information (SEL=0). You can regard it as a special NSAP.

In general, you can configure a NET for a router. If you will redivide an area (combine multiple areas or divide an area into multiple areas), you can configure multiple NETs to ensure correct routes in the case of reconfiguration. Because you can configure up to three area addresses, you can only configure up to three NETs.

For example, there is a NET 47.0001.aaaa.bbbb.cccc.00, in which,

Area=47.0001, System ID=aaaa.bbbb.cccc, SEL=00.

For example, there is a NET 01.1111.2222.4444.00, in which,

Area=01, System ID=1111.2222.4444, and SEL=00.

IS-IS Routing Protocol Packets

IS-IS packets are directly encapsulated in the data link frames and mainly divided into 3 kinds, Hello, LSP and SNP.

Hello packets

Hello packets, which is also called IIH (IS-to-IS Hello PDUs), can establish and maintain neighbor relations. The Level-1 router in a broadcast LAN forwards Level-1 LAN IIH; the Level-2 router in a broadcast LAN forwards Level-2 LAN IIH; non-broadcast network forwards Point-to-Point IIH.

LSP

Link state packet (LSP) can switch link state information. LSP can be divided into Level-1 LSP and Level-2 LSP. Level-2 routers transmit Level-2 LSPs; Level-1 routers transmit Level-1 LSPs; Level-1-2 routers transmit both Level-2 LSPs and Level-1 LSPs.

SNP

Sequence Number Packet (SNP) can confirm the LSPs last received from neighbors. SNPs function as acknowledge packets, but SNPs function more validly. SNP includes complete SNP (CSNP) and partial SNP (PSNP). SNP can be further divided into Level-1 CSNP, Level-2 CSNP, Level-1 PSNP and Level-2 PSNP.

PSNP only lists one or more last received LSP sequence numbers, and confirms multiple LSPs. When detecting asynchronous LSDBs, the system asks neighbors to send new LSPs by PSNPs.

CSNP contains all LSP digest information in a LSDB, synchronizing LSDBs for neighbor routers. On a broadcast network, a DIS sends CSNPs periodically (the default sending period is 10 seconds). On the point-to-point line, a DIS sends CSNPs only when the neighbors are established for the first time.

IS-IS configuration includes:

- 1 IS-IS basic configuration
 - Enabling IS-IS and Entering the IS-IS View
 - Setting Network Entity Title
 - Enabling IS-IS on the Specified Interface
 - Setting Priority for DIS Election
 - Setting Router Type
 - Setting Interface Circuit Level
- 2 Configuration related to IS-IS route
 - Configuring IS-IS to Import Routes of Other Protocols
 - Configuring IS-IS Route Filtering
 - Configuring IS-IS Routing Leak
 - Setting IS-IS Route Summary
 - Setting to Generate Default Route
- 3 Default route generation
 - Setting the Preference of IS-IS Protocol
 - Configuring IS-IS Route Metric Type
 - Setting IS-IS Link State Routing Cost
 - Configuring IS-IS Timers
 - Setting Parameters Related to LSP
 - Setting Parameters Related to SPF
- 4 Configuration related to IS-IS networking
 - Setting IS-IS Authentication
 - Setting Overload Flag Bit
 - Setting to Discard the LSPs with Checksum Errors
 - Setting to Log the Peer Changes
 - Setting the Mesh Group of the Interface
 - Enabling/Disabling IS-IS Packet
 - Configuring IS-IS GR
- 5 Some operation commands
 - Resetting All the IS-IS Data Structure
 - Resetting the Specified IS-IS Peer

Enabling IS-IS and Entering the IS-IS View

After creating an IS-IS routing process, you should also activate this routing process at an interface that may correlate with another router. After that, the IS-IS protocol can be started and run.

Perform the following configuration in system view.

Table 308 Enable IS-IS and enter the IS-IS view

Operation	Command
Enable the IS-IS and enter the IS-IS view	isis [<i>tag</i>]

The *tag* argument identifies the IS-IS process. In the present version, just one IS-IS process is allowed.

By default, the IS-IS routing process is disabled.

Setting Network Entity Title

Network Entity Titles (hereafter referred to as NETs) defines the current IS-IS area address and the system ID of the router.

Perform the following configurations in IS-IS view.

Table 309 Set NETs

Operation	Command
Set a NET	network-entity <i>network-entity-title</i>
Delete a NET	undo network-entity <i>network-entity-title</i>

The format of the *network-entity-title* argument is X...X.XXXXXXXXXXXXXX.XX, among which the first "X...X" is the area address, the twelve Xs in the middle is the System ID of the router. The last XX should be 00.

Enabling IS-IS on the Specified Interface

After enabling IS-IS, you need to specify on which Interfaces the IS-IS will be run.

Perform the following configuration in interface view.

Table 310 Enable IS-IS on the specified interface

Operation	Command
Enable IS-IS on the specified Interface	isis enable [<i>tag</i>]
Cancel this designation	undo isis enable [<i>tag</i>]

Setting Priority for DIS Election

In the broadcast network, the IS-IS needs to elect a DIS from all the routers.

When you need to select a DIS from the IS-IS neighbors on the broadcast network, you should select level-1 DIS and level-2 DIS respectively. The higher the priority is, the more possible it is selected. If there are two or more routers with the highest priority in the broadcast network, the one with the greatest MAC address will be selected. If all the adjacent routers' priorities are 0, the one with the greatest MAC address will be selected.

The DISs of Level-1 and Level-2 are elected separately. You can set different priorities for DIS election at different levels.

Perform the following configuration in interface view.

Table 311 Set priority for DIS election

Operation	Command
Set the priorities for DIS election on the interface	isis dis-priority <i>value</i> [level-1 level-2]
Restore the default priorities for DIS election on the interface	undo isis dis-priority [level-1 level-2]

By default, the interface priority is 64. If the level-1 or level-2 is not specified, it defaults to setting the priority of Level-1.

Setting Router Type

Based upon the position of the router, the levels can be divided into Level-1 (intra-domain router), Level-2 (inter-domain router) and Level-1-2 (that is, intra-domain router as well as inter-domain router).

Perform the following configuration in IS-IS view.

Table 312 Set the router type

Operation	Command
Set the router type	is-level { level-1 level-1-2 level-2 }
Restore the default router type	undo is-level

By default, the router type is **level-1-2**.

Setting Interface Circuit Level

Perform the following configuration in Interface view.

Table 313 Set the interface circuit level

Operation	Command
Set the interface circuit level	isis circuit-level [level-1 level-1-2 level-2]
Restore the default interface circuit level	undo isis circuit-level



Only when the router to which the interface belongs is of Level-1-2 type, is the modification to the interface circuit level meaningful. Otherwise, the type of the router determines the level of adjacency relation.

You can set the circuit level to limit what adjacency can be established for the interface. For example, Level-1 interface can only have Level-1 adjacency. Level-2 interface can only have Level-2 adjacency. For the Level-1-2 router, you can configure some interfaces to Level-2 to prevent transmitting Level-1 Hello packets to Level-2 backbone so as to save the bandwidth. However, Level-1 and Level-2 use the same kind of Hello packet over the **p2p** link, and therefore such setting is unnecessary in this case.

By default, the circuit-level on the interface is **level-1-2**.

Configuring IS-IS to Import Routes of Other Protocols

For IS-IS, the routes discovered by other routing protocols are processed as the routes outside the routing domain. When importing the routes of other protocols, you can specify the default cost for them.

When IS-IS imports routes, you can also specify to import the routes to Level-1, Level-2 or Level-1-2.

Perform the following configuration in IS-IS view.

Table 314 Import routes of other protocols

Operation	Command
Import routes of other protocols	import-route <i>protocol</i> [cost <i>value</i> type { external internal } [level-1 level-1-2 level-2] route-policy <i>route-policy-name</i>]*
Cancel importing routes from other protocols	undo import-route <i>protocol</i> [cost <i>value</i> type { external internal } [level-1 level-1-2 level-2] route-policy <i>route-policy-name</i>]*

If the level is not specified in the command for importing the route, it defaults to importing the routes into **level-2**.

protocol specifies the routing protocol sources that can be imported, which can be direct, static, rip, bgp, and ospf, etc.

By default, IS-IS does not import routing information from any other protocols.

For more about importing routing information, refer to the "Configuring IP Routing Policy" part.

Configuring IS-IS Route Filtering

IS-IS protocol can filter the received and advertised routes according to the access control list specified by *acl-number*.

Perform the following configuration in IS-IS view.

Configuring to filter the routes received by IS-IS

Table 315 Configure to filter the received routes

Operation	Command
Configure to filter the received routes	filter-policy <i>acl-number</i> import
Cancel filtering the received routes	undo filter-policy <i>acl-number</i> import

Configuring to filter the advertised routes

Table 316 Configure to filter the advertised routes

Operation	Command
Configure to filter the routes advertised by IS-IS	filter-policy <i>acl-number</i> export [<i>routing-protocol</i>]
Configure not to filter the routes advertised by IS-IS	undo filter-policy <i>acl-number</i> export [<i>routing-protocol</i>]

By default, IS-IS does not filter the route advertised by other routing protocols.

protocol specifies the routing protocol sources for advertising routes, which can be direct, static, rip, bgp, ospf, ospf-ase, ospf-nssa and so on.



- The **filter-policy import** command only filters the ISIS routes received from the neighbors, and routes that cannot pass the filter will not be added to the routing table. This command takes effect on Level-1-2 routers.

- The **filter-policy export** command only takes effect to the routes imported by the **import-route** command. If you configure the switch with only the **filter-policy export** command, but without configuring the **import-route** command to import other external routes, then the **filter-policy export** command does not take effect.
- If the **filter-policy export** command does not specify which route to be filtered, then the all the routes imported by the **import-route** command will be filtered.

Configuring IS-IS Routing Leak

By virtual of IS-IS routing leak function, a Level-1-2 router can advertise the routing information of a Level-2 area it knows to a Level-1 router.

Perform the following configuration in IS-IS view.

Table 317 Configure IS-IS routing leak

Operation	Command
Enable IS-IS routing leak	import-route isis level-2 into level-1 [acl <i>acl-number</i>]
Disable IS-IS routing leak	undo import-route isis level-2 into level-1 [acl <i>acl-number</i>]

By default, a Level-2 router does not advertise its routing information to a Level-1 area.

Setting IS-IS Route Summary

Users can set the routes with the same next hops as one route in the routing table. Perform the following configurations in IS-IS view.

Table 318 Set a summary route

Operation	Command
Set a summary route	summary <i>ip-address ip-mask</i> [level-1 level-1-2 level-2]
Delete the summary route	undo summary <i>ip-address ip-mask</i> [level-1 level-1-2 level-2]

By default, the system disables route summary.

Setting to Generate Default Route

In the IS-IS route domain, the Level-1 router only has the LSDB of the local area, so it can only generate the routes in the local areas. But the Level-2 router has the backbone LSDB in the IS-IS route domains and generates the backbone network routes only. If a Level-1 router in one area wants to forward the packets to other areas, it needs to first forward the packets to the closest Level-1-2 router in the local area along its default route. You do not need to configure the default Level-1 route, but need to manually configure the default Level-2 route.

Perform the following configurations in IS-IS view.

Table 319 Set to generate default route

Operation	Command
Set to generate default route	default-route-advertise [route-policy <i>route-policy-name</i>]
Set not to generate default route	undo default-route-advertise [route-policy <i>route-policy-name</i>]

The default route generated by this command will only be imported to the router at the same level.

Setting the Preference of IS-IS Protocol

In a router on which several routing protocols are concurrently operating, there is an issue of sharing and selecting the routing information among all the routing protocols. The system sets a preference for each routing protocol. When various routing protocols find the route to the same destination, the protocol with the higher preference will take effect.

Perform the following configuration in IS-IS view.

Table 320 Configure the preference of IS-IS protocol

Operation	Command
Configure the preference of IS-IS protocol	preference <i>value</i>
Restore the default preference of IS-IS protocol	undo preference

By default, the preference of IS-IS route is 15.

Configuring IS-IS Route Metric Type

IS-IS routing protocol has two styles of route metric:

- Narrow: The value of route metric ranges from 1 to 63.
- Wide: The value of route metric ranges from 1 to 16,777,215.

A router can choose either or both of the styles.

Perform the following configuration in IS-IS view.

Table 321 Configure the style for route metric values of IS-IS packets

Operation	Command
Configure the style for route metric values of IS-IS packets	cost-style { narrow wide wide-compatible { compatible narrow-compatible } [relax-spf-limit] }
Restore the default settings	undo cost-style

By default, IS-IS only receives and sends the packets whose route metric is in narrow style.

Setting IS-IS Link State Routing Cost

Users can configure the interface cost, namely, the default routing cost.

Perform the following configuration in interface view.

Table 322 Set IS-IS link state routing cost

Operation	Command
Set the routing cost of the interface	isis cost <i>value</i> [level-1 level-2]
Restore the default routing cost of the interface	undo isis cost [level-1 level-2]

If the level is not specified, the default setting is Level-1 routing cost.

The *value* argument is configured according to the link state of the interface.

By default, the routing cost of IS-IS on an interface is 10.

Configuring IS-IS Timers **Setting the Hello packet broadcast interval**

The IS-IS periodically sends the Hello packets from the interface and the routers maintain the adjacency through the transmitting/receiving of the Hello packets. The Hello packet interval can be modified.

Perform the following configuration in interface view.

Table 323 Set the Hello packet broadcast interval

Operation	Command
Set Hello packet interval, measured in seconds.	isis timer hello <i>seconds</i> [level-1 level-2]
Restore the default Hello packet interval on the interface	undo isis timer hello [level-1 level-2]

Usually, two types of Hello packets are transported over a broadcast link: Level-1 and Level-2 Hello packets. For different packets, different broadcast intervals should be set. However, there are two exceptions. One is when there is no level separation in the link, parameters of Level-1 and Level-2 need not be specified in the command (adopt the default values). So the system will set the broadcast intervals of all packets as that of the level-1 Hello packet. The other is if Hello packets are not separated according to level-1 and level-2 on the **p2p** links, the attribute of the packets need not be set either.

By default, Hello packets are transmitted on an interface every 10 seconds.

This command specifies to send Hello packets of the corresponding levels in the Fast Hello mode (by setting the minimum value of Hello interval to 1 second). If the number of packets is not specified in the related command, three Hello packets will be sent per second.

Perform the following configuration in interface view.

Table 324 Configure to send Hello packets of the corresponding levels in the Fast Hello mode

Operation	Command
Configure to send Hello packets of the corresponding levels in the Fast Hello mode	isis timer hello minimal [level-1 level-2]
Restore the default value of Hello interval in the Fast Hello mode.	undo isis timer hello minimal [level-1 level-2]

If neither **level-1** nor **level-2** is specified, the default setting is Level-1 and Level-2 Hello interval. Namely, the command works on both Level-1 and Level-2.

Setting the CSNP packet broadcast interval

The CSNP packet is transmitted by the DIS over the broadcast network to synchronize the link state database (LSDB). The CSNP packet is regularly broadcast over the broadcast network at an interval, which can be set by users.

Perform the following configuration in interface view.

Table 325 Set the CSNP packet broadcast interval

Operation	Command
Set the CSNP packet broadcast interval	isis timer csnp <i>seconds</i> [level-1 level-2]
Restore the default CSNP packet broadcast interval on the interface	undo isis timer csnp [level-1 level-2]

If the level is not specified, it defaults to setting CSNP packet broadcast interval for Level-1.

By default, the CSNP packet is transmitted via interface every 10 seconds.

Setting LSP packet generation interval

As specified in the IS-IS protocol, when an event takes place, the related LSP packet should be generated again. If LSP packets are generated frequently, a large amount of resources will be occupied and the route's efficiency will be affected. The exponent digression method can improve the efficiency to a certain degree. The LSP packet generation interval can you be configured as per the actual requirement.

Perform the following configuration in IS-IS view.

Table 326 Set LSP packet generation interval

Operation	Command
Set LSP packet generation interval	timer lsp-generation <i>x y z</i> [level-1 level-2]
Restore the default value of LSP packet generation interval	undo timer lsp-generation <i>x y z</i> [level-1 level-2]

Setting the LSP packet transmission interval

LSP carries the link state records for propagation throughout the area.

Perform the following configuration in interface view.

Table 327 Set the LSP packet transmission interval

Operation	Command
Set LSP packet interval on the interface.	isis timer lsp <i>time</i>
Restore the default LSP packet interval on the interface	undo isis timer lsp

By default, the LSP packet is transmitted via the interface every 33 milliseconds.

Setting LSP packet retransmission interval

Over a **p2p** link, if the local end does not receive the response within a period of time after it sends an LSP packet, it considers that the originally transmitted LSP packet has been lost or dropped. In order to guarantee the transmission reliability, the local router will retransmit the original LSP packet.

Perform the following configuration in interface view.

Table 328 Set LSP packet retransmission interval

Operation	Command
Set the retransmission interval of the LSP packet over p2p links	isis timer retransmit <i>seconds</i>
Restore the default retransmission interval of the LSP packet over p2p links	undo isis timer retransmit

By default, the LSP packet is transmitted every five seconds over the **p2p** link.

Configuring number of invalid Hello packets for the interface

The router maintains the adjacency by sending/receiving Hello packets. When receiving no Hello packets from the peer within a time interval, the local router regards the neighbors are invalid. The time interval is called Holddown time for the IS-IS.

Setting invalid number of Hello packets can adjust the Holddown time in the IS-IS. That is to say, after continuously receiving no specified number of Hello packets, the router regards the neighbors are invalid.

Table 329 Set number of invalid Hello packets for the interface

Operation	Command
Set the number of invalid Hello packets	isis timer holding-multiplier <i>value</i> [level-1 level-2]
Restore the default setting	undo isis timer holding-multiplier [level-1 level-2]

By default, the number of the invalid Hello packets is set to 3.

If this command does not specify **level-1** or **level-2**, the system regard the invalid Hello packets are set for both Level-1 and Level-2 routers.

Setting IS-IS Authentication

Setting interface authentication

The authentication password set on the interface is mainly used in the Hello packet so as to confirm the validity and correctness of its peers. The authentication passwords at the same level of all the interfaces of a network should be identical.

Perform the following configuration in interface view.

Table 330 Set interface authentication password

Operation	Command
Set authentication password	isis authentication-mode { simple md5 } <i>password</i> [{ level-1 level-2 } [ip osi]]
Delete authentication-mode password	undo isis authentication-mode { simple md5 } <i>password</i> [{ level-1 level-2 } [ip osi]]

By default, the interface is not configured with any authentication password nor performs authentication. If the level is not specified, it defaults to setting the authentication password of Level-1.

Setting IS-IS area or IS-IS routing domain authentication password

Users can configure the IS-IS area or the IS-IS routing domain with authentication password.

If area authentication is needed, the area authentication password will be encapsulated into the level-1 LSP, CSNP and PSNP packets, in the specified mode. If other routers in the same area also have started the area authentication, their authentication modes and passwords must be identical to those of their neighbors, so that they can work normally. Similarly, for domain authentication, the password will also be encapsulated into the level-2 LSP, CSNP and PSNP packets in the specified mode. If the routers in the backbone layer (level-2) also need domain authentication, their authentication mode and password must be identical to those of their neighbors.

Note that the passwords for authentication of the routers on the same network segment must be identical.

Perform the following configurations in IS-IS view.

Table 331 Set IS-IS authentication password

Operation	Command
Set authentication-mode password	area-authentication-mode { simple md5 } <i>password</i> [ip osi]
Delete authentication-mode password	undo area-authentication-mode { simple md5 } [ip osi]
Set routing domain authentication password	domain-authentication-mode { simple md5 } <i>password</i> [ip osi]
Delete routing domain authentication password	undo domain-authentication-mode { simple md5 } [ip osi]

By default, the system does not require password or perform authentication.

Setting the IS-IS to use the MD5 algorithm compatible with that of the other vendors

You must configure this command when the switch needs to authenticate the devices of other vendors using MD5 algorithm in IS-IS.

Perform the following configuration in IS-IS view.

Table 332 Set the IS-IS to use the MD5 algorithm compatible with that of the other vendors

Operation	Command
Set the IS-IS to use the MD5 algorithm compatible with that of the other vendors	md5-compatible
Set the IS-IS to use the default MD5 algorithm	undo md5-compatible

By default, the system uses the MD5 algorithm in IS-IS which is compatible with that of 3Com.

Setting Overload Flag Bit

Sometimes, the router in the IS-IS domain may encounter some problems in operation thus errors may occur in the whole routing area. In order to avoid this problem, you can set the overload flag bit for this router.

When the overload threshold is set, other routers should not send this router the packets which should be forwarded by it.

Perform the following configurations in IS-IS view.

Table 333 Set overload flag bit

Operation	Command
Set overload flag bit	set-overload
Remove the overload flag bit	undo set-overload

By default, no over load bit is set.

Setting to Discard the LSPs with Checksum Errors

After receiving an LSP packet, the local IS-IS will calculate its checksum and compares the result with the checksum in the LSP packet. This process is the checksum authentication over the received LSP. By default, even when the checksum in the packet is not consistent with the calculated result, the LSP packet is not discarded. However, when not ignoring LSP checksum error is set with the **ignore-lsp-checksum-error** command, the LSP packet will be discarded if the checksum error is found.

Perform the following configuration in IS-IS view.

Table 334 Set to discard the LSPs with checksum errors

Operation	Command
Set to discard the LSP with checksum error	ignore-lsp-checksum-error
Set to ignore the LSP checksum error	undo ignore-lsp-checksum-error

By default, the LSP checksum error is ignored.

Setting to Log the Peer Changes

After peer changes log is enabled, the IS-IS peer changes will be output on the configuration terminal until the log is disabled.

Perform the following configuration in IS-IS view.

Table 335 Set to log the peer changes

Operation	Command
Enable peer changes log	log-peer-change
Disable peer changes log	undo log-peer-change

By default, the peer changes log is disabled.

Setting LSP Refreshment Interval

In order to ensure that the LSPs in the whole area can maintain the synchronization, all the current LSPs will be transmitted periodically.

Perform the following configuration in IS-IS view.

Table 336 Set LSP refreshment interval

Operation	Command
Set LSP refreshment interval	timer lsp-refresh <i>seconds</i>
Restore the default LSP refreshment interval	undo timer lsp-refresh

By default, LSP is refreshed every 900 seconds (15 minutes).

Setting Lifetime of LSP

When a router generates the LSP of the system, it will fill in the maximum lifetime of this LSP. When other routers receive this LSP, its life time will be reduced continuously as the time goes. If updated LSP has not been received before the old one times out, this LSP will be deleted from the LSDB.

Perform the following configuration in IS-IS view.

Table 337 Set Lifetime of LSP

Operation	Command
Set lifetime of LSP	timer lsp-max-age <i>seconds</i>
Restore the default LSP lifetime	undo timer lsp-max-age

By default, LSP can live for 1200 seconds (20 minutes).

Setting Parameters Related to SPF

Setting SPF calculation interval

When IS-IS LSDB changes, the router will compute the shortest path again. However, the immediate calculation upon every change will occupy too many resources and affect the efficiency of the router. In the case that SPF computing interval is set, when LSDB changes, SPF algorithm will be run after the SPF interval times out.

Perform the following configuration in IS-IS view.

Table 338 Set SPF calculation interval

Operation	Command
Set SPF calculation interval	timer spf <i>second</i> [level-1 level-2]
Restore default SPF calculation interval	undo timer spf [level-1 level-2]

If the level is not specified, it defaults to setting the SPF calculation interval of Level-1.

By default, SPF calculation runs every 10 seconds.

Setting SPF calculation in slice

When there is a large number of routes in the routing table (over 150,000), SPF calculation of IS-IS may occupy the system resources for a long time. To prevent such a case, SPF calculation can be set to perform in slice.

Perform the following configuration in IS-IS view.

Table 339 Set SPF calculation in slice

Operation	Command
Set the duration of one cycle in second of SPF calculation	spf-slice-size <i>seconds</i>
Restore the default configuration	undo spf-slice-size

By default, SPF calculation is not divided into slices but runs to the end once, which can also be implemented by setting the *seconds* argument to 0.

After slice calculation is set, the routes that are not processed once will be calculated in one second.

Normally, the user is not recommended to modify the default configuration. When the number of routes is between 150,000 and 200,000, it is recommended to set the *seconds* argument to 1, that is, the duration time for SPF calculation each time is 1 second.

Setting SPF to release CPU actively

To prevent SPF calculation from occupying the system resources for a long time, which affects the response speed of the console, SPF can be set to automatically release the system CPU resources after processing a certain number of routes and the unprocessed routes will be calculated in one second.

Perform the following configuration in IS-IS view.

Table 340 Set SPF to release CPU actively

Operation	Command
Specify the number of routes to process before releasing CPU	spf-delay-interval <i>number</i>
Restore the default configuration	undo spf-delay-interval

By default, CPU is released once when every 2500 routes are processed by the SPF of IS-IS.

Enabling/Disabling IS-IS Packet Transmission

To prevent the IS-IS routing information from being obtained by some router in a certain network, the **silent-interface** command can be used to prohibit sending IS-IS packets via the interface connecting with the router.

Perform the following configuration in IS-IS view.

Table 341 Enable/Disable IS-IS packet transmission

Operation	Command
Disable the interface from sending IS-IS packets	silent-interface <i>interface-type</i> <i>interface-number</i>
Enable the interface to send IS-IS packets	undo silent-interface <i>interface-type</i> <i>interface-number</i>

By default, the interface is allowed to receive and send IS-IS packets.

The **silent-interface** command is only used to restrain the IS-IS packets not to be sent on the interface, but the interface routes can still be sent from other

interfaces. On a switch, this command can disable/enable the specified VLAN interface to send IS-IS packets.

Configuring IS-IS GR

The network is interrupted temporarily when an IS-IS router is restarted because the neighbor relationship of this router with other neighbors is removed and LSP packets are flooded. The GR feature of IS-IS can solve this problem. This feature enables the restarted router to notify its neighbors of its restart state and permits the neighbors to establish new adjacency relation without disconnection. The GR feature of IS-IS has the following benefits:

- This GR feature is applied on the restarted routers and initially started routers, and enables the restarted routers to send connection requests to neighbors again instead of ending the adjacency relation.
- This GR feature reduces the influence on the network caused by waiting for database synchronization before generating LSP packets to the utmost extent.
- This feature sets overload flag bits in LSP packets until database synchronization for the routers started first, so that route loops do not occur in the network.

Table 342 Configure IS-IS GR

Operation	Command	Description
Enter system view	system-view	-
Enable the IS-IS routing process and enter IS-IS view	isis [<i>process id</i>]	Required The IS-IS routing process can not be enabled by default
Enable IS-IS GR capability	graceful-restart	Required IS-IS GR capability is disabled by default
Configure the restart interval	graceful-restart interval <i>timer</i>	Optional The restart interval is 300 seconds by default
Configure SA suppression when a router is restarted	graceful-restart suppress-sa	Required By default, the SA bit is not suppressed



- The restart interval specifies the interval of restarting routers. The restart interval is set as holdtime in Hello PDU of IS-IS. In this way, the neighbors of a router will not break adjacency relations with it when it is restarted.
- The restarted router suppresses SA bits in Hello PDU to request its neighbors to suppress advertising the adjacency relation in the set time range. SA bits are deleted when the database of this router is synchronized. You can use the **graceful-restart suppress-sa** command to disable this function if you do not want to enable this router to set SA bits in Hello PDU. With the help of this feature, the black hole effect caused by sending/receiving LSP packets can be avoided during the GR process.

Resetting All the IS-IS Data Structure

When it is necessary to refresh some LSPs immediately, perform the following configuration in user view.

Table 343 Reset all the IS-IS data structures

Operation	Command
Reset the IS-IS data structure	reset isis all

By default, the IS-IS data structure is not cleared.

Resetting the Specified IS-IS Peer

When it is necessary to connect a specified peer again, perform the following configuration in user view.

Table 344 Reset the specified IS-IS peer

Operation	Command
Reset the specified IS-IS peer	reset isis peer <i>system-id</i>

By default, the IS-IS peer is not cleared.

Displaying and Debugging Integrated IS-IS

After completing the above configuration, execute the **display** command in any view to display the running state of the IS-IS configuration, and to verify the effect of the configuration. Execute the **debugging** command in user view to debug the IS-IS module.

Through the following configuration operations, you can view the LSDB of the IS-IS, the transmitting/receiving of various packets of the IS-IS and the SPF calculation so as to determine the IS-IS route maintenance conditions.

Table 345 Display and debug IS-IS

Operation	Command
Display IS-IS LSDB	display isis lsdb [[I1 I2 level-1 level-2] [[LSPID local] verbose]*]*
Display IS-IS SPF calculation log	display isis spf-log
Display IS-IS routing information	display isis route
Display IS-IS neighbor information	display isis peer [verbose]
Display mesh group information	display isis mesh-group
Enable IS-IS debugging	debugging isis { adjacency all authentication-error checksum-error circuit-information configuration-error datalink-receiving-packet datalink-sending-packet general-error interface-information memory-allocating receiving-packet-content restart-events self-originate-update sending-packet-content snp-packet spf-event spf-summary spf-timer task-error timer update-packet }
Disable IS-IS debugging	undo debugging isis { adjacency all authentication-error checksum-error circuit-information configuration-error datalink-receiving-packet datalink-sending-packet general-error interface-information memory-allocating receiving-packet-content restart-events self-originate-update sending-packet-content snp-packet spf-event spf-summary spf-timer task-error timer update-packet }

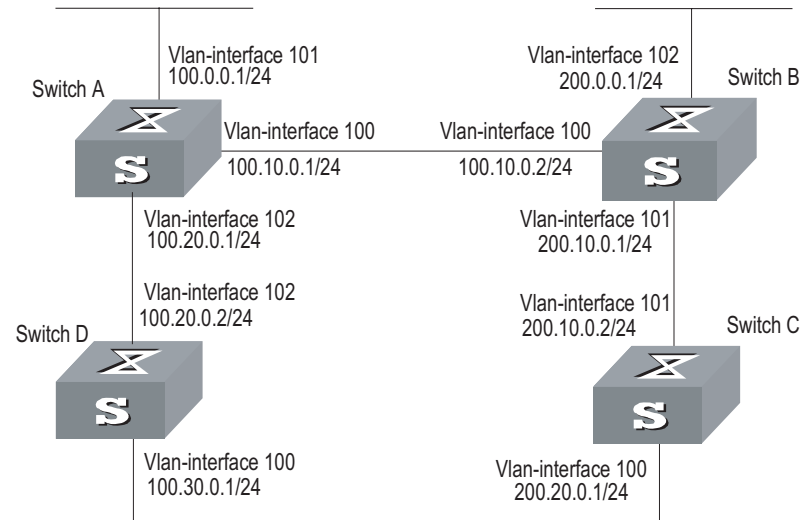
Typical Integrated IS-IS Configuration Example

Network requirements

As is shown in Figure 89, Switches A, B, C and D belong to the same autonomous system. The IS-IS routing protocol is running in these four switches so as to implement route interconnection. In the network design, switches A, B, C and D belong to the same area.

Network diagram

Figure 89 IS-IS configuration example



Configuration procedure

Configure Switch A

```
[Switch A] isis
[Switch A-isis] network-entity 86.0001.0000.0000.0005.00
[Switch A] interface vlan-interface 100
[Switch A-Vlan-interface100] ip address 100.10.0.1 255.255.255.0
[Switch A-Vlan-interface100] isis enable
[Switch A] interface vlan-interface 101
[Switch A-Vlan-interface101] ip address 100.0.0.1 255.255.255.0
[Switch A-Vlan-interface101] isis enable
[Switch A] interface vlan-interface 102
[Switch A-Vlan-interface102] ip address 100.20.0.1 255.255.255.0
[Switch A-Vlan-interface102] isis enable
```

Configure Switch B

```
[Switch B] isis
[Switch B-isis] network-entity 86.0001.0000.0000.0006.00
[Switch B] interface vlan-interface 101
[Switch B-Vlan-interface101] ip address 200.10.0.1 255.255.255.0
[Switch B-Vlan-interface101] isis enable
[Switch B] interface vlan-interface 102
[Switch B-Vlan-interface102] ip address 200.0.0.1 255.255.255.0
[Switch B-Vlan-interface102] isis enable
[Switch B] interface vlan-interface 100
[Switch B-Vlan-interface100] ip address 100.10.0.2 255.255.255.0
[Switch B-Vlan-interface100] isis enable
```

Configure Switch C

```
[Switch C] isis
[Switch C-isis] network-entity 86.0001.0000.0000.0007.00
[Switch C] interface vlan-interface 101
[Switch C-Vlan-interface101] ip address 200.10.0.2 255.255.255.0
[Switch C-Vlan-interface101] isis enable
[Switch C] interface vlan-interface 100
[Switch C-Vlan-interface100] ip address 200.20.0.1 255.255.255.0
[Switch C-Vlan-interface100] isis enable
```

Configure Switch D

```
[Switch D] isis
[Switch D-isis] network-entity 86.0001.0000.0000.0008.00
[Switch D] interface vlan-interface 102
[Switch D-Vlan-interface102] ip address 100.20.0.2 255.255.255.0
[Switch D-Vlan-interface102] isis enable
[Switch D] interface vlan-interface 100
[Switch D-Vlan-interface100] ip address 100.30.0.1 255.255.255.0
[Switch D-Vlan-interface100] isis enable
```

BGP/MBGP Overview

Introduction to BGP

Border gateway protocol (BGP) is an inter-autonomous system (inter-AS) dynamic route discovery protocol. Three early versions of BGP are BGP-1 (RFC 1105), BGP-2 (RFC 1163) and BGP-3 (RFC 1267). The current version is BGP-4 (RFC 1771) that is applied to advertised structures and supports classless inter-domain routing (CIDR). Actually, BGP-4 is becoming the external routing protocol standard of the Internet, which is frequently used between ISPs.

The characteristics of BGP are as follows:

- BGP is an external gateway protocol (EGP). Different from such internal routing protocols as OSPF and RIP, it focuses on route propagation control and selection of best routes other than discovery and calculation of routes.
- It eliminates routing loop by adding AS path information to BGP routes.
- It enhances its own reliability by using TCP as the transport layer protocol.
- When routes are updated, BGP only transmits updated routes, which greatly reduces bandwidth occupation by route propagation and can be applied to propagation of a great amount of routing information on the Internet.
- BGP-4 supports CIDR, which is an important improvement to BGP-3.
- In consideration of management and security, users desire to perform control over outgoing and incoming routing information of each AS. BGP-4 provides abundant route policies to implement flexible filtering and selecting of routes.
- BGP-4 can be extended easily to support new developments of the network.



- CIDR handles IP addresses in an entirely new way, that is, it does not distinguish networks of Class A, Class B and Class C. For example, an invalid Class C network address 192.213.0.0 (255.255.0.0) can be expressed as 192.213.0.0/16 in CIDR mode, which is a valid super network. Here /16 means that the subnet mask is composed of the first 16 bits from the left.
- The introduction of CIDR simplifies route summary. Actually, route summary is the process of aggregating several different routes, which turns advertisement processes of several routes to the advertisement of single route so as to simplify the routing table.

BGP runs on a router in any of the following modes:

- Internal BGP (IBGP)
- External BGP (EBGP)

The BGP is called IBGP when it runs in an AS and EBGP when it runs among different ASs.

BGP Message Types

BGP is driven by messages, which include the following types:

- Type 1, OPEN: The first message sent after the creation of a connection to create association between BGP peers.
- Type 2, UPDATE: The most important information in BGP system used to exchange routing information between peers. It is composed of up to three parts, that is, unreachable route, path attributes and network layer reachable information (NLRI).
- Type 3, NOTIFICATION: Used to notify errors.
- Type 4, KEEPALIVE: Used to check connectivity.
- Type 5, ROUTE-REFRESH: Used to advertise its own route refreshing capability.

The first four types are defined in RFC1771, while the last one is in RFC2918 (Route Refresh Capability for BGP-4).

BGP Routing Mechanism

On the first startup of the BGP system, the BGP router exchanges routing information with its peers by transmitting the complete BGP routing table, after that only Update messages are exchanged. In the operating of the system, keepalive messages are received and transmitted to check the connections between various neighbors.

The router transmitting BGP messages is called a BGP speaker, which receives and generates new routing information continuously and advertises the information to the other BGP speakers. When a BGP speaker receives a new route from another AS, it will advertise the route, if the route is better than the currently known route or is a new route, to all the other BGP speakers in the AS.

BGP speakers among which messages are exchanged are peers to one another. Multiple related peers compose a peer group.

Route advertisement policy

In the implementation of Switch 8800 Family series, these policies are used by BGP when advertising routes:

- If there are multiple routes available, a BGP speaker only selects the optimum one.
- A BGP only advertises its own route to its peers.
- A BGP advertises the routes obtained from EBGP to all its BGP peers (including EBGP and IBGP peers).
- A BGP speaker does not advertise the routes obtained from IBGP to its IBGP peers.
- A BGP speaker advertises the routes obtained from IBGP to its IBGP peers (In 3Com Switch 8800 Family series, BGP and IGP are asynchronous.)
- Once the connection is set up, a BGP speaker will advertise all its BGP routes to its peers.

Route selection policy

In the implementation of Switch 8800 Family series, these policies are adopted for BGP to select routes:

- First discard the routes unreachable to the next hop.
- First select the routes with the highest local preference.
- First select the routes rooted from the router itself.
- First select the routes with the least AS-paths.
- First select the routes with the lowest origin.
- First select the routes with the lowest MED value.
- First select the routes learned from EBGp.
- First select the routes advertised by the router with the lowest ID.

MBGP MBGP overview

As described at the beginning of this chapter, BGP, as the practical exterior gateway protocol, is widely used in interconnection between autonomous systems. The traditional BGP-4 can only manage the routing information of IPv4 and has limitation in inter-AS routing when used in the application of other network layer protocols (such as IPv6 etc).

In order to support multiple network layer protocols, IETF extended BGP-4 and formed MBGP (Multiprotocol Extensions for BGP-4, multiple protocols extension of BGP-4). The present MBGP standard is RFC2858.

MBGP is backward compatible, that is, a router supporting BGP extension can be interconnected with a router that does not support it.

MBGP extension attributes

In the packets BGP-4 uses, three pieces of information related to IPv4 are carried in the update packet. They are network layer reachability information (NLRI), Next_Hop (The next hop address) in path attribute and Aggregator in path attribute (This attribute includes the BGP speaker address which forms the summary route).

When multiple network layer protocols are supported, it is necessary for BGP-4 to reflect the information of the specified network layer protocol to NLRI and the Next_Hop. Two new routing attributes are introduced in MBGP:

- MP_REACH_NLRI: Multiprotocol Reachable NLRI, used to advertise reachable routes and the next hop information.
- MP_UNREACH_NLRI: Multiprotocol Unreachable NLRI, used to delete unreachable routes.

These two attributes are optional non-transitive. Therefore, the BGP speaker that does not provide multiple protocols ability will ignore the information of them nor transfer them to other peers.

Address family

The network layer protocols are differentiated by address families in BGP. See RFC1700 (assigned numbers) for the possible values of these address families.

Switch 8800 Family series provide various MBGP extended applications, including extension of multicast, VPN, and so on. Different extended applications should be configured in their own address family views.

For more information about the commands executed in MBGP address family view, see "Multicast Protocol" and "MPLS Configuration" of this manual.

BGP Peer and Peer Group

Definition of peer and peer group

As described in Section "BGP Routing Mechanism" "BGP Routing Mechanism", BGP speakers among which messages are exchanged are peers to one another. Multiple related peers compose a peer group, and multiple related peers compose a peer group.

Relationship between peer configuration and peer group configuration

In Switch 8800 Family series, a BGP peer must belong to a peer group. If you want to configure a BGP peer, you need first to create a peer group and then add a peer into the group.

BGP peer group feature can simplify user configuration and improve route advertisement efficiency. When added into a peer group, a peer inherits all the configuration of the group.

If the configuration of a peer group changes, the configuration of its member peers also alters. Some attributes can be configured to a particular member peer by specifying its IP address. The attributes configured in this way is with higher priority than those by configuring for peer group. It should be noted that all member peers must use the same update policy as its group, but may use different ingress policy.

Configuring BGP

These categories are involved in BGP configuration:

- 1** Basic BGP configuration
 - "Enabling BGP"
 - "Configuring Basic Features for BGP Peer"
- 2** BGP peer configuration
 - "Configuring application features of a BGP peer (group)"
 - "Configuring Route Filtering of a Peer (group)"
- 3** BGP route configuration
 - "Configuring Network Routes for BGP Distribution"
 - "Configuring the Interaction between BGP and IGP (Importing IGP Routes)"
 - "Configuring to Permit BGP to Import Default Routes of Other Protocols"
 - "Configuring BGP Route Aggregation"
 - "Configuring BGP Route Filtering"
 - "Configuring BGP Route Dampening"
- 4** BGP protocol configuration
 - "Configuring BGP Preference"

- “Configuring BGP Timer”
 - “Configuring the Local Preference”
 - “Configuring MED for AS”
- 5 BGP application configuration
- “Comparing the MED Routing Metrics from the Peers in Different ASs”
- 6 BGP networking configuration
- “Configuring BGP Route Reflector”
 - “Configuring BGP AS Confederation Attribute”
 - “Configuring BGP Load Balancing”
 - “Setting the Switch for Adjacency State Output”
- 7 Others
- “Clearing BGP Connection”
 - “Refreshing BGP Routes”

Enabling BGP

To enable BGP, local AS number should be specified. After the enabling of BGP, local router listens to BGP connection requests sent by adjacent routers. To make the local router send BGP connection requests to adjacent routers, refer to the configuration of the **peer** command. When BGP is disabled, all established BGP connections will be disconnected.

Perform the following configuration in system view.

Table 346 Enable/Disable BGP

Operation	Command
Enable BGP and enter the BGP view	bgp <i>as-number</i>
Disable BGP	undo bgp [<i>as-number</i>]

By default, BGP is not enabled.

Configuring Basic Features for BGP Peer

When configuring a MBGP peer (group), you should first configure AS ID for it and then enter the corresponding address family view to activate the association.

Perform the following configurations in BGP view.

Creating a peer group

A BGP peer must belong to a peer group. Before configuring a BGP peer, a peer group to which the peer belongs must be created first.

Table 347 Create a peer group

Operation	Command
Create a peer group	group <i>group-name</i> [internal external]
Delete the specified peer group	undo group <i>group-name</i>

There are two types of BGP peer group, IBGP and EBGP. Using the **internal** keyword to create an IBGP peer group. You can use the **external** keyword to

create an EBGP peer group and sub-AS peer groups inside a confederation. *group-name* is locally significant.

The default type of BGP peer group is IBGP.

Configuring AS number of an EBGP peer group

You can specify AS number for an EBGP peer group, but IBGP needs no AS number. When a peer group is specified with an AS number, all its member peers inherit the AS number.

Table 348 Configure AS number of a EBGP peer group

Operation	Command
Configure the AS number of the EBGP peer group	peer <i>group-name</i> as-number <i>as-number</i>
Delete the AS number of the EBGP peer group	undo peer <i>group-name</i> as-number <i>as-number</i>

If a peer group has peers, you cannot specify an AS number for the peer group. In addition, deleting the AS number of a peer group will delete all peers in it.

Adding a member to a peer group

A BGP peer must belong to a peer group. If you want to configure a BGP peer, you need first to create a peer group and then add a peer into the group.

Table 349 Create a peer group and add a member

Operation	Command
Add a peer to the peer group	peer <i>peer-address</i> group <i>group-name</i> [as-number <i>as-number</i>]
Delete a peer	undo peer <i>peer-address</i>

If you want to add a peer to an IBGP peer group, this command cannot specify AS numbers.

When a peer is added to an EBGP peer group and the peer group is defined with an AS number, all its member peers inherits the configuration of the group and you cannot specify the AS numbers. If the AS number of the peer group is not specified, each peer added to it should be specified with its own AS number. AS numbers of peers in a same peer group can be different.

Configuring the state of a peer/peer group

BGP peer/peer group has two types of state: enabled and disabled. The BGP speakers do not exchange routing information with the disabled peer or peer group.

Table 350 Configure the state of a peer/peer group

Operation	Command
Enable a peer/peer group	peer { <i>group-name</i> <i>peer-address</i> } enable
Disable a peer/peer group	undo peer { <i>group-name</i> <i>peer-address</i> } enable

By default, only BGP peer groups of IPv4 unicast address family are enabled. Other peer types or peer group types are disabled, consequently exchanging no routing information.

When exchanging routing information between BGP speakers, the peer group must be enabled first and then the peer should be added to the enabled peer group.

Configuring the Graceful-restart ability of a peer or peer group

Table 351 Enable/disable the Graceful-restart ability of a peer or peer group

Operation	Command
Enable the Graceful-restart ability of a peer or peer group	peer { <i>peer-address</i> <i>group-name</i> } graceful-restart
Disable the Graceful-restart ability of a peer or peer group	undo peer { <i>peer-address</i> <i>group-name</i> } graceful-restart

Configuring Graceful-restart Restart-time of a peer or peer group

Table 352 Configure Graceful-restart Restart-time of a peer or peer group

Operation	Command
Configure Graceful-restart Restart-time of a peer or peer group	peer <i>group-name</i> restart-timer <i>time-value</i>
Restore the default value of Graceful-restart Restart-time of a peer or peer group	undo peer <i>group-name</i> restart-timer

The setting of the Restart-time value is not directly related to the configuration of Graceful-restart. That is, the Restart-time can be configured before the configuration of the Graceful-restart ability. The default value of the Restart-time is 180 seconds.

Configuring description of a peer (group)

Description of a peer (group) can be configured to facilitate network maintenance.

Table 353 Configure description of a peer (group)

Operation	Command
Configure description of a peer (group)	peer { <i>group-name</i> <i>peer-address</i> } description <i>description-line</i>
Delete description of a peer (group)	undo peer { <i>group-name</i> <i>peer-address</i> } description

By default, no BGP peer (group) description is set.

Configuring timer of a peer (group)

The **peer timer** command is used to configure timers of a BGP peer (group), including the keep-alive message interval and the hold timer. The preference of this command is higher than the **timer** command that is used to configure timers for the whole BGP peers.

Perform the following configuration in BGP view.

Table 354 Configure timer of a peer (group)

Operation	Command
Configure keep-alive message interval and hold timer of a peer (group)	peer { <i>group-name</i> <i>peer-address</i> } timer keep-alive <i>keepalive-interval</i> hold <i>holdtime-interval</i> }

Table 354 Configure timer of a peer (group)

Operation	Command
Restore the default value of keep-alive message interval and hold timer of a peer (group)	undo peer { <i>group-name</i> <i>peer-address</i> } timer

By default, the Keep-alive message is sent every 60 seconds and the value of the hold timer is 180 seconds.

Configuring the interval at which route update messages are sent by a peer group

Table 355 Configure the interval at which route update messages are sent by a peer group

Operation	Command
Configure the route update message interval of a peer group	peer <i>group-name</i> route-update-interval <i>seconds</i>
Restore the default route update message interval of a peer group	undo peer <i>group-name</i> route-update-interval

By default, the intervals at which route update messages are sent by an IBGP and EBGP peer group are 5 seconds and 30 seconds respectively

Configuring application features of a BGP peer (group)

Configuring to permit connections with EBGP peer groups on indirectly connected networks

Generally, EBGP peers must be connected physically. Otherwise the command below can be used to perform the configuration to make them communicate with each other normally.

Perform the following configuration in BGP view.

Table 356 Configure to permit connections with EBGP peer groups on indirectly connected networks

Operation	Command
Configure to permit connections with EBGP peer groups on indirectly connected networks	peer <i>group-name</i> ebgp-max-hop [<i>ttl</i>]
Configure to permit connections with EBGP peer groups on directly connected network only	undo peer <i>group-name</i> ebgp-max-hop

By default, only the connections with EBGP peer groups on directly connected networks are permitted. *ttl* refers to time-to-live in the range of 1 to 255 with the default value as 64.

Configuring an IBGP peer group to be a client of a route reflector

Perform the following configuration in BGP view.

Table 357 Configure an IGMP peer group to be a client of a route reflector

Operation	Command
Configure a peer group to be a client of a route reflector	peer <i>group-name</i> reflect-client

Table 357 Configure an IGMP peer group to be a client of a route reflector

Operation	Command
Cancel the configuration of making the peer group as the client of the BGP route reflector	undo peer <i>group-name</i> reflect-client

This configuration can be applied to IBGP peer groups only.

By default, all IBGP peers in the autonomous system must be fully connected. Moreover, neighbors do not notify the learned IBGP routes.

Configuring to send default route to a peer group

If you only need to notify a default route between a pair of BGP peer instead of transmitting the default route within the whole network, you can use the **peer default-route-advertise** command.

Perform the following configuration in BGP view.

Table 358 Configure to send default route to a peer group

Operation	Command
Configure to send default route to a peer group	peer <i>group-name</i> default-route-advertise
Configure not to send default route to a peer group	undo peer <i>group-name</i> default-route-advertise

By default, a BGP speaker does not send default route to any peer group.

After you use the **peer default-route-advertise** command, the local router will send a default route with the next hop as itself to the peer unconditionally, even if there is no default route in BGP routing table.

Configuring itself as the next hop when advertising routes

In general, when sending routes to the EBGP peer, the BGP speaker will set the next hop address of the routing information as the local address. When sending routes to the IBGP peer, the BGP speaker will not modify the next hop address.

In some networking conditions, when the routes are sent to the IBGP peer, you can configure the local address of the sender as the next hop, consequently ensuring the IBGP neighbors can find the correct next hop.

Perform the following configuration in BGP view.

Table 359 Configure itself as the next hop when advertising routes

Operation	Command
Configure itself as the next hop when advertising routes	peer <i>group-name</i> next-hop-local
Disable the specification of itself as the next hop when advertising routes	undo peer <i>group-name</i> next-hop-local

Removing private AS numbers while transmitting BGP update messages

Generally, the AS numbers (public AS numbers or private AS numbers) are included in the AS paths while transmitting BGP update messages. This command

is used to configure certain outbound routers to ignore the private AS numbers while transmitting update messages.

Perform the following configuration in BGP view.

Table 360 Remove private AS numbers while transmitting BGP update messages

Operation	Command
Remove private AS numbers while transmitting BGP update messages	peer <i>group-name</i> public-as-only
Include private AS numbers while transmitting BGP update messages	undo peer <i>group-name</i> public-as-only

By default, the private AS numbers are included during BGP update messages transmission.

The configuration can only be applied to the peer group.

Configuring to send the community attributes to a peer group

Perform the following configuration in BGP view.

Table 361 Configure to send the community attributes to a peer group

Operation	Command
Configure to send the community attributes to a peer group	peer <i>group-name</i> advertise-community
Configure not to send the community attributes to a peer group	undo peer <i>group-name</i> advertise-community

By default, the BGP speaker does not send the community attributes to a peer group.

Configuring the repeating time of local AS

BGP records the passed AS numbers in the routing information, and checks route loop depending on whether the AS number are repeated. In some special applications, it is allowed to receive the routing information with the repeated AS number.

Perform the following configuration in BGP view.

Table 362 Configure the repeating time of local AS

Operation	Command
Configure the repeating time of local AS	peer { <i>group-name</i> <i>peer-address</i> } allow-as-loop [<i>number</i>]
Remove the repeating time of local AS	undo peer { <i>group-name</i> <i>peer-address</i> } allow-as-loop

By default, the allowed repeating time of local AS is set to 1.

Specifying the source interface of a route update packet

Generally, the system specified the source interface of a route update packet. When the interface fails to work, in order to keep the TCP connection valid, the

interior BGP session can be configured to specify the source interface. This command is usually used on the Loopback interface.

Table 363 Specify the source interface of a route update packet

Operation	Command
Specify the source interface of a route update packet	peer { <i>peer-address</i> <i>group-name</i> } connect-interface <i>interface-type interface-name</i>
Use the best source interface	undo peer { <i>peer-address</i> <i>group-name</i> } connect-interface <i>interface-type interface-name</i>

By default, BGP uses the interface to establish BGP links for the source interface of a route update packet.

Configuring BGP MD5 authentication password

BGP uses TCP as its transport layer. For the sake of high security, you can configure MD5 authentication password when setting up a TCP connection. In other words, BGP MD5 authentication just sets password for TCP connection, but not for authenticating BGP packets. The authentication is implemented by TCP.

Perform the following configuration in BGP view.

Table 364 Configure BGP MD5 authentication

Operation	Command
Configure MD5 authentication password	peer { <i>group-name</i> <i>peer-address</i> } password { cipher simple } <i>password</i>
Cancel MD5 authentication	undo peer { <i>group-name</i> <i>peer-address</i> } password

In BGP, no MD5 authentication is performed in setting up TCP connections by default.



The multicast extension configured in BGP view is also available in MBGP, since they use the same TCP link.

Configuring Route Filtering of a Peer (group)

Switch 8800 Family series support filtering imported and advertised routes for peers (groups) through Route-policy, AS path list, ACL and ip prefix list.

The route filtering policy of advertised routes configured for each member of a peer group must be same with that of the peer group but their route filtering policies of ingress routes may be different.

Perform the following configuration in BGP view.

Configuring route policy for a peer (group)

Table 365 Configure route policy for a peer (group)

Operation	Command
Configure the ingress route policy for a peer (group)	peer { <i>group-name</i> <i>peer-address</i> } route-policy <i>route-policy-name</i> import
Remove the ingress route policy of a peer (group)	undo peer { <i>group-name</i> <i>peer-address</i> } route-policy <i>policy-name</i> import
Configure the egress route policy for a peer group	peer <i>group-name</i> route-policy <i>route-policy-name</i> export

Table 365 Configure route policy for a peer (group)

Operation	Command
Remove the egress route policy of a peer group	undo peer <i>group-name</i> route-policy <i>route-policy-name</i> export

Configuring route filtering policy based on IP ACL for a peer (group)**Table 366** Configure route filtering policy based on IP ACL for a peer (group)

Operation	Command
Configure the ingress route filtering policy based on IP ACL for a peer (group)	peer { <i>group-name</i> <i>peer-address</i> } filter-policy <i>acl-number</i> import
Remove the ingress route filtering policy based on IP ACL of a peer (group)	undo peer { <i>group-name</i> <i>peer-address</i> } filter-policy <i>acl-number</i> import
Configure the egress route filtering policy based on IP ACL for a peer (group)	peer <i>group-name</i> filter-policy <i>acl-number</i> export
Remove the egress route filtering policy based on IP ACL for a peer (group)	undo peer <i>group-name</i> filter-policy <i>acl-number</i> export

Configuring route filtering policy based on AS path list for a peer (group)**Table 367** Configure route filtering policy based on AS path list for a peer (group)

Operation	Command
Configure the ingress route filtering policy based on AS path list for a peer (group)	peer { <i>group-name</i> <i>peer-address</i> } as-path-acl <i>acl-number</i> import
Remove the ingress route filtering policy based on AS path list of a peer (group)	undo peer { <i>group-name</i> <i>peer-address</i> } as-path-acl <i>acl-number</i> import
Configure the egress route filtering policy based on IP ACL for a peer group	peer <i>group-name</i> as-path-acl <i>acl-number</i> export
Remove the egress route filtering policy based on IP ACL for a peer group	undo peer <i>group-name</i> as-path-acl <i>acl-number</i> export

The *acl-number* argument indicates AS path list number, which is configured by means of the **ip as-path-acl** command instead of the **acl** command. For the detailed configuration, refer to “IP Routing Policy Configuration”.

Configuring route filtering policy based on address prefix list for a peer (group)**Table 368** Configure route filtering policy based on address prefix list for a peer (group)

Operation	Command
Configure the ingress route filtering policy based on address prefix list for a peer (group)	peer { <i>group-name</i> <i>peer-address</i> } ip-prefix <i>prefixname</i> import
Remove the ingress route filtering policy based on address prefix list of a peer (group)	undo peer { <i>group-name</i> <i>peer-address</i> } ip-prefix <i>prefixname</i> import
Configure the egress route filtering policy based on address prefix list for a peer group	peer <i>group-name</i> ip-prefix <i>prefixname</i> export
Remove the egress route filtering policy based on address prefix list for a peer group	undo peer <i>group-name</i> ip-prefix <i>prefixname</i> export

By default, route filtering based on address prefix list for a peer (group) is disabled.

Configuring Network Routes for BGP Distribution

Perform the following configuration in BGP view.

Table 369 Configure network routes for BGP distribution

Operation	Command
Configure the local network route for BGP distribution	network <i>ip-address address-mask</i> [route-policy <i>policy-name</i>]
Remove the local network route for BGP distribution	undo network <i>ip-address address-mask</i> [route-policy <i>policy-name</i>]

By default, no network route is configured for BGP distribution.

Configuring the Interaction between BGP and IGP (Importing IGP Routes)

BGP can transmit the internal network information of local AS to other AS. To reach such objective, the network information about the internal system learned by the local router via IGP routing protocol can be transmitted.

Perform the following configuration in BGP view.

Table 370 Import IGP routing information

Operation	Command
Configure BGP to import routes of IGP protocol	import-route <i>protocol</i> [med <i>med-value</i>] [route-policy <i>route-policy-name</i>]
Configure BGP not to import routes of IGP protocol	undo import-route <i>protocol</i>

The *protocol* argument specifies the imported source route protocols. The specified and imported source route protocols can be direct, static, rip, isis, ospf, ospf-ase, and ospf-nssa.

By default, BGP does not import the route information of other protocols.

Note that when BGP imports other routes, the default routes of other protocols are not imported.

After you configure the **import-route** command in a BGP view, you cannot import the default route of the imported source route protocols to BGP by default.

Configuring to Permit BGP to Import Default Routes of Other Protocols

Perform the following configuration in BGP view.

Table 371 Configure to permit BGP to import default routes of other protocols

Operation	Command
Configure to permit BGP to import routes of other protocols	default-route imported
Configure to permit BGP to filter the default routes of a protocol when this protocol is imported	undo default-route imported

By default, BGP does not import the default routes of other protocols when BGP is importing the routes of other protocols.

Configuring BGP Route Aggregation

The BGP supports two forms of route aggregation:

- Automatic aggregation (by means of the **summary** command): The aggregation of IGP subnet routes imported by the BGP. With automatic aggregation enabled, the BGP will not receive subnet routes imported from the IGP, and routes on natural network segments will be aggregated;
- Manual aggregation (by means of the **aggregate** command): The aggregation of the BGP local routes. In general, the preference of manual aggregation is higher than that of automatic aggregation.

Perform the following configuration in BGP view.

Table 372 Configure BGP route aggregation

Operation	Command
Enable automatic aggregation of subnet routes	summary
Disable automatic aggregation of subnet routes	undo summary
Enable local route aggregation	aggregate <i>address mask</i> [as-set attribute-policy <i>route-policy-name</i> detail-suppressed origin-policy <i>route-policy-name</i> suppress-policy <i>route-policy-name</i>]*
Disable local route aggregation	undo aggregate <i>address mask</i> [as-set attribute-policy <i>route-policy-name</i> detail-suppressed origin-policy <i>route-policy-name</i> suppress-policy <i>route-policy-name</i>]*

By default, the BGP does not perform local route aggregation.

Configuring BGP Route Filtering

Configuring BGP to filter the received route information

The routes received by the BGP can be filtered, and only those routes that meet the certain conditions will be received by the BGP.

Perform the following configuration in BGP view.

Table 373 Configure imported route filtering

Operation	Command
Filter received routing information advertised by specified address	filter-policy gateway <i>ip-prefix-name</i> import
Disable filtering of received routing information advertised by specified address	undo filter-policy gateway <i>ip-prefix-name</i> import
Filter received global routing information	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } import
Disable filtering of received global routings information	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } import

By default, the BGP does not filter the received routes.

Configuring to filter the routes advertised by other protocols

Perform the following configuration in the BGP view.

Table 374 Configure to filter the routes advertised by other routing protocols

Operation	Command
Configure to filter the routes advertised by other routing protocols	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>routing-protocol</i>]

Table 374 Configure to filter the routes advertised by other routing protocols

Operation	Command
Cancel the filtering of the routes advertised by other routing protocols	undo filter-policy <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>routing-protocol</i>]

By default, BGP does not receive the routing information advertised by other routing protocols.



- The **filter-policy import** command filters BGP route received from the neighbors. The routes that cannot pass the filter will not be added to the routing table, and will not be advertised to the neighbors.
- The **filter-policy export** command filters all the advertised routes, including routes imported by using the **import-route** command, and BGP routes learned from the neighbors.
- If the **filter-policy export** command does not specify which route to be filtered, then the all the routes imported by the **import-route** command and the advertised BGP routes will be filtered.

Configuring BGP Route Dampening

Configure BGP route dampening

Route dampening is primarily used to address the route instability problem. The main possible reason for route instability is the intermittent disappearance and re-emergence of the route that formerly existed in the routing table, and this situation is called flapping. When flapping occurs, update packet will be propagated on the network repeatedly, which will occupy much bandwidth and much processing time of the router. You have to find measures to avoid it. The technology controlling unstable route is called route dampening.

The dampening divides the route into the stable route and unstable route, the latter of which shall be suppressed (not to be advertised). The history performance of the route is the basis to evaluate the future stability. When the route flapping occurs, penalty will be given, and when the penalty reaches a specific threshold, the route will be suppressed. With time going, the penalty value will decrease according to power function, and when it decreases to certain specific threshold, the route suppression will be eliminated and the route will be re-advertised.

Perform the following configuration in BGP view.

Table 375 Configure BGP route dampening

Operation	Command
Configure BGP route dampening	dampening [<i>half-life-reachable</i> <i>half-life-unreachable</i> <i>reuse suppress ceiling</i>] [route-policy <i>route-policy-name</i>]
Cancel BGP route dampening	undo dampening

By default, route dampening is disabled.

Clear route dampening information

Perform the following configuration in user view to clear route dampening information.

Table 376 Clear route dampening information

Operation	Command
Clear route dampening information	reset bgp dampening [<i>network-address</i> [<i>mask</i>]]

After you use the **reset bgp dampening** command, the command will release the suppression of suppressed routes.

Configuring BGP Preference

Three types of routes may be involved in BGP: routes learned from external peers (EBGP), routes learned from internal peers (IBGP) and local-originated routes. You can set preference values for the three types of route.

Perform the following configuration in BGP view.

Table 377 Configure BGP preference

Operation	Command
Configure BGP preference	preference <i>ebgp-value ibgp-value local-value</i>
Restore the default preference	undo preference

The *ebgp-value*, *ibgp-value* and *local-value* arguments are in the range of 1 to 256. By default, the first two is 256 and the last one is 130.

Configuring BGP Timer

After a BGP connection is established between two peers, they send Keepalive message to each other periodically. If a router receives no Keepalive message or any other type of packet within the set connection holdtime, the router regards the BGP connection has been interrupted and quits the BGP connection.

When a router establishes a BGP connection with a peer, the router will compare their holdtime values and uses the smaller time as the negotiated holdtime. If the negotiation result is 0, the router will not send Keepalive message and will not detect whether the holdtime expires.

Perform the following configuration in BGP view.

Table 378 Configure BGP timers

Operation	Command
Configure BGP timers	timer keep-alive <i>keepalive-interval hold</i> <i>holdtime-interval</i>
Restore the default timer value	undo timer

By default, the interval of sending keepalive is 60 seconds. The holdtime value is 180 seconds.

The reasonable maximum interval of sending Keepalive is one third of the holdtime value. The interval of sending Keepalive cannot be less than 1 second. As a result, if the holdtime is not 0 seconds, the minimum holdtime value is 3 seconds.

Configuring the Local Preference

When BGP select routes, it will select the route of the highest local preference.

Perform the following configuration in BGP view.

Table 379 Configure the local preference

Operation	Command
Configure the local preference	default local-preference <i>value</i>
Restore the default local preference	undo default local-preference

The local preference is transmitted only when the IBGP peers exchange the update packets and it will not be transmitted beyond the local AS.

By default, the local preference is 100.

Configuring MED for AS

Multi-Exit Discriminators (MED) attribute is the external metric for a route. AS uses the local preference to select the route to the outside, and uses the MED to determine the optimum route for entering the AS. When a router running BGP gets routes with the same destination address but different next hops through different external peers, it will select the route of the smallest MED as the optimum route, provided that all the other conditions are the same.

Perform the following configuration in BGP view.

Table 380 Configure an MED metric for the system

Operation	Command
Configure an MED metric for the system	default med <i>med-value</i>
Restore the default MED metric of the system	undo default med

By default, MED metric is 0.

The router configured above only compares the route MED metrics of different EBGP peers in the same AS. Using the **compare-different-as-med** command, you can compare the route MED metrics of the peers in different ASs.

Comparing the MED Routing Metrics from the Peers in Different ASs

It is used to select the best route. The route with smaller MED value will be selected.

Perform the following configuration in BGP view.

Table 381 Compare the MED routing metrics from the peers in different ASs

Operation	Command
Compare the MED routing metrics from peers in different ASs	compare-different-as-med
Disable comparison of the MED routing metrics from peers in different ASs	undo compare-different-as-med

By default, MED comparison is not allowed among the routes from the neighbors in different ASs.

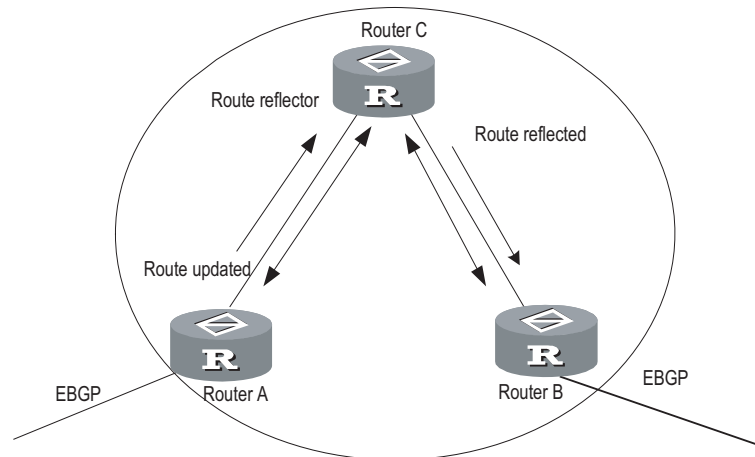
It is not recommended to use this configuration unless you can make sure that the ASs adopt the same IGP and routing method.

Configuring BGP Route Reflector

To ensure the interconnection between IBGP peers, it is necessary to establish a fully connected network. If there are many IBGP peers, large overhead is needed to establish a fully connected network.

Route reflecting can solve the problem. Route reflector is the centralized point of other routers, and other routers are called the clients. The client is the peer of the route reflector and switching the routing information with it. The route reflector will reflect the information in order among the clients.

Figure 90 The route reflector diagram



In Figure 90, Router C is a route reflector with two peer clients: Router A and Router B. Router A sends to Router C the update packet from an external peer. Router C sends the update packet to Router B. After using reflecting technology, you do not need to establish a connection between Router A and Router B. You only need to connect Router C to Router A and Router B respectively.

If a BGP router is not either a reflector or client, we call the BGP router non-client. You still need connect non-clients to reflectors and non-clients.

You only need to configure route reflecting for the route reflector. When configuring the route reflector, you must specify the routers to serve as clients.

Configuring an IBGP peer group as route reflector client

Perform the following configuration in BGP view.

Table 382 Configure an IBGP peer group as route reflector client

Operation	Command
Configure an IBGP peer group as route reflector client	peer group-name reflect-client
Disable an IBGP peer group from being a route reflector client	undo peer group-name reflect-client

This command works on IBGP peer groups only.

By default, all IBGP routes in an AS must be full-connected, and neighbors do not advertise learned IBGP routes to one another.

Configuring the route reflection between clients

Perform the following configuration in BGP view.

Table 383 Configure the route reflection between clients

Operation	Command
Enable route reflection between clients	reflect between-clients
Disable route reflection between clients	undo reflect between-clients

By default, the route reflection between clients is allowed. If the clients are fully connected, for the purpose of overhead reduction, it is recommended to use the **undo reflect between-clients** command to disable the route reflection between clients.

Configuring the cluster ID

Generally, there is only one route reflector in a cluster which is identified by the router ID of the route reflector.

Perform the following configuration in BGP view.

Table 384 Configure the Cluster_ID of the route reflector

Operation	Command
Configure the Cluster_ID of the route reflector	reflector cluster-id { <i>cluster-id</i> <i>address</i> }
Cancel the Cluster_ID of the route reflector	undo reflector cluster-id

The autonomous system possibly generates routing loop due to the route reflector in a cluster. After leaving a cluster, a routing update packet possibly tries to go back to the cluster. Because the routing update packet has not left an AS, the traditional AS path method cannot detect the loop inside the AS. When configuring route reflectors, you can use the following two methods to avoid loop inside the AS. One is to use the cluster ID; the other is to use Originator_ID of a route reflector.

If you configure Originator_ID improperly, the originator will discard the update packet when the update packet goes back to the originator. You do not need to configure Originator_ID. Originator_ID automatically takes effect when BGP is enabled.

Configuring BGP AS Confederation Attribute

Confederation provides the method to handle the booming IBGP network connections inside AS. It divides the AS into multiple sub-AS, in each of which all IBGP peers are fully connected, and are connected with other sub-AS of the confederation.

The shortcomings of confederation are that it is required that the route be re-configured upon switching from non-confederation to confederation solution, and that the logic topology be basically changed. Furthermore, the path selected via confederation may not be the best path if there is no manually-set BGP policy.

Configuring confederation_ID

In the eye of the BGP speakers that are not included in the confederation, multiple sub-ASs that belong to the same confederation are a whole. The external network

does not need to know the status of internal sub-ASs, and the confederation ID is the AS number identifying the confederation as a whole.

Perform the following configuration in BGP view.

Table 385 Configure confederation_ID

Operation	Command
Configure confederation_ID	confederation id <i>as-number</i>
Cancel confederation_ID	undo confederation id

By default, the confederation_ID is not configured.

The configured confederation_ID and the existing AS number of a peer or peer group cannot be the same.

Configuring sub-AS belonging to the confederation

Configure confederation_ID first, and then configure the sub-AS belonging to the confederation. One confederation includes up to 32 sub-AS.

Perform the following configuration in BGP view.

Table 386 Configure sub-AS belonging to the confederation

Operation	Command
Configure a confederation consisting of which sub-ASs	confederation peer-as <i>as-number-1</i> [... <i>as-number-n</i>]
Cancel the specified sub-AS in the confederation	undo confederation peer-as [<i>as-number-1</i>] [... <i>as-number-n</i>]

By default, no autonomous system is configured as a member of the confederation.

The configured sub-AS number is valid only inside the confederation. In addition, the number cannot be the same as the AS number of a peer in the peer group for which you have not configured an AS number.

Configuring AS confederation attribute compatible with nonstandard

If it is necessary to perform the interconnection with the devices whose implementation mechanism is different from that of RFC1965, you must configure all the routers in the confederation.

Perform the following configuration in BGP view.

Table 387 Configure AS confederation attribute compatible with nonstandard

Operation	Command
Configure AS confederation attribute compatible with nonstandard router	confederation nonstandard
Cancel AS confederation attribute compatible with nonstandard router	undo confederation nonstandard

By default, the configured confederation is consistent with RFC1965.

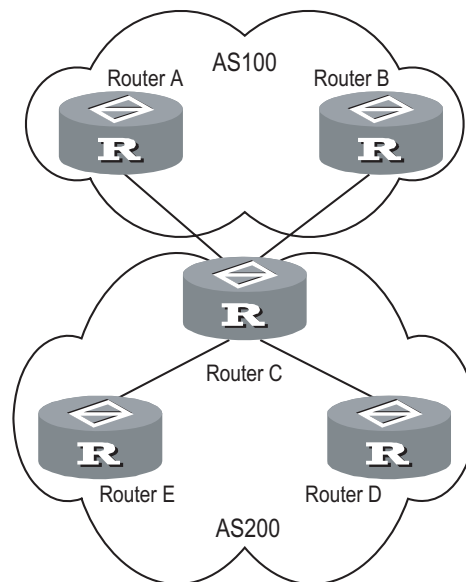
Configuring BGP Load Balancing

As BGP is a routing protocol for route selection only, it does not provide a route calculation method. Therefore, it is not possible to determine whether to enable load balancing based on a definite metric value. However, the BGP owns a variety of route selection rules, so it supports conditional load balancing after route selection, namely, by adding load balancing into the BGP route selection rules.

With BGP load balancing enabled, during route selection, the BGP will add rule between the last two route selection rules "select routes learned from EBGP with preference" and "select routes advertised by the router with the lowest BGP ID": if load balancing is enabled, and if there are multiple exterior routes to the same AS or AS confederation, the BGP will select multiple routes, depending on the number of routes, for load balancing. The BGP supports load balancing for routes learned from EBGP/IBGP under the following conditions:

- In case of routes learned from EBGP, the BGP performs load balancing for routes from the same AS and with the same med value only;
- In case of routes learned from IBGP, the BGP performs load balancing for routes with the same med value, local_pref, AS_PATH and origin attributes.

Figure 91 A schematic diagram of BGP load balancing



As shown in Figure 91, Router D and Router E are IBGP peers of Router C. When Router A and Router B simultaneously advertise two routes to the same destination to Router C, if Router C is load balancing enabled (such as balance 2), while satisfying a certain route selection rule, Router C will add both routes into the forwarding table if the two routes have the same AS_PATH attribute, so as to achieve the purpose of BGP route balancing. Router C forwards the routes to Router D and Router E only once. The AS_PATH attribute will remain unchanged, but the NEXT_HOP attribute will be changed to the address of Router C, instead of the address of the original EBGP peer. The BGP will directly transfer the other transient attributes as attributes of the optimal route.

The BGP balancing feature also applies to routing between ASs within an AS confederation.



Load balancing is not available for BGP default routes.

Perform the following configuration in BGP view.

Table 388 Enable/disable BGP load balancing

Operation	Command
Enable BGP load balancing	balance <i>balance-number</i>
Disable BGP load balancing	undo balance

By default, the BGP does not implement load balancing.

Setting the Switch for Adjacency State Output

When the switch for adjacency state output is enabled, the BGP adjacency state changes will be output to the configured terminal until the switch for adjacency state output is disabled.

Perform the following configuration in BGP view.

Table 389 Set the switch for BGP adjacency state output

Operation	Command	Description
Enter system view	system-view	-
Enter BGP view	bgp <i>as-number</i>	Required
Enable the switch for adjacency state output	log-peer-change	The BGP peer changes are not reported by default

Clearing BGP Connection

After the user changes BGP policy or protocol configuration, they must cut off the current connection so as to enable the new configuration.

Perform the following configuration in user view.

Table 390 Clear BGP connection

Operation	Command
Clear the connection between BGP and the specified peers	reset bgp <i>peer-address</i>
Clear all connections of BGP	reset bgp all
Clear the connections between the BGP and all the members of a group	reset bgp group <i>group-name</i>

Refreshing BGP Routes

It is required to re-compute associated route information when BGP routing policy changes.

Perform the following configuration in user view.

Table 391 Refresh BGP routes

Operation	Command
Refresh general BGP routes	refresh bgp { all <i>peer-address</i> group <i>group-name</i> } [multicast vpn-instance <i>instance-name</i> vpn4] { import export }

Displaying and Debugging BGP

After the above configuration, execute the **display** command in any view to display the running of the BGP configuration, and to verify the effect of the configuration. Execute the **reset** command in user view to clear the statistics of the configuration. Execute the **debugging** command in user view to debug the configuration. Execute the **reset** command in user view to reset the statistic information of BGP.

Table 392 Display and debug BGP

Operation	Command
Display the routing information in BGP routing table	display bgp routing-table [<i>ip-address</i> [<i>mask</i>]]
Display filtered AS path information in the BGP	display ip as-path-acl [<i>acl-number</i>]
Display CIDR routes	display bgp routing-table cidr
Display the routing information of the specified BGP community	display bgp routing-table community [<i>aa:nn</i>]* [no-export-subconfed no-advertise no-export]* [whole-match]
Display the routing information allowed by the specified BGP community list	display bgp routing-table community-list <i>community-list-number</i> [whole-match]
Display BGP dampened paths	display bgp routing-table dampened
Display the routing information the specified BGP peer advertised or received	display bgp routing-table peer <i>peer-address</i> { advertised received } [<i>network-address</i> [<i>mask</i>]] statistic]
Display the total number or route entries received or advertised by all BGP peers	display bgp routing-table [advertised received] statistic
Display the routes matching with the specified access-list	display bgp routing-table as-path-acl <i>acl-number</i>
Display route flapping statistics information	display bgp routing-table flap-info [regular-expression <i>as-regular-expression</i> as-path-acl <i>acl-number</i> <i>network-address</i> [<i>mask</i>]] longer-match]]
Display routes from different source ASs	display bgp routing-table different-origin-as
Display peers information	display bgp peer [<i>peer-address</i>] [verbose]
Display the configured routing information	display bgp network
Display AS path information	display bgp paths <i>as-regular-expression</i>
Display peer group information	display bgp group [<i>group-name</i>]
Display the AS path information matching the specified regular expression	display bgp routing-table regular-expression <i>as-regular-expression</i>
Display configured route-policy information	display route-policy [<i>route-policy-name</i>]
Enable/disable debugging of all BGP packets	[undo] debugging bgp all
Enable/disable BGP event debugging	[undo] debugging bgp event
Enable/disable BGP Keepalive debugging	[undo] debugging bgp keepalive [receive send] [verbose]

Table 392 Display and debug BGP

Operation	Command
Enable/Disable BGP Open debugging	[undo] debugging bgp open [receive send] [verbose]
Enable /Disable BGP packet debugging	[undo] debugging bgp packet [receive send] [verbose]
Enable/disable BGP Route-Refresh packet debugging	[undo] debugging bgp route-refresh [receive send] [verbose]
Enable/Disable information debugging of BGP normal functions.	[undo] debugging bgp normal
Enable/disable BGP Update packet debugging	[undo] debugging bgp update [receive send] [verbose]
Reset BGP flapping statistics information	reset bgp flap-info [regular-expression <i>as-regular-expression</i> as-path-acl <i>acl-number</i> <i>network-address</i> [<i>mask</i>]]

Typical BGP Configuration Examples

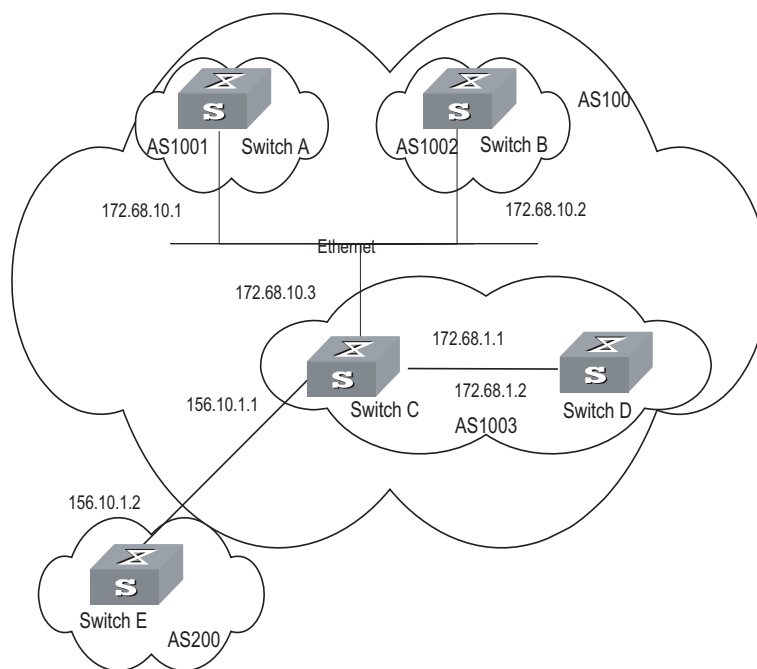
Configuring BGP AS Confederation Attribute

Network requirements

Divide the following AS 100 into three sub-AS: 1001, 1002, and 1003, and configure EBGP, confederation EBGP, and IBGP.

Network diagram

Figure 92 Network diagram for AS confederation configuration



Configuration procedure

Configure Switch A:


```
[Switch A] bgp 1001
[Switch A-bgp] confederation id 100
[Switch A-bgp] confederation peer-as 1002 1003
[Switch A-bgp] group confed1002 external
[Switch A-bgp] peer confed1002 as-number 1002
[Switch A-bgp] group confed1003 external
[Switch A-bgp] peer confed1003 as-number 1003
[Switch A-bgp] peer 172.68.10.2 group confed1002
[Switch A-bgp] peer 172.68.10.3 group confed1003
```

Configure Switch B:

```
[Switch B] bgp 1002
[Switch B-bgp] confederation id 100
[Switch B-bgp] confederation peer-as 1001 1003
[Switch B-bgp] group confed1001 external
[Switch B-bgp] peer confed1001 as-number 1001
[Switch B-bgp] group confed1003 external
[Switch B-bgp] peer confed1003 as-number 1003
[Switch B-bgp] peer 172.68.10.1 group confed1001
[Switch B-bgp] peer 172.68.10.3 group confed1003
```

Configure Switch C:

```
[Switch C] bgp 1003
[Switch C-bgp] confederation id 100
[Switch C-bgp] confederation peer-as 1001 1002
[Switch C-bgp] group confed1001 external
[Switch C-bgp] peer confed1001 as-number 1001
[Switch C-bgp] group confed1002 external
[Switch C-bgp] peer confed1002 as-number 1002
[Switch C-bgp] peer 172.68.10.1 group confed1001
[Switch C-bgp] peer 172.68.10.2 group confed1002
[Switch C-bgp] group ebgp200 external
[Switch C-bgp] peer 156.10.1.2 group ebgp200 as-number 200
[Switch C-bgp] group ibgp1003 internal
[Switch C-bgp] peer 172.68.1.2 group ibgp1003
```

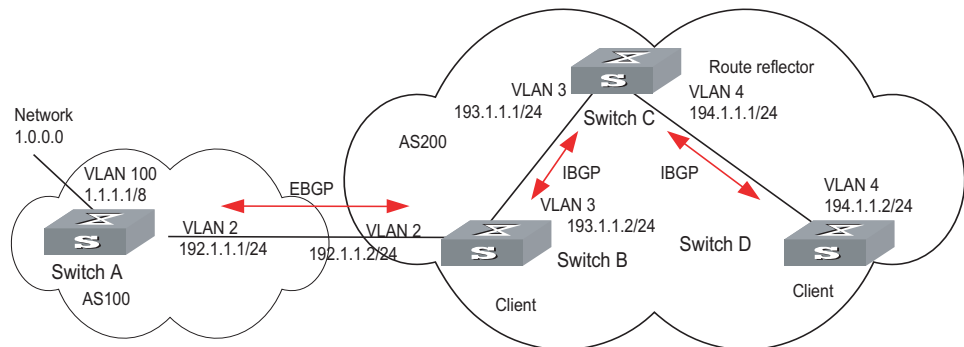
Configuring BGP Route Reflector

Network requirements

Switch B receives an update packet passing EBGp and transmits it to Switch C. Switch C is a reflector with two clients: Switch B and Switch D. When Switch C receives a route update from Switch B, it will transmit such information to Switch D. It is required to establish an IBGP connection between Switch B and Switch D, because Switch C reflects information to Switch D.

Network diagram

Figure 93 Network diagram for BGP route reflector configuration



Configuration procedure

1 Configure Switch A:

```
[Switch A] interface vlan-interface 2
[Switch A-Vlan-interface2] ip address 192.1.1.1 255.255.255.0
[Switch A-Vlan-interface2] interface Vlan-interface 100
[Switch A-Vlan-interface100] ip address 1.1.1.1 255.0.0.0
[Switch A-Vlan-interface100] quit
[Switch A] bgp 100
[Switch A-bgp] network 1.0.0.0 255.0.0.0
[Switch A-bgp] group ex external
[Switch A-bgp] peer 192.1.1.2 group ex as-number 200
```

2 Configure Switch B:

Configure VLAN 2:

```
[Switch B] interface Vlan-interface 2
[Switch B-Vlan-interface2] ip address 192.1.1.2 255.255.255.0
```

Configure VLAN 3:

```
[Switch B] interface Vlan-interface 3
[Switch B-Vlan-interface3] ip address 193.1.1.2 255.255.255.0
```

Configure BGP peers.

```
[Switch B] bgp 200
[Switch B-bgp] group ex external
[Switch B-bgp] peer 192.1.1.1 group ex as-number 100
[Switch B-bgp] group in internal
[Switch B-bgp] peer 193.1.1.1 group in
```

3 Configure Switch C:

Configure VLAN 3:

```
[Switch C] interface Vlan-interface 3
[Switch C-Vlan-interface3] ip address 193.1.1.1 255.255.255.0
```

Configure VLAN 4:

```
[Switch C] interface vlan-Interface 4
[Switch C-Vlan-interface4] ip address 194.1.1.1 255.255.255.0
```

Configure BGP peers and route reflector.

```
[Switch C] bgp 200
[Switch C-bgp] group rr internal
[Switch C-bgp] peer rr reflect-client
[Switch C-bgp] peer 193.1.1.2 group rr
[Switch C-bgp] peer 194.1.1.2 group rr
```

4 Configure Switch D:

Configure VLAN 4:

```
[Switch D] interface vlan-interface 4
[Switch D-Vlan-interface4] ip address 194.1.1.2 255.255.255.0
```

Configure BGP peers

```
[Switch D] bgp 200
group in internal
[Switch D-bgp] peer 194.1.1.1 group in
```

Using the **display bgp routing-table** command, you can view BGP routing table on Switch B. Note: Switch B has known the existence of network 1.0.0.0.

Using the **display bgp routing-table** command ,you can view the BGP routing table on Switch D. Note: Switch D also knows the existence of network 1.0.0.0.

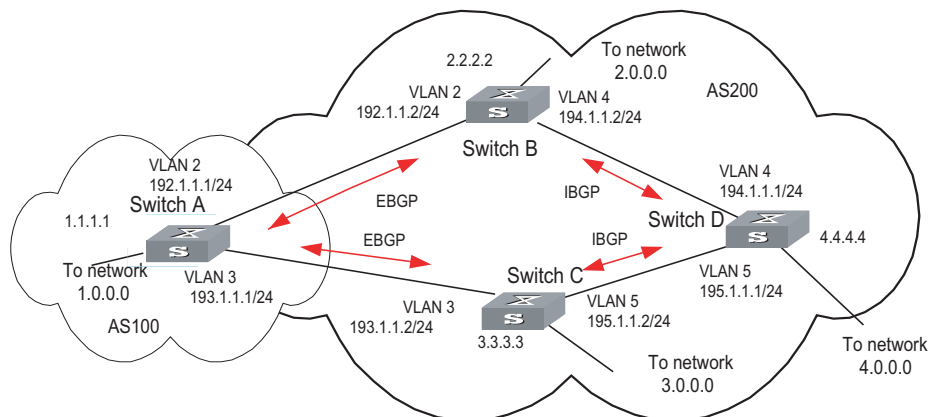
Configuring BGP Routing

Network requirements

This example illustrates how the administrators manage the routing via BGP attributes. All switches are configured with BGP, and IGP in AS 200 utilizes OSPF. Switch A is in AS 100, and Switch B, Switch C and Switch D are in AS 200. Switch A, Switch B, and Switch C operate EBGP. Switch B, Switch C and Switch D operate IBGP.

Network diagram

Figure 94 Networking diagram for BGP routing configuration



Configuration procedure**1** Configure Switch A:

```
[Switch A] interface Vlan-interface 2
[Switch A-Vlan-interface2] ip address 192.1.1.1 255.255.255.0
[Switch A] interface Vlan-interface 3
[Switch A-Vlan-interface3] ip address 193.1.1.1 255.255.255.0
```

Enable BGP

```
[Switch A] bgp 100
```

Specify the network that BGP sends to

```
[Switch A-bgp] network 1.0.0.0
```

Configure the peers

```
[Switch A-bgp] group ex192 external
[Switch A-bgp] peer 192.1.1.2 group ex192 as-number 200
[Switch A-bgp] group ex193 external
[Switch A-bgp] peer 193.1.1.2 group ex193 as-number 200
[Switch A-bgp] quit
```

Configure the MED attribute of Switch A

Add ACL on Switch A, enable network 1.0.0.0.

```
[Switch A] acl number 2000
[Switch A-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[Switch A-acl-basic-2000] rule deny source any
```

Define two route policies, one is called Apply_med_50 and the other is called Apply_med_100. The first MED attribute with the route policy as network 1.0.0.0 is set as 50, while the MED attribute of the second is 100.

```
[Switch A] route-policy apply_med_50 permit node 10
[Switch A-route-policy] if-match acl 2000
[Switch A-route-policy] apply cost 50
[Switch A-route-policy] quit
[Switch A] route-policy apply_med_100 permit node 10
[Switch A-route-policy] if-match acl 2000
[Switch A-route-policy] apply cost 100
[Switch A-route-policy] quit
```

Apply route policy Apply_med_50 to egress route update of Switch C (193.1.1.2), and apply route policy Apply_med_100 on the egress route of Switch B (192.1.1.2)

```
[Switch A] bgp 100
[Switch A-bgp] peer ex193 route-policy apply_med_50 export
[Switch A-bgp] peer ex192 route-policy apply_med_100 export
```

2 Configure Switch B:

```
[Switch B] interface vlan-interface 2
[Switch B-Vlan-interface2] ip address 192.1.1.2 255.255.255.0
[Switch B] interface vlan-interface 4
```

```
[Switch B-Vlan-interface4] ip address 194.1.1.2 255.255.255.0
[Switch B] ospf
[Switch B-ospf-1] area 0
[Switch B-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[Switch B] bgp 200
[Switch B-bgp] group ex external
[Switch B-bgp] peer 192.1.1.1 group ex as-number 100
[Switch B-bgp] group in internal
[Switch B-bgp] peer 194.1.1.1 group in
[Switch B-bgp] peer 195.1.1.2 group in
```

3 Configure Switch C:

```
[Switch C] interface Vlan-interface 3
[Switch C-Vlan-interface3] ip address 193.1.1.2 255.255.255.0
[Switch C] interface vlan-interface 5
[Switch C-Vlan-interface5] ip address 195.1.1.2 255.255.255.0
[Switch C] ospf
[Switch C-ospf-1] area 0
[Switch C-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[Switch C-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[Switch C] bgp 200
[Switch C-bgp] group ex external
[Switch C-bgp] peer 193.1.1.1 group ex as-number 100
[Switch C-bgp] group in internal
[Switch C-bgp] peer 195.1.1.1 group in
[Switch C-bgp] peer 194.1.1.2 group in
```

4 Configure Switch D:

```
[Switch D] interface vlan-interface 4
[Switch D-Vlan-interface4] ip address 194.1.1.1 255.255.255.0
[Switch D] interface vlan-interface 5
[Switch D-Vlan-interface5] ip address 195.1.1.1 255.255.255.0
[Switch D] ospf
[Switch D-ospf-1] area 0
[Switch D-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[Switch D-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[Switch D-ospf-1-area-0.0.0.0] network 4.0.0.0 0.255.255.255
[Switch D] bgp 200
[Switch D-bgp] group ex external
[Switch D-bgp] peer ex as-number 200
[Switch D-bgp] peer 195.1.1.2 group ex
[Switch D-bgp] peer 194.1.1.2 group ex
```

To enable the configuration, all BGP neighbors will be reset using the **reset bgp all** command.

After above configuration, due to the fact that the MED attribute of route 1.0.0.0 discovered by Switch C is less than that of Switch B, Switch D will first select the route 1.0.0.0 from Switch C.

If the MED attribute of Switch A is not configured, the local preference on Switch C is configured as follows:

Configure the local preference attribute of Switch C

- Add ACL 2000 on Switch C and permit network 1.0.0.0

```
[Switch C] acl number 2000
[Switch C-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[Switch C-acl-basic-2000] rule deny source any
```

Define a route policy named Localpref, and set the local preference of routes matching ACL 2000 to 200, and that of routes not matching to 100.

```
[Switch C] route-policy localpref permit node 10
[Switch C-route-policy] if-match acl 2000
[Switch C-route-policy] apply local-preference 200
[Switch C-route-policy] route-policy localpref permit node 20
[Switch C-route-policy] apply local-preference 100
[Switch C-route-policy] quit
```

Apply this route policy to ingress traffic from BGP neighbor 193.1.1.1 (Switch A)

```
[Switch C] bgp 200
[Switch C-bgp] peer 193.1.1.1 route-policy localpref import
```

By then, due to the fact that the Local preference attribute value (200) of the route 1.0.0.0 learned by Switch C is higher than that of Switch B (Switch B is not configured with local Preference attribute, 100 by default), Switch D will also first select the route 1.0.0.0 from Switch C.

Troubleshooting BGP

Symptom 1: The neighborhood cannot be established (The Established state cannot be entered).

Solution: The establishment of BGP neighborhood needs the router able to establish TCP connection through port 179 and exchange Open packets correctly. Perform the check according to the following steps:

Check whether the configuration of the neighbor's AS number is correct.

Check whether the neighbor's IP address is correct.

If using the Loopback interface, check whether the connect-source loopback command has been configured. By default, the router uses the optimal local interface to establish the TCP connection, not using the loopback interface.

If it is the EBGP neighbor not directly connected, check whether the **peer ebgp-max-hop** command has been configured.

Use the **ping** command to check whether the TCP connection is normal. Since one router may have several interfaces able to reach the peer, the extended **ping -a ip-address** command should be used to specify the source IP address sending ping packet.

If the Ping operation fails, use the **display ip routing-table** command to check if there is available route in the routing table to the neighbor.

If the Ping operation succeeds, check if there is an ACL denying TCP port 179. If the ACL is configured, cancel the denying of port 179.

Symptom 2: BGP route cannot be advertised correctly after route of IGP is imported with the **network** command.

Solution: Route imported by the **network** command should be same as a route in the current routing table, which should include destination segment and mask. Route covering large network segment cannot be imported. For example, route 10.1.1.0/24 can be imported, while 10.0.0.0/8 may cause error. If Ospf is used, after a large network segment is imported to the local route by means of the **network** command, the router will automatically make changes according to the network segment actually used by the interface. Consequently, the **network** command will fail to, or incorrectly, import routes, which can cause routing errors when some network faults exist.

Introduction to IP Routing Policy

When a router advertises or receives routing information, it possibly needs to implement some policies to filter the routing information, so as to receive or advertise the routing information which can meet the specified condition only. A routing protocol, e.g. RIP, may need import the routing information discovered by other protocols to enrich its routing knowledge. While importing the routing information, it possibly only needs import the information meeting the conditions and set some special attributes to make them meet its requirement.

For implementing the routing policy, you need define a set of matching rules by specifying the characteristics of the routing information to be filtered. You can set the rules based on such attributes like destination address and source address of the information. The matching rules can be set in advance and then used in the routing policy to advertise, receive and import the route information.

Filter In Switch 8800 Family series, five kinds of filters, Route-policy, ACL, AS-path, Community-list, and IP-prefix, are provided to be called by the routing protocols. The following sections introduce these filters respectively.

ACL

The access control list (ACL) used by routing policy can be divided into the following types:

- Number-based basic ACLs
- Name-based basic ACLs
- Number-based advanced ACLs
- Name-based advanced ACLs
- Number-based L2 ACLs
- Name-based L2 ACLs

For routing information filtering, the basic ACL is generally used. When users define the ACL, they will define the range of an IP address or subnet to the destination network segment address or the next-hop address of the routing information. If an advanced ACL is used, perform the matching operation by the specified source address range.

IP-prefix

The function of the IP-prefix is similar to that of ACL, but it is more flexible and easy for the users to understand. When the IP-prefix is applied to the routing information filtering, its matching objects are the destination address information domain of the routing information.

An IP-prefix is identified by the IP-prefix name. Each IP-prefix can include multiple list items, and each list item can independently specify the match range of the network prefix forms and is identified with an index-number. The index-number designates the matching check sequence in the IP-prefix.

During the matching, the router checks list items identified by the sequence-number in the ascending order. Once a single list item meets the condition, it means that it has passed the IP-prefix filtering and will not enter the testing of the next list item.

AS-path

The AS-path list is only used in the BGP. The routing information packet of the BGP includes an autonomous system path domain (During the process of routing information exchanging of the BGP, the autonomous system paths the routing information has passed through will be recorded in this domain). Targeting at the AS path domain, the AS-path specifies the match condition.

Community-list

The community-list is only used in the BGP. The routing information packet of the BGP includes a community attribute domain to identify a community. Targeting at the community attribute, the community-list specifies the match condition.

Routing Policy Application

Two routing policy applications are as follows:

When advertising/receiving routing information, the router filters the information according to the route policy, and receives or advertises the routing information which can meet the specified condition only.

When importing other routes detected by other routing protocol, the router only imports the routing information, which can meet the specified condition only, according to the route policy.

Configuring IP Routing Policy

The routing policy configuration includes:

- 1 Filter configuration includes:
 - "Configuring a Route-policy"
 - "Configuring ip-prefix"
 - "Configuring the AS Path List"
 - "Configuring a Community Attribute List"



For the configuration of ACL, refer to the "QoS/ACL Operation" part of this manual.

- 2 Applications of routing policies include:
 - "Applying Route Policy on Imported Routes"
 - "Applying Route Policy on Received or Advertised Routes"

Configuring a Route-policy

A route-policy can comprise multiple nodes. Each node is a unit for matching operation. The nodes will be tested against by *node-number*.

Each node consists of a group of **if-match** clauses and **apply** clauses.

The **if-match** clauses define the matching rules. The different **if-match** clauses for a node have the relationship of "AND". That is, the route must satisfy all the **if-match** clauses for the node to match the node before passing this node.

The **apply** clauses define the executed action after the routing information passes the matching test. That is, the clause sets the routing information attribute.

Defining a route-policy

Perform the following configuration in system view.

Table 393 Define a route-policy

Operation	Command
Enter Route policy view	route-policy <i>route-policy-name</i> { permit deny } node <i>node-number</i>
Remove the specified route-policy	undo route-policy <i>route-policy-name</i> [permit deny node <i>node-number</i>]

The **permit** keyword specifies the matching mode for a defined node in the route-policy to be in permit mode. If a route satisfies all the **if-match** clauses of the node, it will pass the filtering of the node, and the **apply** clauses for the node will be executed without taking the test of the next node. If not, however, the route should take the test of the next node.

The **deny** keyword specifies the matching mode for a defined node in the route-policy to be in deny mode. In this mode, the **apply** clauses will not be executed. If a route satisfies all the **if-match** clauses of the node, it will be denied by the node and will not take the test of the next node. If not, however, the route will take the test of the next node.

The nodes have the "OR" relationship. In other words, the router will test the route against the nodes in the route-policy in sequence. Once a node is matched, the route-policy filtering will be passed.

By default, the route-policy is not defined.



If multiple nodes are defined in a route-policy, at least one of them should be in permit mode. Apply the route-policy to filter routing information. If the routing information does not match any node, the routing information will be denied by the route-policy. If all the nodes in the route-policy are in deny mode, all routing information will be denied by the route-policy.

Defining if-match clauses for a route-policy

The **if-match** clauses define the matching rules. That is, the filtering conditions that the routing information should satisfy for passing the route-policy. The matching objects are some attributes of routing information.

Perform the following configuration in route policy view.

Table 394 Define if-match conditions

Operation	Command
Match the AS path domain of the BGP routing information	if-match as-path <i>acl-number</i>
Disable matching the AS path domain of the BGP routing information	undo if-match as-path
Match the community attribute of the BGP routing information	if-match community { <i>basic-community-number</i> [whole-match] <i>adv-community-number</i> }
Disable matching the community attribute of the BGP routing information	undo if-match community
Match the destination address of the routing information	if-match { acl <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> }
Disable matching the destination address of the routing information	undo if-match { acl ip-prefix }
Match the next-hop interface of the routing information	if-match interface <i>interface-type interface-number</i>
Disable matching the next-hop interface of the routing information	undo if-match interface
Match the next-hop of the routing information	if-match ip next-hop { acl <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> }
Disable matching the next-hop of the routing information set by ACL	undo if-match ip next-hop
Disable matching the next-hop of the routing information set by address prefix list	undo if-match ip next-hop ip-prefix
Match the routing cost of the routing information	if-match cost <i>value</i>
Disable matching the routing cost of the routing information	undo if-match cost
Match the tag domain of the OSPF routing information	if-match tag <i>value</i>
Cancel the tag domain of the matched OSPF routing information	undo if-match tag



For the details about the **if-match mpls-label** and **if-match vpn-target** commands, refer to the 08-MPLS command module in the 3Com Switch 8800 Family Series Routing Switches Command Manual.

By default, no matching will be performed.

Note the following:

The **if-match** clauses for a node in the route-policy have the relationship of "AND" for matching. That is, the route must satisfy all the clauses to match the node before the actions specified by the **apply** clauses can be executed.

If no **if-match** clauses are specified, all the routes will pass the filtering on the node.

Defining apply clauses for a route-policy

The **apply** clauses specify actions, which are the configuration commands executed after a route satisfies the filtering conditions specified by the **if-match** clauses. Thereby, some attributes of the route can be modified.

Perform the following configuration in route policy view.

Table 395 Define apply clauses

Operation	Command
Add the specified AS number before the AS-path series of the BGP routing information	apply as-path <i>as-number-1</i> [<i>as-number-2</i> [<i>as-number-3</i> ...]]
Cancel the specified AS number added before the AS-path series of the BGP routing information	undo apply as-path
Set the community attribute in the BGP routing information	apply community [<i>aa:nn</i>]* [[no-export-subconfed no-export no-advertise] * [additive] additive none]
Cancel the set community attribute in the BGP routing information	undo apply community
Set the next-hop address of the routing information	apply ip next-hop <i>ip-address</i>
Cancel the next-hop address of the routing information	undo apply ip next-hop
Specifies to import routes to IS-IS Level-1, Level-2 or Level-1-2	apply isis [level-1 level-2 level-1-2]
Cancel the IS-IS level setting for route import	undo apply isis
Set the local preference of the BGP routing information	apply local-preference <i>local-preference-value</i>
Cancel the local preference of the BGP routing information	undo apply local-preference
Set the routing cost of the routing information	apply cost <i>value</i>
Cancel the routing cost of the routing information	undo apply cost
Set the cost type of the routing information	apply cost-type [internal external]
Remove the setting of the cost type	undo apply cost-type
Set the route origin of the BGP routing information	apply origin { igp egp <i>as-number</i> incomplete }
Cancel the route origin of the BGP routing information	undo apply origin
Set the tag domain of the OSPF routing information	apply tag <i>value</i>
Cancel the tag domain of the OSPF routing information	undo apply tag



For the details about the **apply mpls-label** command, refer to the 08-MPLS command module in the 3Com Switch 8800 Family Series Routing Switches Command Manual.

By default, perform no settings.

Note that if the routing information meets the match conditions specified in the route-policy and also notifies the MED value configured with the **apply cost-type internal** when notifying the IGP route to the EBGp peers, then this value will be regarded as the MED value of the IGP route. The preference configured with the **apply cost-type internal** command is lower than that configured with the **apply cost** command, but higher than that configured with the **default med** command.

Configuring ip-prefix

An IP-prefix-list is identified by an ip-prefix-name. Each IP-prefix-list can include multiple entries each specifying an IP prefix matching range. IP prefix entries are identified by index-numbers. The order in which IP prefix entries are matched against depends on the order of their index numbers.

Perform the following configuration in system view.

Table 396 Define prefix-list

Operation	Command
Define prefix-list	ip ip-prefix <i>ip-prefix-name</i> [index <i>index-number</i>] { permit deny } <i>network len</i> [greater-equal <i>greater-equal</i>] [less-equal <i>less-equal</i>]
Remove prefix-list	undo ip ip-prefix <i>ip-prefix-name</i> [index <i>index-number</i>] { permit deny }

During the matching, the router checks list items identified by the *index-number* in the ascending order. If only one list item meets the condition, it means that it has passed the IP-prefix filtering (will not enter the testing of the next list item).

Note that if more than one ip-prefix item are defined, then the match mode of at least one list item should be the **permit** mode. The list items of the **deny** mode can be defined first to rapidly filter the routing information not satisfying the requirement, but if all the items are in the **deny** mode, no route will pass the ip-prefix filtering. You can define an item of **permit 0.0.0.0/0 greater-equal 0 less-equal 32** after the multiple list items in the **deny** mode so as to let all the other routes pass.

Configuring the AS Path List

The routing information packet of the BGP includes an autonomous system path domain. The as path-list can be used to match with the autonomous system path domain of the BGP routing information so as to filter the routing information, which does not conform to the requirements.

Perform the following configuration in the system view:

Table 397 Define the AS path list

Operation	Command
Define the AS path list	ip as-path-acl <i>acl-number</i> { permit deny } <i>as-regular-expression</i>
Delete the specified AS path list	undo ip as-path-acl <i>acl-number</i>

By default, no AS path list is defined.

Configuring a Community Attribute List

In BGP, community attribute is optional and transitive. Some community attributes known globally are called standard community attributes. Some community attributes are for special purpose. You can also define expanded community attribute.

A route can have one more community attributes. The speakers of multiple community attributes of a route can act according to one, several or all attributes. A router can select community attribute modification before transmitting routes to other peers.

Community lists, which identify community information, can be divided into basic-community-lists and advanced-community-lists. Basic-community-lists range from 1 to 99, while advanced-community-lists range from 100 to 199.

Perform the following configuration in system view.

Table 398 Configure a community attribute list

Operation	Command
Configure a basic community-list	ip community-list <i>basic-comm-list-number</i> { permit deny } [<i>aa:nn</i>]* [internet no-export-subconfed no-advertise no-export]*
Configure an advanced community-list	ip community-list <i>adv-comm-list-number</i> { permit deny } <i>comm-regular-expression</i>
Cancel a community-list	undo ip community-list { <i>basic-comm-list-number</i> <i>adv-comm-list-number</i> }

By default, a BGP community attribute list is not configured.

Applying Route Policy on Imported Routes

A routing protocol can import the routes discovered by other routing protocols to enrich its route information. The route-policy can be used for route information filtering to implement the purposeful redistribution. If the destination routing protocol importing the routes cannot directly reference the route costs of the source routing protocol, you should satisfy the requirement of the protocol by specifying a route cost for the imported route.

Perform the following configuration in routing protocol view.

Table 399 Configure to import the routes of other protocols

Operation	Command
Set to import routes of other protocols	import-route <i>protocol</i> [med <i>med</i> cost <i>cost</i>] [tag <i>value</i>] [type 1 2] [route-policy <i>route-policy-name</i>]
Cancel the setting for importing routes of other protocols	undo import-route <i>protocol</i>

By default, the routes discovered by other protocols will not be advertised.



*In different routing protocol views, the parameter options are different. For details, respectively refer to the **import-route** command in different protocols.*

Applying Route Policy on Received or Advertised Routes

Configuring to filter the received routes

Perform the following configuration in routing protocol view.

Define a policy to filter the routing information not satisfying the conditions while receiving routes with the help of an ACL or address prefix-list. **gateway** specifies that only the update packets from a particular neighboring router will be received.

Table 400 Configure to filter the received routes

Operation	Command
Configure to filter the received routing information advertised by the specified address	filter-policy gateway <i>ip-prefix-name</i> import
Cancel the filtering of the received routing information advertised by the specified address	undo filter-policy gateway <i>ip-prefix-name</i> import
Configure to filter the received global routing information	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> [gateway <i>ip-prefix-name</i>] } import
Cancel the filtering of the received global routing information	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> [gateway <i>ip-prefix-name</i>] } import

Configuring to filter the advertised routes

You may define a route advertisement policy to filter advertised routing information. This can be done by referencing an ACL or IP prefix-list to filter routing information that does not meet the conditions, or by specifying a protocol to filter routing information of that protocol only.

Perform the following configuration in routing protocol view.

Table 401 Configure to filter the advertised routes

Operation	Command
Configure to filter the routes advertised by the protocol	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>routing-protocol</i>]
Cancel the filtering of the routes advertised by the protocol	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>routing-protocol</i>]

By far, the route policy supports importing the routes discovered by the following protocols into the routing table:

direct: The hop (or host) to which the local interface is directly connected.

static: Route configured statically

rip: Route discovered by RIP

ospf: Route discovered by OSPF

ospf-ase: External route discovered by OSPF

ospf-nssa: NSSA route discovered by OSPF

isis: Route discovered by IS-IS

bgp: Route acquired by BGP

By default, the filtering of the received and advertised routes will not be performed.

Displaying and Debugging the Routing Policy

After the above configuration, execute the **display** command in any view to display the running of the routing policy configuration, and to verify the effect of the configuration.

Table 402 Display and debug the route policy

Operation	Command
Display the routing policy	display route-policy [<i>route-policy-name</i>]
Display the path information of the AS filter in BGP	display ip as-path-acl [<i>acl-number</i>]
Display the address prefix list information	display ip ip-prefix [<i>ip-prefix-name</i>]

Typical IP Routing Policy Configuration Example

Configuring to Filter the Received Routing Information

Network requirements

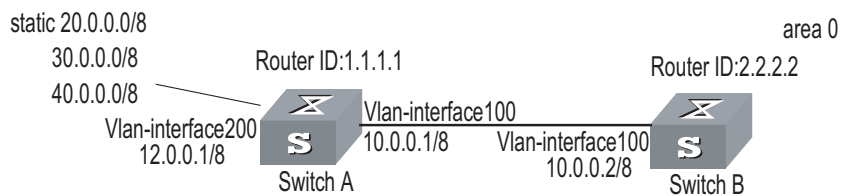
Switch A communicates with Switch B, running OSPF protocol. The router ID of Switch A is 1.1.1.1, and that of Switch B is 2.2.2.2.

Import three static routes through enabling the OSPF protocol on the Switch A.

The route filtering rules can be configured on Switch B to make the received three static routes partially visible and partially shielded. It means that routes in the network segments 20.0.0.0 and 40.0.0.0 are visible while those in the network segment 30.0.0.0 are shielded.

Network diagram

Figure 95 Network diagram for filtering the received routing information



Configuration procedure

1 Configure Switch A:

Configure the IP address of VLAN interface.

```
[Switch A] interface vlan-interface 100
[Switch A-Vlan-interface100] ip address 10.0.0.1 255.0.0.0
[Switch A] interface vlan-interface 200
[Switch A-Vlan-interface200] ip address 12.0.0.1 255.0.0.0
```

Configure three static routes.

```
[Switch A] ip route-static 20.0.0.1 255.0.0.0 12.0.0.2
[Switch A] ip route-static 30.0.0.1 255.0.0.0 12.0.0.2
[Switch A] ip route-static 40.0.0.1 255.0.0.0 12.0.0.2
```

Enable the OSPF protocol and specifies the number of the area to which the interface belongs.

```
[Switch A] router id 1.1.1.1
[Switch A] ospf
[Switch A-ospf-1] area 0
[Switch A-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
```

Import the static routes

```
[Switch A-ospf-1] import-route static
```

2 Configure Switch B:

Configure the IP address of VLAN interface.

```
[Switch B] interface vlan-interface 100
[Switch B-Vlan-interface100] ip address 10.0.0.2 255.0.0.0
```

Configure the access control list.

```
[Switch B] acl number 2000
[Switch B-acl-basic-2000] rule deny source 30.0.0.0 0.255.255.255
[Switch B-acl-basic-2000] rule permit source any
```

Enable OSPF protocol and specifies the number of the area to which the interface belongs.

```
[Switch B] router id 2.2.2.2
[Switch B] ospf
[Switch B-ospf-1] area 0
[Switch B-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
```

Configure OSPF to filter the external routes received.

```
[Switch B-ospf-1] filter-policy 2000 import
```

Troubleshooting Routing Policy

Symptom 1: Routing information filtering cannot be implemented in normal operation of the routing protocol

Solution: Check for the following faults:

The if-match mode of at least one node of the Route-policy should be the **permit** mode. When a Route-policy is used for the routing information filtering, if a piece of routing information does not pass the filtering of any node, then it means that the route information does not pass the filtering of the Route-policy. When all the nodes of the Route-policy are in the **deny** mode, then all the routing information cannot pass the filtering of the Route-policy.

The if-match mode of at least one list item of the ip-prefix should be the permit mode. The list items of the deny mode can be defined first to rapidly filter the routing information not satisfying the requirement, but if all the items are in the deny mode, any routes will not pass the ip-prefix filtering. You can define an item of permit 0.0.0.0/0 less-equal 32 after the multiple list items in the deny mode so as to let all the other routes pass the filtering (If less-equal 32 is not specified, only the default route will be matched).

35

ROUTE CAPACITY CONFIGURATION

Route Capacity Configuration

Introduction to Route Capacity

In an actual network application, a routing table may contain a large quantity of route entries (especially OSPF routes and BGP routes). Generally, the routing information is stored in the memory of the switch and the total size of the switch memory will not change. When the size of the routing table increases to some degree, it may affect the operation of the system. To avoid the occurring of this case, you can set the specifications of routing tables and VRFs (VPN routing and forwarding instances) in the current system; and the system will inhibit any card that below any of the settings from working.

Configuration Tasks

Table 403 Configuration tasks

Items	Description	Details
Set the maximum number of route entries supported by the system	Required	Refer to section "Setting the Maximum Number of Route Entries Supported by the System".
Set the maximum number of VRFs supported by the system	Required	Refer to section "Setting the Maximum Number of VRFs Supported by the System".

Setting the Maximum Number of Route Entries Supported by the System

Table 404 Set the maximum number of route entries supported by the system

Operation	Command	Description
Enter system view	system-view	-
Set the maximum number of route entries supported by the system	router route-limit { 128K 256K 512K }	Required. By default, the system supports up to 128 K routing entries.

Setting the Maximum Number of VRFs Supported by the System

Table 405 Set the maximum number of VRFs supported by the system

Operation	Command	Description
Enter system view	system-view	-
Set the maximum number of VRFs supported by the system	route vrf-limit { 256 512 1024 }	Required. By default, the system supports up to 256 VRFs.

36

RECURSIVE ROUTING CONFIGURATION

Recursive Routing Configuration

Recursive Routing Overview

Every route entry must have its next hop address. For a common route, its next hop address is within the network segment to which the router is directly connected; for a route requiring recursion, its next hop address is not within the network segment to which the router is directly connected. During route forwarding, this non-directly connected next hop address must be recursion-processed once or several times to find out a directly connected next hop address to enable L2 path searching. A recursive route can be a static route or BGP route. Recursive routing can make route entries flexible, independent of a specific interface.

Configuring Recursive Routing

Table 406 Configure recursive routing

Operation	Command	Description
Enter system view	System-view	-
Enable recursive routing	route-rely [bgp static]	By default, both routes learned by the BGP and static routes support recursive routing.



An Ethernet switch functions as a router when it runs IP multicast protocol. A router that is referred to in the following represents a generalized router or a layer 3 Ethernet switch running IP multicast protocol.

IP Multicast Overview

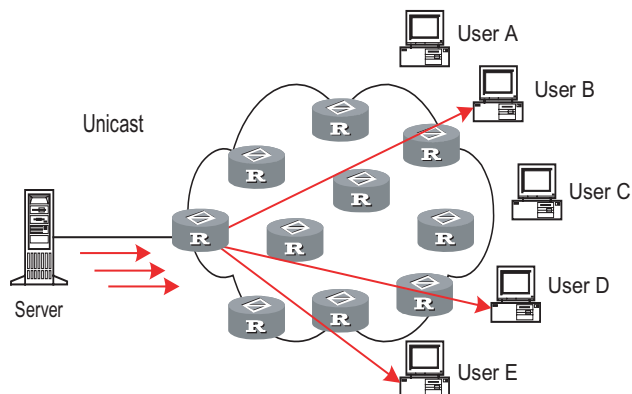
Problems with Unicast/Broadcast

The constant development of the Internet and increasing interaction of versatile data, voice and video information over the network, has promoted the emergence of new services like e-commerce, network conference, online auction, video on demand (VoD), and tele-education. These services require higher information security and greater rewards.

Data transmission in unicast mode

In unicast mode, every user that needs the information receives a copy through the channels the system separately establishes for them. See Figure 96.

Figure 96 Data transmission in unicast mode

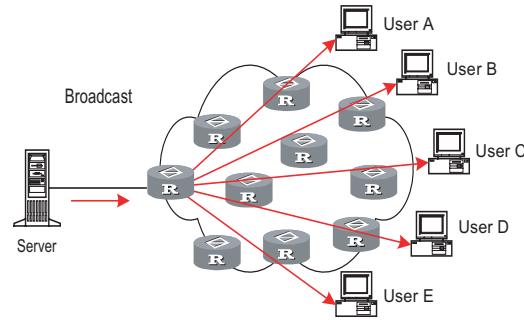


Suppose that Users B, D, and E need the information, the information source Server establishes transmission channels with every of them. Since the traffic in transmission increases with the number of users, excessive copies of the information would spread over the network if there is a large number of users in need of this information. As the bandwidth would turn short, the unicast mode is incapable of massive transmission.

Data transmission in broadcast mode

In broadcast mode, every user on the network receives the information regardless of their needs. See Figure 97 "Data transmission in broadcast mode".

Figure 97 Data transmission in broadcast mode



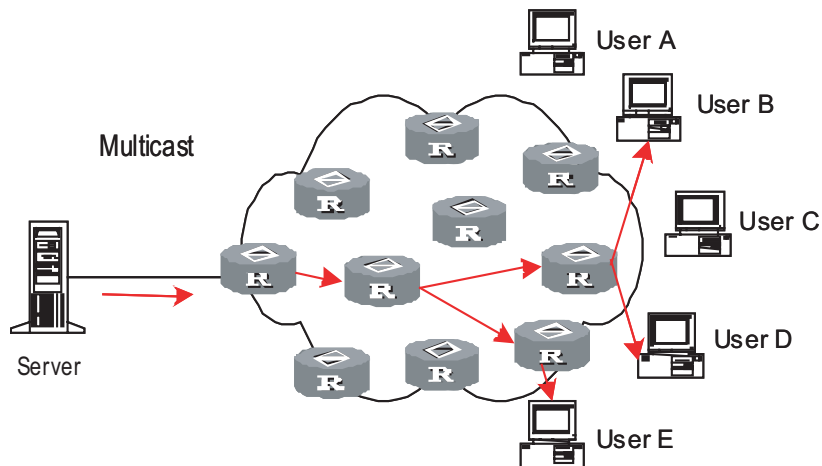
Suppose the Users B, D, and E need the information, the information source Server broadcasts the information through the router; User A and User C can also receive the information. In that case, information security and rewards to services are not guaranteed. Moreover, bandwidth is terribly wasted when only a few part of users are in need of the information.

In short, the unicast mode is useful in networks with scattered users, and the multicast mode is suitable for networks with dense users. When the number of users is uncertain, the adoption of unicast or multicast mode results in low efficiency.

Advantages of Multicast Multicast

IP multicast technology solves those problems. When some users in the network need specific information, it allows the multicast source to send the information only once. With the tree route established by the multicast routing protocol, the information will not be duplicated or distributed until it reaches the bifurcation point as far as possible. See Figure 98 “Data transmission in multicast mode”.

Figure 98 Data transmission in multicast mode



Suppose the Users B, D, and E need the information, they need to be organized into a receiver group to ensure that the information can reach them smoothly. The routers on the network duplicate and forward the information according to the

distribution of these users in the group. Finally, the information is transmitted to the intended receivers B,D and E properly and correctly.

In multicast mode, the information sender is called the "multicast source", the receiver is called the "multicast group", and the routers for multicast information transmission are called "multicast routers". Members of a multicast group can scatter around the network; the multicast group therefore has no geographical limitation. It should be noted that a multicast source does not necessarily belong to a multicast group. It sends data to multicast groups but is not necessarily a receiver. Multiple sources can send packets to a multicast group simultaneously.

Advantages

The main advantages of multicast are:

- Enhanced efficiency: It reduces network traffic and relieves server and CPU of loads.
- Optimized performance: It eliminates traffic redundancy.
- Distributed application: It enables multipoint application.

Application of Multicast

IP multicast technology effectively implements point to multi-point forwarding with high speed, as saves network bandwidth a lot and can relieve network loads. It facilitates also the development of new value-added services in the Internet information service area that include online live show, Web TV, tele-education, telemedicine, network radio station and real-time audio/video conferencing. It takes a positive role in:

- Multimedia and streaming media application
- Occasional communication for training and cooperation
- Data storage and finance (stock) operation
- Point-to-multipoint data distribution

With the increasing popularity of multimedia services over IP network, multicast is gaining its marketplace. In addition, the multicast service becomes popular and prevalent gradually.

Implementation of IP Multicast

IP Multicast Addresses

In multicast mode, there are questions about where to send the information, how to locate the destination or know the receiver. All these questions can be narrowed down to multicast addressing. To guarantee the communication between a multicast source and a multicast group (that is, a group of receivers), the network layer multicast address (namely the IP multicast address) is required, along with the technique to correlate it with the link layer MAC multicast address. Following is the introduction to these two kinds of addresses.

IP Multicast Addresses

According to the definition in Internet Assigned Number Authority (IANA), IP addresses fall into four types: Class A, Class B, Class C and Class D. Unicast packets use IP addresses of Class A, Class B or Class C, depending on specific

packet scales. Multicast packets use IP addresses of Class D as their destination addresses, but Class D IP addresses cannot be contained in the source IP field of IP packets.

During unicast data transmission, a packet is transmitted "hop-by-hop" from the source address to the destination address. However, in IP multicast environment, a packet has more than one destination address, or a group of addresses. All the information receivers are added to a group. Once a receiver joins the group, the data for this group address starts flowing to this receiver. All members in the group can receive the packets. This group is a multicast group.

Membership here is dynamic, and a host can join or leave the group at any time. A multicast group can be permanent or temporary. Some multicast group addresses are allocated by IANA, and the multicast group is called permanent multicast group. The IP addresses of a permanent multicast group are unchangeable, but its membership is changeable, and the number of members is arbitrary. It is quite possible for a permanent group to not a single member. Those not reserved for permanent multicast groups can be used by temporary multicast groups. Class D multicast addresses range from 224.0.0.0 to 239.255.255.255. More information is listed in Table 407 "Ranges and meanings of Class D addresses".

Table 407 Ranges and meanings of Class D addresses

Class D address range	Description
224.0.0.0~224.0.0.255	Reserved multicast addresses (addresses of permanent groups). All but 224.0.0.0 can be allocated by routing protocols.
224.0.1.0~238.255.255.255	Multicast addresses available for users (addresses of temporary groups). They are valid in the entire network.
239.0.0.0~239.255.255.255	Administratively scoped multicast addresses. They are valid only in the specified local range.

Reserved multicast addresses that are commonly used are described in the following table.

Table 408 Reserved multicast address list

Class D address range	Description
224.0.0.0	Base Address (Reserved)
224.0.0.1	Addresses of all hosts
224.0.0.2	Addresses of all multicast routers
224.0.0.3	Unassigned
224.0.0.4	DVMRP routers
224.0.0.5	OSPF routers
224.0.0.6	OSPF DR
224.0.0.7	ST routers
224.0.0.8	ST hosts
224.0.0.9	RIP-2 routers
224.0.0.10	IGRP routers
224.0.0.11	Mobile agents
224.0.0.12	DHCP server/Relay agent

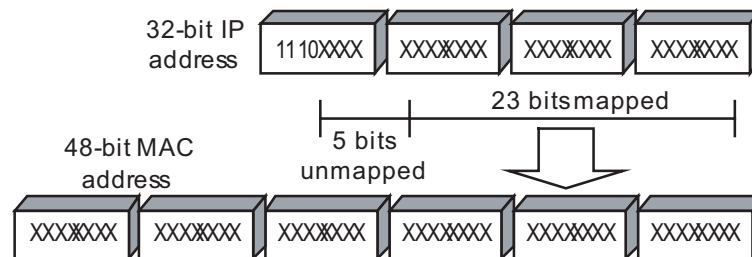
Table 408 Reserved multicast address list

Class D address range	Description
224.0.0.13	All PIM routers
224.0.0.14	RSVP encapsulation
224.0.0.15	All CBT routers
224.0.0.16	Specified SBM
224.0.0.17	All SBMS
224.0.0.18	VRRP
.....

Ethernet Multicast MAC Addresses

When a unicast IP packet is transmitted on the Ethernet, the destination MAC address is the MAC address of the receiver. However, for a multicast packet, the destination is no longer a specific receiver but a group with unspecific members. Therefore, the multicast MAC address should be used.

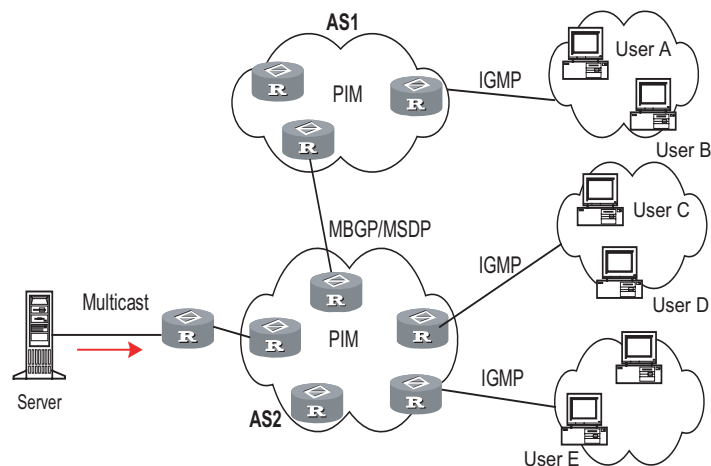
As Internet Assigned Number Authority (IANA) provisions, the high 24 bits of a multicast MAC address are 0x01005e and the low 23 bits of a MAC address are the low 23 bits of a multicast IP address. The high twenty-fifth bit is 0, a fixed value.

Figure 99 Mapping between a multicast IP address and an Ethernet MAC address

The first four bits of the multicast address are 1110, representing the multicast identifier. Among the rest 28 bits, only 23 bits are mapped to the MAC address, and the other five bits are lost. This may result in that 32 IP addresses are mapped to the same MAC address.

IP Multicast Protocols

IP multicast protocols mainly involve multicast group management protocols and multicast routing protocols. Their application positions are shown in Figure 100 "Application positions of multicast-related protocols".

Figure 100 Application positions of multicast-related protocols

Multicast group management protocol

Multicast groups use Internet group management protocol (IGMP) as the management protocols. IGMP runs between the host and multicast router and defines the membership establishment and maintenance mechanism between them.

Multicast routing protocols

A multicast routing protocol runs between multicast routers to create and maintain multicast routes for correct and efficient forwarding of multicast packet. The multicast routing creates a loop-free data transmission path from one source to multiple receivers. The task of multicast routing protocols is to build up the distribution tree architecture. A multicast router can use multiple methods to build up a path for data transmission, that is, a distribution tree.

As in unicast routing, the multicast routing can also be intra-domain or inter-domain. Intra-domain multicast routing is rather mature and protocol independent multicast (PIM) is the most widely used intra-domain protocol, which can work in collaboration with unicast routing protocols. The inter-domain routing first needs to solve how to transfer routing information between ASs. Since the ASs may belong to different telecom carriers, the inter-domain routing information must contain carriers' policies, in addition to distance information. Currently, inter-domain routing protocols include multicast source discovery protocol (MSDP) and MBGP multicast extension.

RPF Mechanism for IP Multicast Packets

To ensure that multicast packets reach a router along the shortest path, the multicast router must check the receiving interface of multicast packets depending on the unicast routing table or a unicast routing table independently provided for multicast. This check mechanism is the basis for most multicast routing protocols to perform multicast forwarding, and is known as Reverse Path Forwarding (RPF) check. A multicast router uses the source address of a received multicast packet to query the unicast routing table or the independent multicast routing table to determine that the receiving interface is on the shortest path from the receiving station to the source. If a source tree is used, the source address is the address of the source host sending the multicast packet. If a shared tree is used, the source

address is the RP address of the shared tree. A multicast packet arriving at the router will be forwarded according to the multicast forwarding entry if it passes the RPF check, or else, it will be discarded.

38

STATIC MULTICAST MAC ADDRESS CONFIGURATION

Static Multicast MAC Address Overview

The concept of "static multicast MAC address" is proposed to fulfill the feature of static Layer 2 multicast. When some network users need some specific information, the multicast information sender (the multicast source) sends the information only once, and the multicast packets are sent to the specified port with the help of the configured static multicast MAC address.

Configuring a Static Multicast MAC Address

Configuration Prerequisites

- The port to be configured and the VLAN both exist;
- The port to be configured is within the specified VLAN.

Configuring a Static Multicast MAC Address

Table 409 Configure a static multicast MAC address

Operation	Command	Remarks
Enter system view	system-view	-
Configure the Static Multicast MAC	mac-address multicast <i>mac-addr interface</i> { { <i>interface-type</i> <i>interface-number</i> } [to { <i>interface-type</i> <i>interface-number</i> }] } &<1-10> vlan <i>vlan-id</i>	Required This command adds the specified port to the static multicast MAC group.



CAUTION:

- Do not enable the PIM on the virtual interface of the VLAN to be configured.
- The multicast MAC address to be configured must not be a multicast MAC address used by a known protocol.
- The port to be configured must be an Ethernet port.
- The port to be configured must not be aggregate port.
- If the MAC address to be configured already exists, the specified port will be added to the existing MAC group. This does not affect other ports existing in the group.

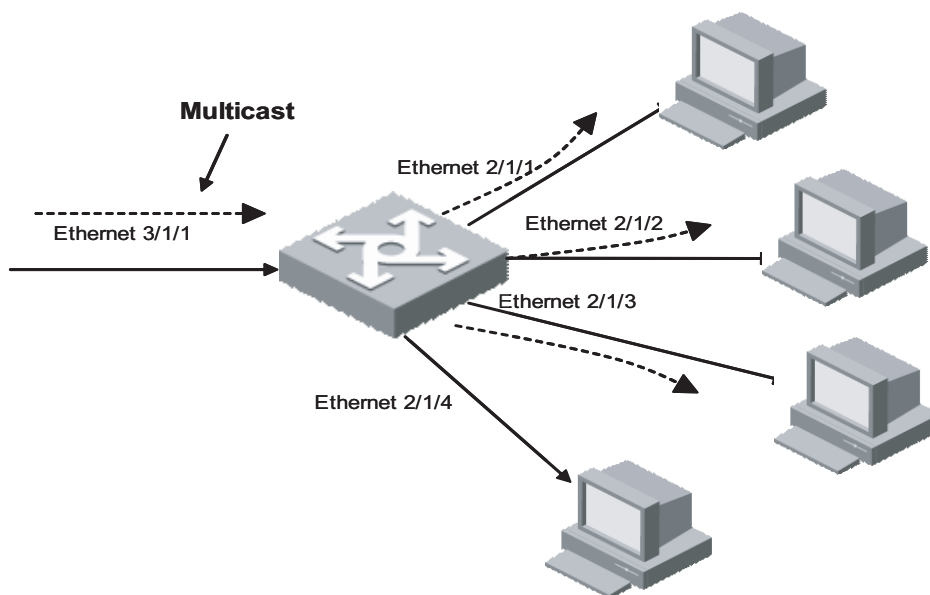
Static Multicast MAC Address Configuration Example

Network requirements

- Data packets with the destination MAC 0100-5e01-018d in VLAN 2 are to be sent to three specified ports, Ethernet 2/1/1, Ethernet 2/1/2, and Ethernet 2/1/3.

Network diagram

Figure 101 Network diagram for static multicast MAC address configuration



Configuration procedure

Enter system view

```
<SW8800> system-view
```

Add a static multicast MAC address group, and add multiple ports into the static multicast address group

```
[SW8800] mac-address multicast 0100-5e01-018d interface Ethernet 2/1/1 to Ethernet 2/1/3 vlan 2
```

Displaying and Maintaining Static Multicast MAC Address Configuration

Execute the **display** command in any view to display the user-configured multicast MAC address.

Table 410 Display a static multicast MAC address

Operation	Command
Display static multicast MAC address	display mac-address multicast static [[<i>mac-addr</i>] vlan <i>vlan-id</i>]

39

IGMP SNOOPING CONFIGURATION

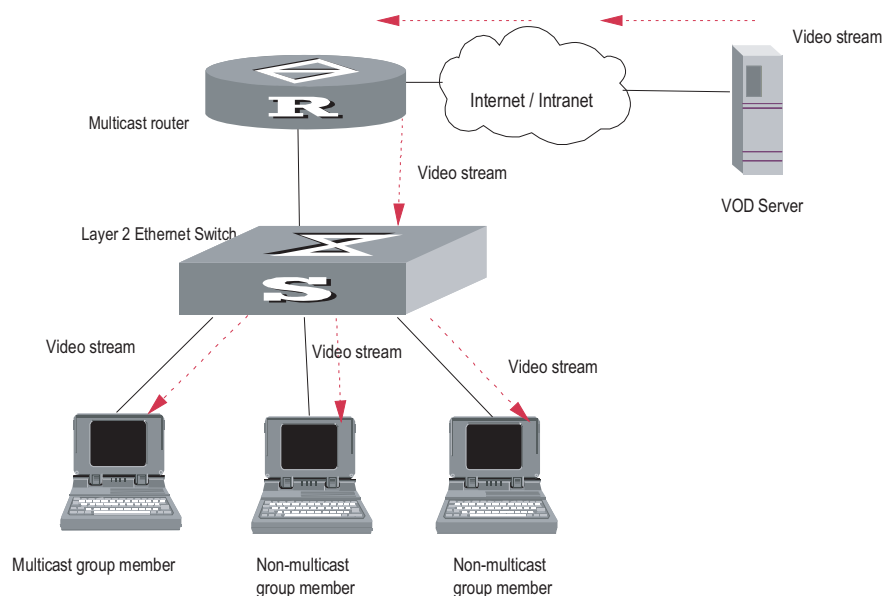
IGMP Snooping Overview

IGMP Snooping Principle Running on the link layer, IGMP Snooping is a multicast control mechanism on the Layer 2 Ethernet switch and it is used for multicast group management and control.

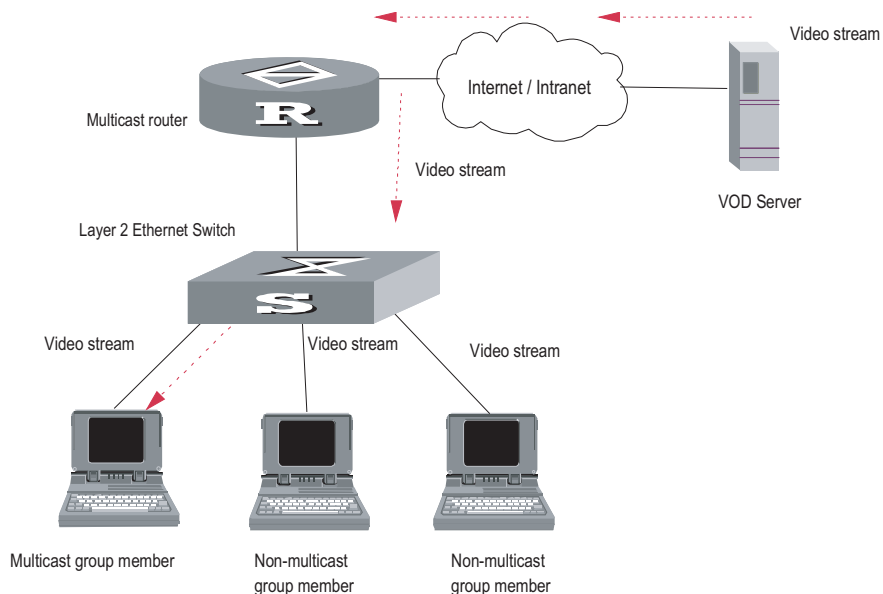
When receiving the IGMP messages transmitted between the host and router, the Layer 2 Ethernet switch uses IGMP Snooping to analyze the information carried in the IGMP messages. If the switch hears IGMP host report message from an IGMP host, it will add the host to the corresponding multicast table. If the switch hears IGMP leave message from an IGMP host, it will remove the host from the corresponding multicast table. The switch continuously listens to the IGMP messages to create and maintain MAC multicast address table on Layer 2. And then it can forward the multicast packets transmitted from the upstream router according to the MAC multicast address table.

When IGMP Snooping is disabled, the packets are broadcasted on Layer 2. See the following figure:

Figure 102 Multicast packet transmission without IGMP Snooping



When IGMP Snooping runs, the packets are multicast rather than broadcasted on Layer 2. See the following figure:

Figure 103 Multicast packet transmission when IGMP Snooping runs

Implementing IGMP Snooping

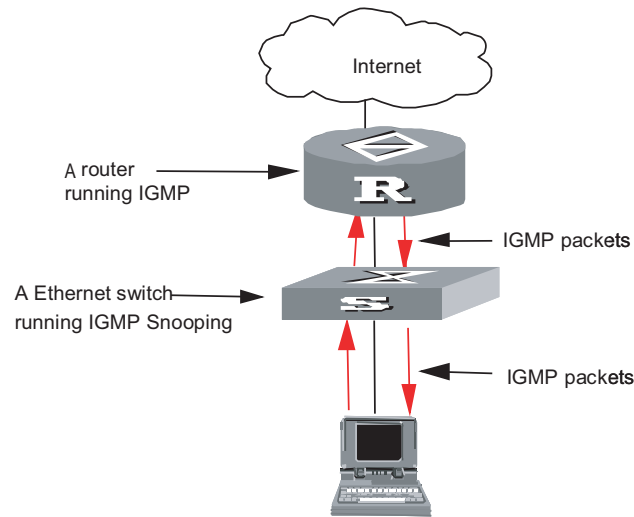
Related concepts of IGMP Snooping

To facilitate the description, this section first introduces some related switch concepts of IGMP Snooping.

- Router Port: The port of the switch, directly connected to the multicast router.
- Multicast member port: The Ethernet switch port connected to the multicast member. The multicast member refers to a host joined a multicast group.
- MAC multicast group: The multicast group is identified with MAC multicast address and maintained by the Ethernet switch.
- Router port aging time: Time set on the router port aging timer. If the switch has not received any IGMP general query message when the timer times out, it considers the port no longer as a router port.
- Multicast group member port aging time: When a port joins an IP multicast group, the aging timer of the port will begin timing. The multicast group member port aging time is set on this aging timer. If the switch has not received any IGMP report message when the timer times out, it transmits IGMP specific query message to the port.
- Maximum response time: When the switch transmits IGMP specific query message to the multicast member port, the Ethernet switch starts a response timer, which times before the response to the query. If the switch has not received any IGMP report message before the timer times out, it will remove the port from the multicast member ports

Implementing Layer 2 multicast with IGMP Snooping

The Ethernet switch runs IGMP Snooping to listen to the IGMP messages and map the host and its ports to the corresponding multicast group address. To implement IGMP Snooping, the Layer 2 Ethernet switch processes different IGMP messages in the way illustrated in the figure below:

Figure 104 Implement IGMP Snooping

- IGMP general query message: Transmitted by the multicast router to the multicast group members to query which multicast group contains member. When an IGMP general query message arrives at a router port, the Ethernet switch will reset the aging timer of the port. When a port other than a router port receives the IGMP general query message, the Ethernet switch will start the aging timer for the port.
- IGMP specific query message: Transmitted from the multicast router to the multicast members and used for querying if a specific group contains any member. When received IGMP specific query message, the switch only transmits the specific query message to the IP multicast group which is queried.
- IGMP report message: Transmitted from the host to the multicast router and used for applying for joining a multicast group or responding to the IGMP query message. When received the IGMP report message, the switch checks if the MAC multicast group, corresponding to the IP multicast group the packet is ready to join exists.

If the corresponding MAC multicast group does not exist, the switch only notifies the router that a member is ready to join a multicast group, creates a new MAC multicast group, adds the port received the message to the group, starts the port aging timer, and then adds all the router ports in the native VLAN of the port into the MAC multicast forwarding table, and meanwhile creates an IP multicast group and adds the port received the report message to it.

If the corresponding MAC multicast group exists but does not contains the port received the report message, the switch adds the port into the multicast group and starts the port aging timer. And then the switch checks if the corresponding IP multicast group exists.

If it does not exist, the switch creates a new IP multicast group and adds the port received the report message to it. If it exists, the switch adds the port to it.

If the MAC multicast group corresponding to the message exists and contains the port received the message, the switch will only reset the aging timer of the port.

- IGMP leave message: Transmitted from the multicast group member to the multicast router to notify that a host left the multicast group. When received a leave message of an IP multicast group, the Ethernet switch transmits the specific query message concerning that group to the port received the message, in order to check if the host still has some other member of this group and meanwhile starts a maximum response timer. If the switch has not receive any report message from the multicast group after the timer expires, the port will be removed from the corresponding MAC multicast group. If the MAC multicast group does not have any member, the switch will notify the multicast router to remove the branch from the multicast tree.

IGMP Snooping Configuration

The main IGMP Snooping configuration includes:

- “Enabling/Disabling IGMP Snooping”
- “Configuring Router Port Aging Time”
- “Configuring Maximum Response Time”
- “Configuring Aging Time of Multicast Group Member Ports”
- “Configuring Unknown Multicast Packets not Broadcasted within a VLAN”
- “Configuring the Filtering Rule of Multicast Groups”
- “Enabling/Disabling IGMP Snooping Fast Leave”

Among the above configuration tasks, enabling IGMP Snooping is required, while others are optional for your requirements.

Enabling/Disabling IGMP Snooping

You can use the following commands to enable/disable IGMP Snooping to control whether MAC multicast forwarding table is created and maintained on Layer 2.

Perform the following configuration in system view and VLAN view.

Table 411 Enable/Disable IGMP Snooping

Operation	Command
Enable/disable IGMP Snooping	igmp-snooping { enable disable }

By default, IGMP Snooping is disabled.



CAUTION:

- First enable IGMP Snooping globally in system view, and then enable IGMP Snooping in VLAN view. Otherwise, IGMP Snooping will not take effect.
- Although layer 2 and layer 3 multicast protocols can be configured in pair, they cannot run on the same VLAN or its corresponding VLAN interface at the same time. For example, if PIM or IGMP is enabled on a VLAN, then IGMP Snooping cannot operate on this VLAN.
- If the VLAN VPN is enabled on a port, the IGMP Snooping feature cannot be enabled on the VLAN for the port or the IGMP feature cannot be enabled on the corresponding VLAN interface.
- If IGMP Snooping feature is enabled on a VLAN, or IGMP is enabled on the VLAN interface, you cannot add the member port on which VLAN VPN is enabled into the VLAN.

- Isolate-user-VLAN supports the IGMP-Snooping function. After IGMP-Snooping is enabled under isolate-user-VLAN, all secondary VLANs are IGMP-Snooping enabled. It makes no sense to enable IGMP-Snooping for a secondary VLAN.
- In a secondary VLAN, IGMP packets will be directly converted and processed in isolate-user-VLAN, namely all the multicast services are implemented within isolate-user-VLAN.
- Ports in secondary VLANs cannot be used as source addresses of multicast.

Configuring Router Port Aging Time

This task is to manually configure the router port aging time. If the switch has not received any general query message from the router before the router port is aged, it will remove the port from all MAC multicast groups.

Perform the following configuration in system view.

Table 412 Configure router port aging time

Operation	Command
Configure router port aging time	igmp-snooping router-aging-time <i>seconds</i>
Restore the default aging time of the router port	undo igmp-snooping router-aging-time

By default, the router port aging time is 105s.

Configuring Maximum Response Time

This task is to manually configure the maximum response time. If the Ethernet switch receives no report message from a port within the maximum response time, it will remove the port from the multicast group.

Perform the following configuration in system view.

Table 413 Configure the maximum response time

Operation	Command
Configure the maximum response time	igmp-snooping max-response-time <i>seconds</i>
Restore the default setting	undo IGMP-snooping max-response-time

By default, the maximum response time is 1 seconds.

Configuring Aging Time of Multicast Group Member Ports

This task is to manually set the aging time of the multicast group member port. If the Ethernet switch receives no multicast group report message during the member port aging time, it will transmit the specific query message to that port and starts a maximum response timer.

Perform the following configuration in system view.

Table 414 Configure aging time of the multicast member ports

Operation	Command
Configure aging time of the multicast member	igmp-snooping host-aging-time <i>seconds</i>
Restore the default setting	undo igmp-snooping host-aging-time

By default, the aging time of the multicast member is 260 seconds.

Configuring Unknown Multicast Packets not Broadcasted within a VLAN

This configuration task is to enable/disable the function of not broadcasting unknown multicast packets within a VLAN. If this function is disabled but IGMP snooping enabled on VLAN, multicast packets are broadcasted on within the VLAN when the destination broadcast group has no member ports. When this function is enabled, however, multicast packets are only forwarded to the router port, but not broadcasted within the VLAN if no member port exists. In addition, since the router sends regularly IGMP Query and PIM Hello packets, the switch can identify which ports are router ports. If there is no member port or router port, the packets will be directly dropped, instead of being forwarded.



CAUTION: *If IGMP snooping is not enabled on the VLAN (nor Layer 3 multicast), unknown multicast packets are broadcasted within the VLAN no matter whether this function is enabled or not. Therefore, to disable unknown multicast packets from flooding within a VLAN, you must enable igmp-snooping in this VLAN and carry out the **igmp-snooping nonflooding-enable** command.*

Perform the following configuration in system view.

Table 415 Globally enable/disable multicast packets not broadcasted within a VLAN

Operation	Command
Enable multicast packets not to be broadcasted within a VLAN	igmp-snooping nonflooding-enable
Disable multicast packets not to be broadcasted within a VLAN	undo igmp-snooping nonflooding-enable

By default, unknown multicast packets are broadcasted within the VLAN.

Configuring the Filtering Rule of Multicast Groups

On the IGMP snooping-enabled switch, you can configure ACL rules whether the specified multicast group can be joined to a VLAN or not. This feature filters every received IGMP join packet. According to the destination group address of the packets and the ACL rule bound to the VLAN, the switch determines whether to discard the packets or let them pass.

By setting the filtering rule of multicast groups in the VLAN, you can control access to IP multicast groups. You can only configure one ACL rule for each VLAN, and the new configured rule will replace the old one.

Perform the following configuration in system view.

Table 416 Configure the filtering rule of multicast group

Operation	Command
Set the filtering rule of multicast groups in the specified VLAN	igmp-snooping group-policy acl-number
Cancel the filtering rule of multicast groups in the specified VLAN	undo igmp-snooping group-policy

By default, no filtering rule is set for a VLAN. In this case, a host can be joined to any multicast group.

**CAUTION:**

- If an inexistent *acl-number* is bound to the VLAN, or if the bound *acl-number* is not configured with a rule, a host is still allowed to join any multicast group.
- If no *acl-number* exists, you can also configure the filtering rule of multicast groups in VLAN view. That is, this rule is not restricted by the ACL itself, and is valid for all members in the specified VLAN.

Enabling/Disabling IGMP Snooping Fast Leave

An IGMP Snooping-enabled Layer 2 switch directly removes a fast leave-enabled port from the list of member ports of the multicast group when the port receives a leave packet. That is, the switch removes the port from the multicast group without forwarding the multicast data, or sending the specific group query messages to the port,, or enabling response query timer to the port.

Table 417 Enable/Disable IGMP Snooping fast leave

Operation	Command	Remarks
Enter system view	system-view	-
Enable IGMP Snooping fast leave in system view	igmp-snooping fast-leave [vlan { <i>vlan-id</i> [to <i>vlan-id</i>] } &<1-10>]	IGMP Snooping fast leave is disabled by default.
Enter Ethernet port view	interface interface-type interface-number	-
Enable IGMP Snooping fast leave in Ethernet port view	igmp-snooping fast-leave [vlan { <i>vlan-id</i> [to <i>vlan-id</i>] } &<1-10>]	IGMP Snooping fast leave is disabled by default.
Disable IGMP Snooping fast leave	undo igmp-snooping fast-leave [vlan { <i>vlan-id</i> [to <i>vlan-id</i>] } &<1-10>]	-

For detailed configuration, refer to the *3Com Switch 8800 Family Series Routing Switches Command Manual*.



- Fast leave configurations that are configured in system view and Ethernet port view operate separately.
- Fast leave works on all ports of the specified VLANs if you configure it in system view. However, it only works on the current port (e.g., when a Trunk port belongs to multiple VLANs) in the specified VLANs if you configure it in Ethernet port view.

**CAUTION:**

- Fast leave configured for a port takes effect only when the VLAN it belongs to is IGMP Snooping-enabled.
- Fast leave does not work if the corresponding specified VLANs do not exist, the port does not belong to any of the specified VLANs, or the VLANs do not have IGMP Snooping enabled.
- A newly configured IGMP Snooping clears all existing fast leave configurations.
- The **igmp-snooping fast-leave** command is useless if you do not enable IGMP Snooping globally. (You can execute the **igmp-snooping enable** command in system view to enable IGMP Snooping globally.)

- When you configure IGMP Snooping fast leave on aggregation ports, the configuration takes effect only on primary aggregation ports.
- If you add an IGMP V1 host of the same multicast group to the port, the switch does not remove the port when the port receives an IGMP Leave packet of the multicast group even you enable IGMP Snooping fast leave for the port.

Multicast Static Routing Port Configuration

Introduction By configuring a port in a VLAN to be a static routing port, you can enable IGMP packets to be transparently transmitted through the port, meeting the requirements of specific networks.

- Prerequisites**
- Ports and VLANs involved already exist.
 - Ports to be configured belong to corresponding VLANs.

Configuring a Multicast Static Routing Port

You can configure a port in a VLAN to be a static routing port in VLAN view.

Table 418 Configure a port in a VLAN to be a static routing port in VLAN view

Operation	Command	Remarks
Enter system view	system-view	-
Enter VLAN view	vlan <i>vlan-id</i>	-
Configure multicast static routing port	multicast static-router-port <i>port-number</i>	Provide the <i>port-number</i> argument in the format of <i>interface-type interface-number</i> , where the <i>interface-type</i> argument can only be Ethernet port type. By default, no static routing port is configured.

You can also configure a port in a VLAN to be a static routing port in the corresponding Ethernet port view.

Table 419 Configure a port in a VLAN to be a static routing port in Ethernet port view

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type interface-number</i>	The <i>interface-type</i> argument can only be Ethernet port type.
Configure multicast static routing port	multicast static-router-port <i>vlan vlan-id</i>	By default, no static routing port is configured.



CAUTION:

- You will fail to configure a port to be a static routing port if the port identified by the *port-number* argument does not exist, or the port does not belong to the VLAN.

- You will fail to configure a port to be a static routing port if the VLAN identified by the *vlan-id* argument does not exist or the port does not belong to the VLAN.
- You can configure multiple ports in a VLAN to be static routing ports by performing the above configuration repeatedly. The newly configured ports do not replace the existing static routing ports.
- When a trunk port belongs to multiple VLANs, this port can be configured as the static routing port for multiple VLANs.
- Static routing ports can be configured in VLAN view or Ethernet port view. However, you can verify the configured static routing ports only by executing the **display this** command in Ethernet port view.
- The configuration of a static routing port takes effect on the current port only, no matter whether the current port is an aggregated port or not. To configure all ports in an aggregation group as static routing ports, you can enable the static routing port function on all the ports in the aggregation group.
- Static routing port is valid when IGMP-snooping, IGMP, PIM-DM or PIM-SM is enabled in the VLAN.

Displaying and Maintaining IGMP Snooping

After the above configuration, execute **display** command in any view to display the running of the IGMP Snooping configuration, and to verify the effect of the configuration.

Use the **debugging mpm** command in user view to carry out multicast debugging.

Table 420 Display and debug IGMP Snooping

Operation	Command
Display the information about current IGMP Snooping configuration	display igmp-snooping configuration
Display IGMP Snooping statistics of received and sent messages	display igmp-snooping statistics
Display IP/MAC multicast group information in the VLAN	display igmp-snooping group [vlan <i>vlan-id</i>[<i>group-address</i>]]
Enable IGMP Snooping debugging	debugging mpm { abnormal all event forward groups packets timer }
Clear IGMP Snooping statistics information	reset igmp-snooping statistics

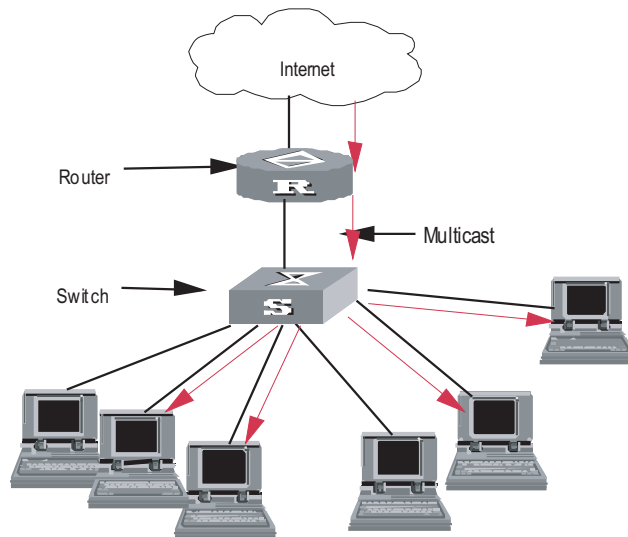
IGMP Snooping Configuration Example

Enable IGMP Snooping Network requirements

To implement IGMP Snooping on the switch, you need to enable IGMP Snooping on the switch first. The switch is connected with the router via the router port, and connected with user PC through the non-router ports.

Network diagram

Figure 105 Network diagram for IGMP Snooping configuration



Configuration procedure

Suppose you need to enable IGMP Snooping on VLAN10. The procedures are as follows:

Display the current state of IGMP Snooping.

```
<SW8800> display igmp-snooping configuration
```

If IGMP Snooping is not enabled, enable it in system view.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] igmp-snooping enable
```

Display the status of the VLAN10 interface, to check if PIM or IGMP is enabled on this interface.

```
[SW8800] display current-configuration interface Vlan-interface 10
```

You can enable IGMP Snooping in VLAN view only if PIM or IGMP is not running on VLAN10.

```
[SW8800] vlan10
[3Com-vlan10] igmp-snooping enable
```

Troubleshooting IGMP Snooping

Fault: Multicast function cannot be implemented on the switch.

Troubleshooting:

- 1 IGMP Snooping is disabled.
 - Carry out the **display current-configuration** command in any view to display the status of IGMP Snooping.

- If IGMP Snooping is not enabled, carry out the **igmp-snooping enable** command in system view to enable IGMP Snooping. Then, use the same command in VLAN view to enable IGMP Snooping in the corresponding VLAN.
- 2** Multicast forwarding table set up by IGMP Snooping is incorrect.
- Carry out the **display igmp-snooping group** command in any view to display if the multicast group is the expected one.
 - If the multicast group created by IGMP Snooping is not correct, turn to professional maintenance personnel for help.
 - Continue with diagnosis 3 if the second step is completed.
- 3** Multicast forwarding table set up on the bottom layer is incorrect.
- In any view, carry out the **display mac-address vlan** command to check whether the MAC multicast forwarding table established in the bottom layer by *vlan-id* is consistent with that established by IGMP Snooping.
 - If they are not consistent, please contact the maintenance personnel for help.

Multicast VLAN Overview

Based on the current multicast on demand, when users in different VLANs request the service, multicast flow is duplicated in each VLAN and thus a great deal of bandwidth is wasted. To solve this problem, we provide the multicast VLAN feature. With this feature, you can add switch ports to a multicast VLAN and enable IGMP Snooping to allow users in different VLANs to share the same multicast VLAN. In this way, multicast flow is transmitted in one multicast VLAN instead of multiple user VLANs and bandwidth is greatly saved.

As multicast VLAN is isolated from user VLANs, this guarantees both security and enough bandwidth. After you configure the multicast VLAN, multicast information flow can be transmitted to users continuously.

Multicast VLAN Configuration

Multicast VLAN is based on layer 2 multicast. The following table describes the multicast VLAN configuration tasks:

Table 421 Configure multicast VLAN

Item	Command	Remarks
Enter system view	system-view	-
Enable IGMP Snooping in system view	igmp-snooping enable	Required
Enter VLAN view	vlan <i>vlan-id</i>	-
IGMP Snooping is enabled on the VLAN	igmp-snooping enable	Required
Enable IGMP Snooping in VLAN view	igmp-snooping enable	Required
Enable multicast VLAN	service-type multicast	Required
Quit VLAN view	quit	
Enter the view of the Ethernet port connected to the user	interface <i>interface-type</i> <i>interface-number</i>	-
Define the port type to hybrid	port link-type hybrid	Required
Add ports to corresponding VLANs	port hybrid vlan <i>vlan-id-list</i> untagged	Required



- A port can only belong to one multicast VLAN.
- The type of the ports connected to user terminals must be hybrid untagged.
- The current system supports up to three multicast VLANs.

Multicast VLAN Configuration Example

Network requirements

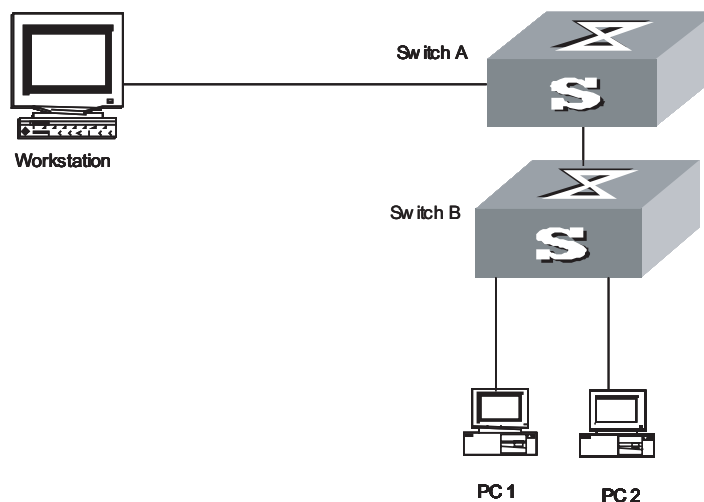
Configure a multicast VLAN, so that users in VLAN 2 and VLAN 3 receive multicast flows through the multicast VLAN10.

Table 422 Device number and description

Device	Description	Requirement
Switch A	Layer 3 switch	The IP address of VLAN 2 interface is 168.10.1.1. The port E1/1/1 belongs to VLAN 2 and is connected to the Workstation The IP address of VLAN 10 interface is 168.20.1.1. The port E1/1/10 belongs to VLAN 10 and is connected to Switch B Configure layer 3 multicast PIM DM and IGMP on VLAN 10
Switch B	Layer 2 switch	VLAN 2 contains the port E1/1/1 and VLAN 3 contains the port E1/1/2. The ports E1/1/1 and E1/1/2 are connected to PC1 and PC2 respectively. The port E1/1/10 is connected to Switch A.
PC 1	User 1	PC1 is connected to the port E1/1/1 of Switch B.
PC 2	User 2	PC2 is connected to the port E1/1/2 of Switch B.

Network diagram

Figure 106 Network diagram for multicast VLAN configuration



Configuration procedure

Before performing the following configurations, you should configure the IP addresses and connect the devices correctly.

1 Configure Switch A

Configure the IP address of the VLAN 2 interface to 168.10.1.1. Enable the PIM-DM protocol.

```
<Switch A> system-view
System View: return to User View with Ctrl+Z.
[Switch A] multicast routing-enable
[Switch A] interface vlan-interface 2
[Switch A-Vlan-interface2] ip address 168.10.1.1 255.255.255.0
```



```
[Switch A-Vlan-interface2] pim dm
[Switch A-Vlan-interface2] quit
```

Configure the IP address of the VLAN 10 interface to 168.20.1.1. Enable the PIM-DM and IGMP protocols.

```
[Switch A] interface vlan-interface 10
[Switch A-Vlan-interface10] ip address 168.20.1.1 255.255.255.0
[Switch A-Vlan-interface10] pim dm
[Switch A-Vlan-interface10] igmp enable
[Switch A-Vlan-interface10] quit
```

Define Ethernet 1/1/10 as a trunk port and add this port to VLAN 10.

```
[Switch A] interface Ethernet1/1/10
[Switch A-Ethernet1/1/10] port link-type trunk
[Switch A-Ethernet1/1/10] port trunk permit vlan 10
```

2 Configure Switch B

Enable IGMP Snooping.

```
<Switch B> system-view
System View: return to User View with Ctrl+Z.
[Switch B] igmp-snooping enable
```

Enable IGMP-Snooping on VLAN 2 and VLAN 3.

```
[Switch B] vlan 2
[Switch B-vlan 2] igmp-snooping enable
[Switch B-vlan 2] quit
[Switch B] vlan 3
[Switch B-vlan 3] igmp-snooping enable
```

Configure VLAN 10 as multicast VLAN. Enable IGMP Snooping.

```
[Switch B] vlan 10
[Switch B-vlan10] igmp-snooping enable
[Switch B-vlan10] service-type multicast
[Switch B-vlan10] quit
```

Define Ethernet 1/1/10 as trunk port. Add the port to VLAN 10.

```
[Switch B] interface Ethernet 1/1/10
[Switch B-Ethernet 1/1/10] port link-type trunk
[Switch B-Ethernet 1/1/10] port trunk vlan 10
[Switch B-Ethernet 1/1/10] quit
```

Define Ethernet 1/1/1 as hybrid port. Add the port to VLAN 2 and VLAN 10. Make the port carry no VLAN label when it transmits packets of VLAN 2 and VLAN 10. Set the default VLAN ID of the port to VLAN 2.

```
[Switch B] interface Ethernet 1/1/1
[Switch B-Ethernet 1/1/1] port link-type hybrid
[Switch B-Ethernet 1/1/1] port hybrid vlan 2 10 untagged
[Switch B-Ethernet 1/1/1] port hybrid pvid vlan 2
[Switch B-Ethernet 1/1/1] quit
```

Define Ethernet 1/1/2 as hybrid port. Add the port to VLAN 3 and VLAN 10. Make the port carry no VLAN label when it transmits packets of VLAN 3 and VLAN 10. Set the default VLAN ID of the port to VLAN 3.

```
[Switch B] interface Ethernet 1/1/2
[Switch B-Ethernet 1/1/2] port link-type hybrid
[Switch B-Ethernet 1/1/2] port hybrid vlan 3 10 untagged
[Switch B-Ethernet 1/1/2] port hybrid pvid vlan 3
[Switch B-Ethernet 1/1/2] quit
```

41

COMMON MULTICAST CONFIGURATION

Introduction to Common Multicast Configuration

The multicast common configuration is for both the multicast group management protocol and the multicast routing protocol. The configuration includes enabling IP multicast routing, displaying multicast routing table and multicast forwarding table, etc.

Common Multicast Configuration

Common multicast configuration includes:

- Enabling multicast routing
- Configuring multicast route limit
- Clearing MFC (Multicast Forwarding Cache) forwarding entries or its statistic information
- Configuring managed multicast
- Clearing route entries from the kernel multicast routing table
- Configuring broadcast/multicast suppression

Enabling Multicast Routing

Enable multicast routing first before enabling multicast routing protocol.

Perform the following configuration in system view.

Table 423 Enable multicast routing

Operation	Command
Enable multicast routing	multicast routing-enable
Disable multicast routing	undo multicast routing-enable

By default, multicast routing is disabled.



CAUTION: Multicast routing must be enabled before other multicast configurations can take effect.

Configuring Multicast Routing Table Size Limit

Because too many multicast routing table entries may exhaust the router memory, you need to limit the size of the multicast routing table.

Table 424 Configure multicast routing table size limit

Operation	Command	Remarks
Enter system view	system-view	-
Configure multicast routing table size limit	multicast route-limit limit	By default, the maximum multicast routing table entries is 512



- When you insert a new interface module, if this interface module does not support the current multicast router table size configured in the system, this interface module will be disabled.
- The new configuration replaces the earlier one when you execute this command repeatedly,

**CAUTION:**

During the configuration of multicast routing table size limit,

- If the current multicast routing table size limit is bigger than the configured value, the system prompts "Warning: Modifying the limit will delete all multicast routing-tables. Do you want to continue? [Y/N]"; if you choose "Y", the system removes all multicast routing tables, and sets new multicast routing table size.
- If the current multicast routing table size limit is smaller the configured value, or the current system does not support this kind of interface module, the system prompts "Slot X does not support the limit, configuration failed"; otherwise, a new multicast routing table size is successfully configured.

Clearing MFC Forwarding Entries or Its Statistic Information

You can clear MFC forward entries or statistic information of FMC forward entries via the following command.

Perform the following configuration in user view.

Table 425 Clear MFC forwarding entries or its statistic information

Operation	Command
Clear MFC forwarding entries or its statistic information	reset multicast forwarding-table [statistics] { all { <i>group-address</i> [mask { <i>group-mask</i> <i>group-mask-length</i> }] <i>source-address</i> [mask { <i>source-mask</i> <i>source-mask-length</i> }] incoming-interface { null <i>NULL-interface-number</i> <i>interface-type interface-number</i> } * }

Clearing Route Entries from the Kernel Multicast Routing Table

You can clear route entries from the kernel multicast routing table, as well as MFC forwarding entries via the following command.

Perform the following configuration in user view.

Table 426 Clear routing entries of multicast routing table

Operation	Command
Clear routing entries of multicast routing table	reset multicast routing-table { all { <i>group-address</i> [mask { <i>group-mask</i> <i>group-mask-length</i> }] <i>source-address</i> [mask { <i>source-mask</i> <i>source-mask-length</i> }] incoming-interface <i>vlan-interface interface-number</i> } * }

The corresponding forwarding entries in MFC are cleared together with the clearing of routing entries of multicast routing table,

Managed multicast Configuration

Managed multicast Overview

The managed multicast feature controls user's authority to join multicast groups. This feature is based on ports: users must first pass the 802.1x authentication set for their ports. Then they are allowed to join the multicast groups specifically configured for them but are prohibited from joining any multicast group they are not authorized to join. In this way, users access to specific multicast groups under control.

Prerequisites of multicast authentication:

- 802.1x is enabled both globally and on ports. Then, when you enable managed multicast, all IGMP report messages are legal. Then the system allows users to join any group and cannot control the access to multicast groups.
- The managed multicast is based on port. The 802.1x mode on port must be port authentication. Otherwise, the system discards all IGMP report messages without any processing.

Configuring Managed Multicast

Perform the following configurations in system view.

Table 427 Set/remove the managed multicast function of the system

Operation	Command
Enable managed multicast	ip managed-multicast
Disable managed multicast	undo ip managed-multicast

Table 428 Set managed multicast for users in a specific domain

Operation	Command
Set the multicast group which users in the specified domain are authorized to join	local-user multicast [domain <i>domain-name</i>] <i>ip-address</i> [<i>mask-length</i>]
Remove the multicast group which users in the specified domain are authorized to join	undo local-user multicast [domain <i>domain-name</i>] <i>ip-address</i>

Perform the following configuration in local user view.

Configure managed multicast in local user view

Table 429 Set/remove the multicast group which users are authorized to join

Operation	Command
Set multicast group which users are authorized to join (managed multicast)	multicast <i>ip-address</i> [<i>ip-address</i> &<1-9> <i>mask-length</i>]
Remove the specified managed multicast	undo multicast { <i>ip-address</i> [<i>ip-address</i> &<1-9>] all }



CAUTION: In local user view, before executing this command, you must configure user service type to LAN-ACCESS, which is the only one supported by managed multicast at present.

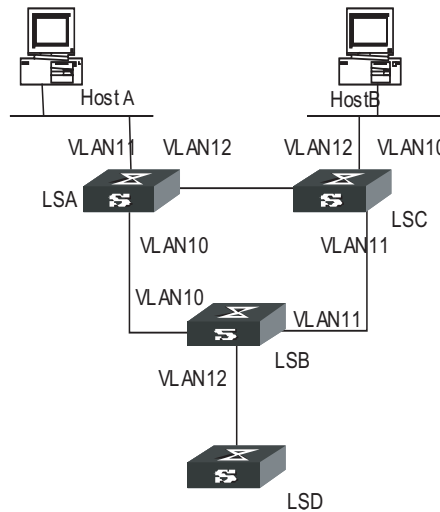
Managed Multicast Configuration Example

Network requirements

As shown in Figure 107, HostA and HostB join the multicast group. Layer 3 multicast is enabled on LSA, LSB, LSC and LSD. Managed multicast is enabled on LSA and LSC. Because managed multicast combines multicast with 802.1x, 802.1x must be enabled on LSA and LSC.

Network diagram

Figure 107 Network diagram for managed multicast



Configuration procedure

Managed multicast is a module combined with 802.1x, so you need to perform the following configuration beside multicast configuration:

Enable managed multicast globally.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] ip managed-multicast
```

Enable 802.1x globally.

```
[SW8800] dot1x
```

Enable 802.1x on the controlled ports (the access ports for LSA and LSC).

```
[SW8800]interface GigabitEthernet2/1/1
[3Com-GigabitEthernet2/1/1] dot1x
[3Com-GigabitEthernet2/1/1] interface GigabitEthernet2/1/2
[3Com-GigabitEthernet2/1/2] dot1x
```

Configure the authentication mode on the controlled ports to port-based mode.

```
[3Com-GigabitEthernet2/1/2] dot1x port-method portbased
[3Com-GigabitEthernet2/1/2] interface GigabitEthernet2/1/1
[3Com-GigabitEthernet2/1/1] dot1x port-method portbased
[3Com-GigabitEthernet2/1/1] quit
```

```
# Create a local-user in system view. Then set the password and service type for
the user.
```

```
[SW8800] local-user liu
[3Com-luser-liu] password simple aaa
[3Com-luser-liu] service-type lan-access
```

```
# In user view, configure the allowed multicast group for the user to join.
```

```
[3Com-luser-liu] multicast 227.1.1.1
```

Configuring Broadcast/Multicast Suppression

Introduction To prevent port congestion resulting from broadcast/multicast packet flooding, the switch supports broadcast/multicast suppression. You can enable broadcast/multicast suppression by setting the speed percentage or bandwidth values.

Configuration

Table 430 Configure Broadcast/Multicast Suppression

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	Required <i>interface-type</i> must be Ethernet
Configure multicast suppression ration Ethernet port	multicast-suppression { <i>ratio</i> bandwidth <i>bandwidth</i> }	Optional By default, the multicast suppression ratio is 100%
Configure broadcast suppression ration Ethernet port	broadcast-suppression { <i>ratio</i> bandwidth <i>bandwidth</i> }	Optional By default, the broadcast suppression ratio is 50%



CAUTION:

- You cannot enable both broadcast suppression and multicast suppression simultaneously on the same card. Namely, once you have enabled broadcast suppression on some ports of a card, you cannot enable multicast suppression on the other ports of the card, and vice versa.
- If multicast suppression is enabled, broadcast packets are also suppressed at the same time, while broadcast suppression does not work on multicast suppression.
- No distinction is made between known multicast and unknown multicast for multicast suppression.

Displaying and Debugging Common Multicast Configuration

After the above configuration, execute **display** command in any view to display the running of the multicast configuration, and to verify the effect of the configuration.

Execute **debugging** command in user view for the debugging of multicast.

Table 431 Display and Debug Common Multicast Configuration

Operation	Command
Display the multicast routing table	display multicast routing-table [<i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }]] <i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }] incoming-interface { <i>vlan-interface</i> <i>vlan-interface-number</i> register }]*
Display the multicast forwarding table	display multicast forwarding-table [<i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }]] <i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }]] incoming-interface { <i>interface-type</i> <i>interface-number</i> null <i>NULL-interface-number</i> register }]*
View port-specific multicast forwarding table information	display mpm forwarding-table [<i>group-address</i> <i>source-address</i>]
View IP multicast group and MAC multicast group information of all VLANs or a specific VLAN	display mpm group [<i>vlan</i> <i>vlan-id</i> [<i>ip-address</i>]]
Enable multicast packet forwarding debugging	debugging multicast forwarding
Disable multicast packet forwarding debugging	undo debugging multicast forwarding
Enable multicast forwarding status debugging	debugging multicast status-forwarding
Disable multicast forwarding status debugging	undo debugging multicast status-forwarding
Enable multicast kernel routing debugging	debugging multicast kernel-routing
Disable multicast kernel routing debugging	undo debugging multicast kernel-routing

The multicast routing tables can be layered as follows:

- Each multicast routing protocol has a multicast routing table of itself.
- All the multicast routing tables can be summarized into the multicast kernel routing tables.
- The multicast kernel routing tables should keep consistent with the multicast forwarding tables which actually control the forwarding of the multicast data packets.

The multicast forwarding tables are mainly used for debugging. Usually, users can view the multicast kernel routing tables to get the required information.

IGMP Overview

Introduction to IGMP

Internet Group Management Protocol (IGMP) is a protocol in the TCP/IP suite responsible for management of IP multicast members. It is used to establish and maintain multicast membership among IP hosts and their directly connected neighboring routers. IGMP excludes transmitting and maintenance of membership information among multicast routers, which are completed by multicast routing protocols. All hosts participating in multicast must implement IGMP.

Hosts participating in IP multicast can join and leave a multicast group at any time. The number of members of a multicast group can be any integer and the location of them can be anywhere. A multicast router does not need and cannot keep the membership of all hosts. It only uses IGMP to learn whether receivers (i.e., group members) of a multicast group are present on the subnet connected to each interface. A host only needs to keep which multicast groups it has joined.

IGMP is not symmetric on hosts and routers. Hosts need to respond to IGMP query messages from the multicast router, i.e., report the group membership to the router. The router needs to send membership query messages periodically to discover whether hosts join the specified group on its subnets according to the received response messages. When the router receives the report that hosts leave the group, the router will send a group-specific query packet (IGMP Version 2) to discover whether no member exists in the group.

Up to now, IGMP has three versions, namely, IGMP Version 1 (defined by RFC1112), IGMP Version 2 (defined by RFC2236) and IGMP Version 3. At present, IGMP Version 2 is the most widely used version.

IGMP Version 2 boasts the following improvements over IGMP Version 1:

Election mechanism of multicast routers on the shared network segment

A shared network segment means that there are multiple multicast routers on a network segment. In this case, all routers running IGMP on the network segment can receive the membership report from hosts. Therefore, only one router is necessary to send membership query messages. In this case, the router election mechanism is required to specify a router as the querier.

In IGMP Version 1, selection of the querier is determined by the multicast routing protocol. While IGMP Version 2 specifies that the multicast router with the smallest IP address is elected as the querier when there are multiple multicast routers on the same network segment.

Leaving group mechanism

In IGMP Version 1, hosts leave the multicast group quietly without informing the multicast router. In this case, the multicast router can only depend on the timeout of the response time of the multicast group to confirm that hosts leave the group. In Version 2, when a host is intended to leave, it will send a leave group message if it is the host who responds to the latest membership query message.

Specific group query

In IGMP Version 1, a query of a multicast router is targeted at all the multicast groups on the network segment, which is known as General Query.

In IGMP Version 2, Group-Specific Query is added besides general query. The destination IP address of the query packet is the IP address of the multicast group. The group address domain in the packet is also the IP address of the multicast group. This prevents the hosts of members of other multicast groups from sending response messages.

Max response time

The Max Response Time is added in IGMP Version 2. It is used to dynamically adjust the allowed maximum time for a host to respond to the group query message.

Introduction to IGMP Proxy

For a large scale network with multicast routing protocol employed, many leaf networks may exist (a leaf network here refers to an end node of a multicast forwarding tree, it is a subnet that contains multicast clients only). It is a heavy load to configure and manage all these leaf networks.

You can ease the workload of configuring and managing leaf networks without affecting the multicast connections in them by enabling IGMP proxy on devices in these leaf networks.

After IGMP proxy is configured, the devices in leaf networks act as a host to the exterior network. They receive the multicast data of the associated group only when some of the hosts directly connected to them are multicast group members.

Description of IGMP proxy configuration

Figure 108 A schematic diagram of IGMP proxy

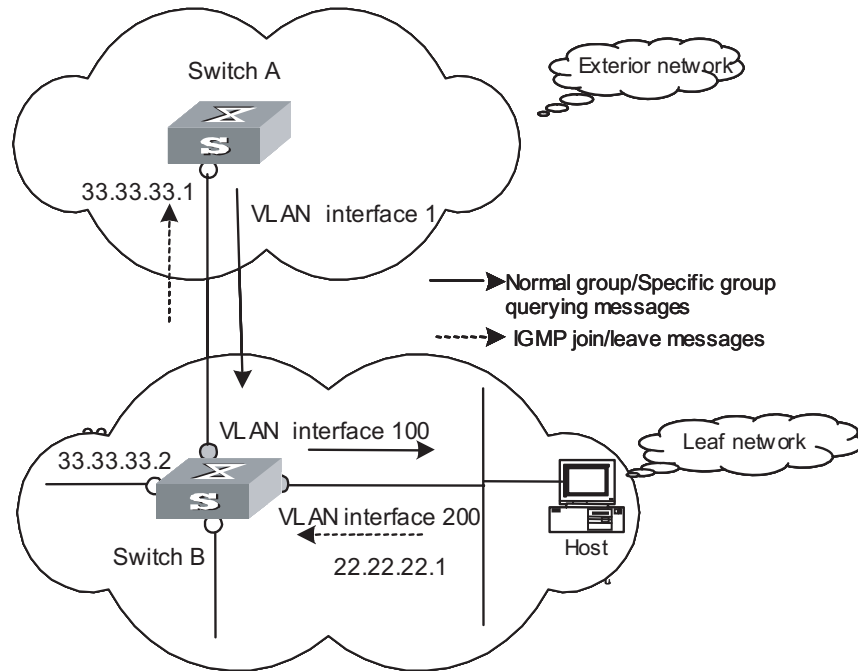


Figure 108 illustrates how IGMP proxy works. In this figure:

Switch B is configured as follows:

- Multicast is enabled.
- PIM and IGMP are configured on the interfaces of VLAN 100 and VLAN 200.
- The interface of VLAN 100 is configured as the IGMP proxy interface of the interface of VLAN 200.

Switch A is configured as follows:

- Multicast is enabled.
- PIM and IGMP are configured on the interface of VLAN 100.
- The **pim neighbor-policy** command is executed in VLAN 100 interface view to filter the PIM neighbors of the network segment 33.33.33.0/24. That is, prevent Switch B from being the PIM neighbor.

Operating mechanism of IGMP Proxy

The procedures to process IGMP join/leave messages are as follows:

- After receiving an IGMP join/leave message sourced from a host through the interface of VLAN 200, Switch B changes the source address of the message to the IP address of VLAN 100 interface (33.33.33.2), which is the outbound interface leading to Switch A.
- Switch B sends the IGMP message to Switch A.

- Switch A processes the message after receiving the IGMP message sent by Switch B through the interface of VLAN 100, just as the message is sent by a host directly connected to the interface of VLAN 100.

The procedures to process IGMP normal group or specific group querying messages are as follows:

- After receiving a normal group or a specific group querying message from Switch A, Switch B changes the source address of the querying message to the address of the outbound interface leading to hosts.
- Switch B transmits the message through the interface of VLAN 200.

IGMP Proxy Configuration

Configuration prerequisites

- IP addresses, PIM, pim neighbor-policy have been configured in the corresponding interfaces of the devices in the exterior network.
- The switches in the leaf networks are multicast-enabled. The related ports are added to specific VLANs. IP addresses, PIM, and IGMP have been configured in the corresponding interfaces.

Configuration procedure

Table 432 Configure IGMP Proxy

Operation	Command	Remarks
Enter system view	system-view	-
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable IGMP Proxy on the current interface and specify the proxy interface for the current interface	igmp proxy <i>interface-type</i> <i>interface-number</i>	Required By default, IGMP Proxy is disabled on the interface



CAUTION:

- Enable PIM protocol on the interface first before configuring IGMP Proxy.
- If you configure IGMP Proxy for an interface multiple times, the latest configuration is valid.
- One interface cannot be the IGMP proxy interface of two or more other interfaces simultaneously.

IGMP Configuration

After the multicast function is enabled, you must enable IGMP on the interface first and then perform other IGMP configurations.

IGMP basic configuration includes:

- Enabling multicast
- Enabling IGMP on an interface

IGMP advanced configuration includes:

- Enabling the compatibility control function of the switch

- Configuring the IGMP version
- Configuring the IGMP query message interval
- Configuring the IGMP querier present timer
- Configuring the maximum query response time
- Configuring the limit of IGMP groups on an interface
- Adding a router to the specified multicast group.
- Configuring the interval of sending IGMP Group-Specific Query packet
- Configuring the number of times of sending IGMP Group-Specific Query packet
- Deleting IGMP Groups Joined on an Interface
- Configuring the Filtering Rule of Multicast Groups
- Enabling/Disabling IGMP Fast Leaving

Enabling Multicast

Only if the multicast function is enabled can the multicast-related configurations take effect.

Refer to “Enabling Multicast Routing” “Enabling Multicast Routing”.

Enabling IGMP on an Interface

This configuration task is to enable IGMP on the interface which needs to maintain the multicast membership. After this, you can initiate IGMP feature configuration.

Perform the following configuration in interface view.

Table 433 Enable/Disable IGMP on an interface

Operation	Command
Enable IGMP on an interface	igmp enable
Disable IGMP on an interface	undo igmp enable

By default, IGMP is disabled on the interface.



CAUTION:

- If the VLAN VPN is enabled on a port, the IGMP Snooping feature cannot be enabled on the VLAN for the port, and the IGMP feature cannot be enabled on the corresponding interface either.
- If IGMP Snooping feature is enabled on a VLAN, or IGMP is enabled on the interface, you cannot add the member port on which VLAN VPN is enabled into the VLAN.

Enabling Compatibility Control Function of the Switch

With the compatibility control function enabled the switch processes the protocol message with the destination IP address 224.0.0.1 in the IGMP Report packet. Otherwise, the switch discards this kind of packets.

Perform the following configuration in system view.

Table 434 Enable compatibility control function of the switch

Operation	Command
Enabling compatibility control function of the switch	igmp-report enhance enable

By default, the compatibility control function of the switch is disabled.

This command is often executed after IGMP or IGMP Spooning protocol is enabled in the system.

Configuring the IGMP Version

Perform the following configuration in VLAN interface view.

Table 435 Configure the IGMP version

Operation	Command
Select the IGMP version that the router uses	igmp version { 2 1 }
Restore the default setting	undo igmp version

By default, IGMP Version 2 is used.



CAUTION: *The system does not support automatic switching between different IGMP versions. Therefore, all routers on a subnet must be configured to run the same IGMP version.*

Configuring the Interval to Send IGMP Query Message

Multicast routers send IGMP query messages to discover which multicast groups are present on attached networks. Multicast routers send query messages periodically to refresh their knowledge of members present on their networks.

Perform the following configuration in VLAN interface view.

Table 436 Configure the interval to send IGMP query message

Operation	Command
Configure the interval to send IGMP query message	igmp timer query seconds
Restore the default value	undo igmp timer query

When there are multiple multicast routers on a network segment, the querier is responsible for sending IGMP query messages to all hosts on the LAN.

By default, the interval is 60 seconds.

Configuring the Interval and the Number of Querying IGMP Packets

On the shared network, it is the query router (querier) that maintains IGMP membership on the interface. The **igmp lastmember-queryinterval** and **igmp robust-count** commands are used to configure the interval and times of sending IGMP group-specific query packets for the querier when it receives an IGMP leave message from a host.

- The host sends the IGMP Leave message.
- Upon receiving the message, IGMP querier sends the group-specific IGMP query message for specified times (defined by the *robust-value* in **igmp robust-count**, with the default value being 2) and at a time interval (defined by the *seconds* in **igmp lastmember-queryinterval**, with the default value being 1 second).

- When other hosts receive the message from the IGMP querier and are interested in this group, they return the IGMP Membership Report message within the defined maximum response time.
- If IGMP querier receives the report messages from other hosts within the period equal to *robust-value* × seconds, it continues membership maintenance for this group.
- If it receives no report message from any other host within this period, it reckons this as timeout and ends membership maintenance for this group.

This configuration takes effect only when the querier runs IGMP version 2. If a host runs IGMP Version 1, it does not send IGMP Leave Group message when it leaves a group. In this case, this configuration does not work for the host.

Please perform the following configurations in VLAN interface view.

Configuring interval for querying IGMP packets

Table 437 Configure interval for querying IGMP packets

Operation	Command
Configure interval for querying IGMP packets	igmp lastmember-queryinterval <i>seconds</i>
Restore the default query interval	undo igmp lastmember-queryinterval

By default, the interval is 1 second.

Configuring the number of last member querying

Table 438 Configure the number of last member querying

Operation	Command
Configure number of last member querying	igmp robust-count <i>robust-value</i>
Restore the default number of querying	undo igmp robust-count

By default, an IGMP group-specific query message is sent for twice.

Configuring the Present Time of IGMP Querier

On shared network, namely a network segment where multiple multicast routers exist, a query router (querier for short) sends query messages on the interface regularly. If a non-query router fails to receive messages from the querier within a period of time, it will deem that the querier has failed and take over the job of the original querier.

In the IGMP V1 version, the querier selection is determined by the multicast routing protocol; in the IGMP V2 version, the router with the smallest IP address on a shared network segment acts as the querier.

The IGMP querier presence time is the period of time before the router takes over as the querier sending query messages, after the previous querier has stopped doing so.

Perform the following configuration in VLAN interface view.

Table 439 Configure the present time of IGMP querier

Operation	Command
Change the present time of IGMP querier	igmp timer other-querier-present <i>seconds</i>
Restore the default value	undo igmp timer other-querier-present

By default, the value is twice the IGMP query message interval, namely 120 seconds.

Configuring Maximum Response Time for IGMP Query Message

When a router receives a query message, the host will set a timer for each multicast group it belongs to. The value of the timer is randomly selected between 0 and the maximum response time. When any timer becomes 0, the host will send the membership report message of the multicast group.

Setting the maximum response time reasonably can enable the host to respond to query messages quickly. In this case, the router can fast master the existing status of the members of the multicast group.

Perform the following configuration in interface view.

Table 440 Configure the maximum response time for IGMP query message

Operation	Command
Configure the maximum response time for IGMP query message	igmp max-response-time <i>seconds</i>
Restore the maximum query response time to the default value	undo igmp max-response-time

The smaller the maximum query response time value, the faster the router prunes groups. The actual response time is a random value in the range from 1 to 25 seconds. By default, the maximum query response time is 10 seconds.

Configuring the limit of IGMP groups on an interface

If there is no limit to the number of IGMP groups added on a router interface or a router, the router memory may be exhausted, which may cause router failure.

You can set number limit for the IGMP groups added on the interface, but not the number limit for the IGMP groups added in the router, which is defined by the system.

Perform the following configuration in VLAN interface view.

Table 441 Configure the limit of IGMP groups on an interface

Operation	Command
Configure the limit of IGMP groups on an interface	igmp group-limit <i>limit</i>
Restore the limit of IGMP groups on an interface to the default value	undo igmp group-limit

By default, the maximum number of IGMP groups on an interface is 512.

Configuring a Router to Join Specified Multicast Group

Usually, the host operating IGMP will respond to IGMP query packet of the multicast router. In case of response failure, the multicast router will consider that there is no multicast member on this network segment and will cancel the corresponding path. Configuring one interface of the router as multicast member can avoid such problem. When the interface receives IGMP query packet, the router will respond, thus ensuring that the network segment where the interface located can normally receive multicast packets.

For an Ethernet switch, you can configure a port in a switch interface to join a multicast group.

Perform the following configuration in the corresponding view.

Table 442 Configure a router to join specified multicast group

Operation	Command
Configure the router to join a specified multicast group (in interface view)	igmp host-join <i>group-address</i> port <i>interface-type interface-number [to interface-type interface-number]</i>
Cancel the configuration (in interface view)	undo igmp host-join <i>group-address</i> port <i>interface-type interface-num [to interface-type interface-number]</i>
Configure the router to join a specified multicast group (in Ethernet port view)	igmp host-join <i>group-address</i> vlan <i>vlan-id</i>
Cancel the configuration (in Ethernet port view)	undo igmp host-join <i>group-address</i> vlan <i>vlan-id</i>



The above two configuration methods have the same result (both takes effect on port). You can select either of them.

By default, a router joins no multicast group. Note that the specified port must belong to this interface on which IGMP is enabled. Otherwise, the configuration does not take effect.

Deleting IGMP Groups Joined on an Interface

This configuration task is to delete all IGMP groups joined on all interfaces or specific interfaces of the router, or to delete the IGMP groups at the specific address or in the specific network segment on the specific interfaces of the router.

Perform the following configuration in user view.

Table 443 Delete IGMP groups joined on an interface

Operation	Command
Delete IGMP groups joined on an interface	reset igmp group { all interface <i>vlan-interface interface-number</i> } { all <i>group-address [group-mask]</i> }

After a group is deleted, if other IGMP membership report messages occur, the interfaces can join the corresponding group again.

Configuring the Filtering Rule of Multicast Groups

On the IGMP snooping-enabled switch, you can configure ACL rules whether the specified multicast group can be joined to a VLAN or not. This feature filters every received IGMP join packet. According to the destination group address of the

packets and the ACL rule bound to the VLAN, the switch determines whether to discard the packets or let them pass.

By setting the filtering rule of multicast groups in the VLAN, you can control access to IP multicast groups. You can only configure one ACL rule for each VLAN, and the new configured rule will replace the old one.

Perform the following configuration in VLAN view.

Table 444 Configure the aging time of multicast group members

Operation	Command
Set the filtering rule of multicast groups in the specified VLAN	igmp-snooping group-policy <i>acl-number</i>
Cancel the filtering rule of multicast groups in the specified VLAN	undo igmp-snooping group-policy

By default, no filtering rule is set for a VLAN. In this case, a host can be joined to any multicast group.



CAUTION:

- If an inexistent *acl-number* is bound to the VLAN, or if the bound *acl-number* is not configured with a rule, a host is still allowed to join any multicast group.
- The multicast group filtering rule is not restricted by the ACL itself, and is valid for all members in the specified VLAN.

Enabling/Disabling IGMP Fast Leave

An IGMP-enabled Layer 3 switch does not query packets of the specific multicast group to a fast leave-enabled port any longer when the port receives an IGMP leave packet. Instead, the switch removes the port from the outbound port lists of all Layer 3 multicast forwarding tables that are of the same multicast group to peel off the port from the multicast group. That is, the switch does not send specific query packet to the port or forward multicast data to the port.

Perform the following configuration in Ethernet port view or system view.

Table 445 Enable/Disable IGMP fast leave

Operation	Command	Remarks
Enter system view	system-view	-
Enable IGMP fast leave in system view	igmp fast-leave [vlan { <i>vlan-id</i> [to <i>vlan-id</i>] } &<1-10>]	IGMP fast leave is disabled by default
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable IGMP fast leave in Ethernet port view	igmp fast-leave [vlan { <i>vlan-id</i> [to <i>vlan-id</i>] } &<1-10>]	IGMP fast leave is disabled by default
Disable IGMP fast leave	undo igmp fast-leave [vlan { <i>vlan-id</i> [to <i>vlan-id</i>] } &<1-10>]	-

For detailed configuration, refer to the *3Com Switch 8800 Family Series Routing Switches Command Manual*.



- Fast leaves that are configured in system view and Ethernet port view operate separately.
- The configuration made in system view will be effective to ports within all the specified VLANs, while the configuration in port view will be effective to the port within the specific VLANs (for example, when a trunk port belongs to multiple VLANs).



CAUTION:

- If the specified VLANs do not exist, the port does not belong to any of the specified VLANs, or the VLANs do not have IGMP enabled, you can still configure the fast leave feature, but the configuration will not take effect.
- You must enable multicast routing globally by executing the **multicast routing-enable** command in system view before you can configure the fast leave feature.
- If global multicast routing is disabled, all existing IGMP fast leave-related configurations will be cleared.
- When you configure IGMP fast leave on aggregation ports, the configuration takes effect only on primary aggregation ports.
- If you have added an IGMP V1 host of the same multicast group to the port, or configured a static host of the same multicast group by using the **igmp host-join** command, the switch does not remove the port when the port receives an IGMP Leave packet of the multicast group even if you have enabled IGMP fast leave for the port.

IGMP Configuration Example

Network requirements

As shown in Figure 109, Switch B resides in a leaf network. Configure IGMP proxy for Switch B to ease the configuration and management work load in the leaf network without affecting multicast connections in it.

You need to perform the following configurations to meet the requirements:

- Enable IGMP and PIM-DM for the related VLAN interfaces on Switch A.
- Enable multicast on Switch B. Enable PIM for the interfaces of VLAN 100 and VLAN 200. Configure the interface of VLAN 100 to be the proxy interface of the interface of VLAN 200.



The following depicts IGMP and IGMP proxy configuration (other related configuration is not covered here).

Enable multicast.

```
<SwitchA>system-view
System View: return to User View with Ctrl+Z.
[SwitchA] multicast routing-enable
```

Enable IGMP and PIM-DM for the interface of VLAN 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface 100] igmp enable
[SwitchA-Vlan-interface 100] pim dm
```

Configure Vlan-interface 100 so that it will not use the IP address 33.33.33.2 as a PIM neighbor

```
[SwitchA-Vlan-interface 100] pim neighbor-policy 2001
[SwitchA-Vlan-interface 100] quit
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule deny source 33.33.33.2 0
[SwitchA-acl-basic-2001] rule permit source any
```

3 Configure Receiver.

Receiver establishes HTTP connections to the multicast source and sends the list of the names of the services provided by the multicast source to the clients (Each service has its own multicast address, which is the multicast group). When a service is selected, the client sends IGMP packets to join the multicast group, through which the receiver can receive the corresponding multicast packets.

Displaying and Debugging IGMP

After the above configuration, execute **display** command in any view to display the running of IGMP configuration, and to verify the effect of the configuration.

Execute **debugging** command in corresponding views for the debugging of IGMP.

Table 446 Display and debug IGMP

Operation	Command
Display the information about members of IGMP multicast groups	display igmp group [<i>group-address</i> interface <i>vlan-interface interface-number</i>]
Display the IGMP configuration and running information about the interface	display igmp interface [<i>vlan-interface interface-number</i>]
Enable the IGMP information debugging	debugging igmp { all event host packet timer }
Disable the IGMP information debugging	undo debugging igmp { all event host packet timer }

43

PIM-DM CONFIGURATION

PIM-DM Overview

Introduction to PIM-DM PIM-DM (Protocol Independent Multicast, Dense Mode) belongs to dense mode multicast routing protocols. PIM-DM is suitable for small networks. Members of multicast groups are relatively dense in such network environments.

PIM-DM Working Principle The working procedures of PIM-DM include neighbor discovery, flood & prune and graft.

Neighbor discovery

The PIM-DM router needs to use Hello messages to perform neighbor discovery when it is started. All network nodes running PIM-DM keep in touch with one another with Hello messages, which are sent periodically.

Flood&Prune

PIM-DM assumes that all hosts on the network are ready to receive multicast data. When a multicast source "S" begins to send data to a multicast group "G", after the router receives the multicast packets, the router will perform RPF check according to the unicast routing table first. If the RPF check is passed, the router will create an (S, G) entry and then flood the data to all downstream PIM-DM nodes. If the RPF check is not passed, that is, multicast packets enter from an error interface, the packets will be discarded. After this process, an (S, G) entry will be created in the PIM-DM multicast domain.

If the downstream node has no multicast group members, it will send a Prune message to the upstream nodes to inform the upstream node not to forward data to the downstream node. Receiving the prune message, the upstream node will remove the corresponding interface from the outgoing interface list corresponding to the multicast forwarding entry (S, G). In this way, a SPT (Shortest Path Tree) rooted at Source S is built. The pruning process is initiated by leaf routers first.

This process is called "flood & prune" process. In addition, nodes that are pruned provide timeout mechanism. Each router re-starts the "flood & prune" process upon pruning timeout. The consistent "flood & prune" process of PIM-DM is performed periodically.

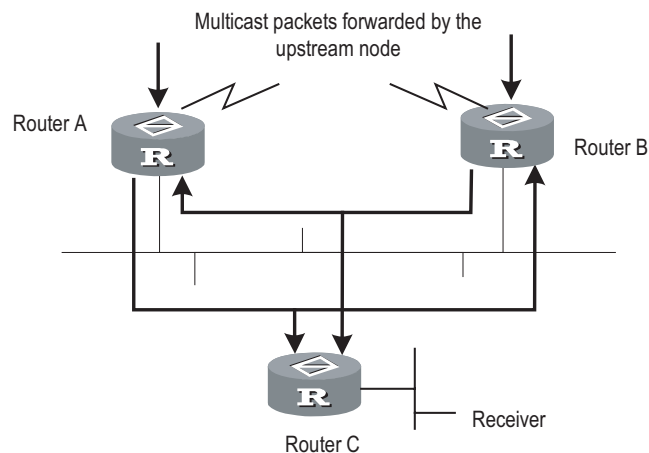
During this process, PIM-DM uses the RPF check and the existing unicast routing table to build a multicast forwarding tree rooted at the data source. When a packet arrives, the router will first judge the correctness of the path. If the interface that the packet arrives is the one indicated by the unicast routing to the multicast source, the packet is regarded to be from the correct path. Otherwise, the packet will be discarded as a redundancy packet without the multicast

forwarding. The unicast routing information as path judgment can come from any unicast routing protocol independent of any specified unicast routing protocol such as the routing information learned by RIP and OSPF

Assert mechanism

As shown in the following figure, both routers A and B on the LAN have their own receiving paths to multicast source S. In this case, when they receive a multicast packet sent from multicast source S, they will both forward the packet to the LAN. Multicast Router C at the downstream node will receive two copies of the same multicast packet.

Figure 110 Assert mechanism diagram



When they detect such a case, routers need to select a unique sender by using the assert mechanism. Routers will send Assert packets to select the best path. If two or more than two paths have the same priority and metric, the path with a higher IP address will be the upstream neighbor of the (S, G) entry, which is responsible for forwarding the (S, G) multicast packet.



Currently assert mechanism is not available on the 3Com Switch 8800 Family Series Routing Switches.

Graft

When the pruned downstream node needs to be restored to the forwarding state, the node will send a graft packet to inform the upstream node.

PIM-DM Configuration

- 1 PIM-DM basic configuration includes:
 - Enabling multicast
 - Enabling PIM-DM
- 2 PIM-DM advanced configuration includes:
 - Configuring the time interval for ports to send Hello packets
 - Entering the PIM view
 - Configuring filtering of multicast source/group
 - Configuring filtering of PIM neighbor

- Configuring the maximum number of PIM neighbor on an interface
- Clearing PIM neighbors

Enabling Multicast Refer to “Enabling Multicast Routing” “Enabling Multicast Routing”.

Enabling PIM-DM PIM-DM needs to be enabled in configuration of all interfaces.

After PIM-DM is enabled on an interface, it will send PIM Hello messages periodically and process protocol packets sent by PIM neighbors.

Perform the following configuration in VLAN interface view.

Table 447 Enable PIM-DM

Operation	Command
Enable PIM-DM on an interface	pim dm
Disable PIM-DM on an interface	undo pim dm

It's recommended to configure PIM-DM on all interfaces in non-special cases. This configuration is effective only after the multicast routing is enabled in system view.

Once enabled PIM-DM on an interface, PIM-SM cannot be enabled on the same interface and vice versa.

Configuring the Time Intervals for Ports to Send Hello Packets

When protocol independent multicast (PIM) protocol is enabled for a port, the port sends Hello packets periodically. The time intervals to send Hello packets vary with the bandwidth and type of the connected networks.

Perform the following configuration in interface view.

Table 448 Configure the time intervals for ports to send Hello packets

Operation	Command
Configure the time intervals for ports to send Hello packets	pim timer hello seconds
Restore the default values of the time intervals	undo pim timer hello

You can configure different time intervals according to the actual networks. By default, the time interval for sending Hello packets is 30 seconds. In general, you need not modify the parameter *seconds*.



- The time interval can be configured only after the PIM protocol such as protocol independent multicast-dense mode (PIM-DM) protocol or protocol independent multicast-sparse mode (PIM-SM) protocol is enabled in interface view.
- When you configure the time interval for a port to send Hello packets, the pim neighbor hold-time value automatically turns into 3.5 times the time interval value. Therefore you need not configure a value for pim neighbor hold-time.

Entering the PIM View Global parameters of PIM should be configured in PIM view.

Perform the following configuration in system view.

Table 449 Entering PIM

Operation	Command
Enter PIM view	pim
Clear the configuration performed in PIM view and return to system view	undo pim

Using **undo pim** command, you can, and back to system view.

Configuring the Filtering of Multicast Source/Group

You can set to filter the source (and group) address of multicast data packets via this command. When this feature is configured, the router filters not only multicast data, but the multicast data encapsulated in the registration packets.

Perform the following configuration in the PIM view.

Table 450 Configure the filtering of multicast source/group

Operation	Command
Configure the filtering of multicast source/group	source-policy <i>acl-number</i>
Remove the configuration of filtering	undo source-policy

If resource address filtering is configured, as well as basic ACLs, then the router filters the resource addresses of all multicast data packets received. Those not matched will be discarded.

If resource address filtering is configured, as well as advanced ACLs, then the router filters the resource and group addresses of all multicast data packets received. Those not matched will be discarded.

This command also filters multicast data encapsulated in registration packets.

If this command is executed for a second time, the previous configuration will be overwritten by the new configuration.

Configuring the Filtering of PIM Neighbor

You can configure basic ACLs to filter the routers which can be PIM neighbors of the current interface.

Perform the following configuration in the interface view.

Table 451 Configure the filtering of PIM neighbor

Operation	Command
Configure filtering of PIM neighbor	pim neighbor-policy <i>acl-number</i>
Remove the configuration of filtering	undo pim neighbor-policy

Configuring the Maximum Number of PIM Neighbor on an Interface

The maximum number of PIM neighbors of a router interface can be configured to avoid exhausting the memory of the router or router faults. The maximum number of PIM neighbors of a router is defined by the system, and is not open for modification.

Perform the following configuration in the interface view.

Table 452 Configure the maximum number of PIM neighbor on an interface

Operation	Command
Configure the maximum number of PIM neighbor on an interface	pim neighbor-limit <i>limit</i>
Restore the limit of PIN neighbor to the default value	pim neighbor-limit

By default, the PIM neighbors on the interface are limited to 128.

If the number of PIM neighbors of an interface has exceeded the configured value by the time of configuration, the existing PIM neighbors will not be deleted.

Clearing PIM Routing Table Entries

Perform the following configuration in user view.

Table 453 Clear multicast route entries from PIM routing table

Operation	Command
Clear multicast route entries from PIM routing table	reset pim routing-table { all { <i>group-address</i> [mask { <i>group-mask</i> <i>group-mask-length</i> }] <i>source-address</i> [mask { <i>source-mask</i> <i>source-mask-length</i> }] } { incoming-interface <i>interface-type interface-number</i> null } } * }

Clearing PIM Neighbors

Perform the following configuration in user view.

Table 454 Reset PIM neighbor

Operation	Command
Clear PIM neighbors	reset pim neighbor { all { <i>neighbor-address</i> interface <i>interface-type interface-number</i> } } *

Displaying and Debugging PIM-DM

After the above configuration, execute **display** command in any view to display the running of PIM-DM configuration, and to verify the effect of the configuration.

Execute **debugging** command in user view for the debugging of PIM-DM.

Table 455 Display and debug PIM-DM

Operation	Command
Display the PIM multicast routing table	display pim routing-table [{ { *g [<i>group-address</i> [mask { <i>mask-length</i> <i>mask</i> }]] } **rp [<i>rp-address</i> [mask { <i>mask-length</i> <i>mask</i> }]] } { <i>group-address</i> [mask { <i>mask-length</i> <i>mask</i> }] <i>source-address</i> [mask { <i>mask-length</i> <i>mask</i> }] } * } incoming-interface <i>interface-type interface-number</i> null } { dense-mode sparse-mode } } *
Display the PIM interface information	display pim interface [<i>Vlan-interface Vlan-interface-number</i>]
Display the information about PIM neighboring routers	display pim neighbor [interface <i>Vlan-interface Vlan-interface-number</i>]
Display BSR information	display pim bsr-info
Display RP information	display pim rp-info [<i>group-address</i>]

Table 455 Display and debug PIM-DM

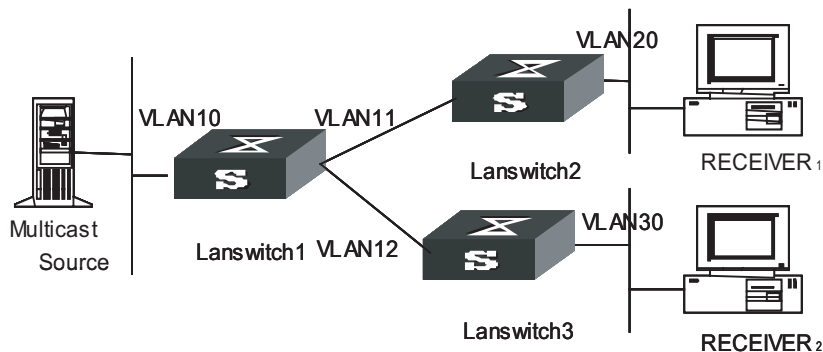
Operation	Command
Enable the PIM debugging	debugging pim common { all event packet timer }
Disable the PIM debugging	undo debugging pim common { all event packet timer }
Enable the PIM-DM debugging	debugging pim dm { alert all mbr mrt timer warning { rcv send } } { all assert graft graft-ack join prune } }
Disable the PIM-DM debugging	undo debugging pim dm { alert all mbr mrt timer warning { rcv send } } { all assert graft graft-ack join prune } }

PIM-DM Configuration Example

Network requirements

Lanswitch1 is connected to the multicast source through VLAN-interface 10, connected to Lanswitch2 through VLAN-interface 11 and connected to Lanswitch3 through VLAN-interface 12. Through running PIM-DM, you can implement multicast among RECEIVER 1, RECEIVER 12 and Multicast Source.

Network diagram

Figure 111 Network diagram for PIM-DM configuration

Configuration procedure

1 Configuration on Lanswitch1

Enable the multicast routing.

```

<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast routing-enable
  
```

Enable IGMP and PIM-DM on the interface.

```

[SW8800] vlan 10
[3Com-vlan10] port ethernet 2/1/2
[3Com-vlan10] quit
[SW8800] vlan 11
[3Com-vlan11] port ethernet 2/1/4
[3Com-vlan11] quit
[SW8800] vlan 12
[3Com-vlan12] port ethernet 2/1/6
[3Com-vlan12] quit
  
```

```
[SW8800] interface vlan-interface 10
[3Com-vlan-interface10] ip address 1.1.1.1 255.255.0.0
[3Com-vlan-interface10] pim dm
[3Com-vlan-interface10] quit
[SW8800] interface vlan-interface 11
[3Com-vlan-interface11] ip address 2.2.2.2 255.255.0.0
[3Com-vlan-interface11] pim dm
[3Com-vlan-interface11] quit
[SW8800] interface vlan-interface 12
[3Com-vlan-interface12] ip address 3.3.3.3 255.255.0.0
[3Com-vlan-interface12] pim dm
```

2 Configuration on Lanswitch2, (configuration on Lanswitch3 is similar)

Enable the multicast routing

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast routing-enable
```

Enable IGMP and PIM-DM on the interface

```
[SW8800] vlan 11
[3Com-vlan11] port ethernet 2/1/2
[3Com-vlan11] quit
[SW8800] vlan 12
[3Com-vlan12] port ethernet 2/1/4
[3Com-vlan12] quit
[SW8800] vlan 20
[3Com-vlan20] port ethernet 2/1/6
[3Com-vlan20] quit
[SW8800] interface vlan-interface 11
[3Com-vlan-interface11] ip address 1.1.1.2 255.255.0.0
[3Com-vlan-interface11] pim dm
[3Com-vlan-interface11] quit
[SW8800] interface vlan-interface 12
[3Com-vlan-interface12] ip address 2.2.2.2 255.255.0.0
[3Com-vlan-interface12] pim dm
[3Com-vlan-interface12] quit
[SW8800] interface vlan-interface 20
[3Com-vlan-interface20] ip address 3.3.3.2 255.255.0.0
[3Com-vlan-interface20] igmp enable
[3Com-vlan-interface20] pim dm
```



You should enable PIM-DM on all equal-cost routes if there are any.

44

PIM-SM CONFIGURATION

PIM-SM Overview

Introduction to PIM-SM PIM-SM (Protocol Independent Multicast, Sparse Mode) belongs to sparse mode multicast routing protocols. PIM-SM is mainly applicable to large-scale networks with broad scope in which group members are relatively sparse.

Different from the flood & prune principle of the dense mode, PIM-SM assumes that all hosts do not need to receive multicast packets, unless there is an explicit request for the packets.

PIM-SM uses the RP (Rendezvous Point) and the BSR (Bootstrap Router) to advertise multicast information to all PIM-SM routers and uses the join/prune information of the router to build the RP-rooted shared tree (RPT), thereby reducing the bandwidth occupied by data packets and control packets and reducing the process overhead of the router. Multicast data flows along the shared tree to the network segments the multicast group members are on. When the data traffic is sufficient, the multicast data flow can switch over to the SPT (Shortest Path Tree) rooted on the source to reduce network delay. PIM-SM does not depend on the specified unicast routing protocol but uses the present unicast routing table to perform the RPF check.

Note that, the creation and interaction of the RPs and BSRs are implemented through periodical RP advertisements and BSR Bootstrap packets respectively.

To make PIM-SM operate, you must configure candidate RPs and BSRs. BSRs collect and broadcast the information from candidate RPs.

PIM-SM Working Principle The PIM-SM working process is as follows: neighbor discovery, building the RP-rooted shared tree (RPT), multicast source registration and SPT switchover etc. The neighbor discovery mechanism is the same as that of PIM-DM, which will not be described any more.

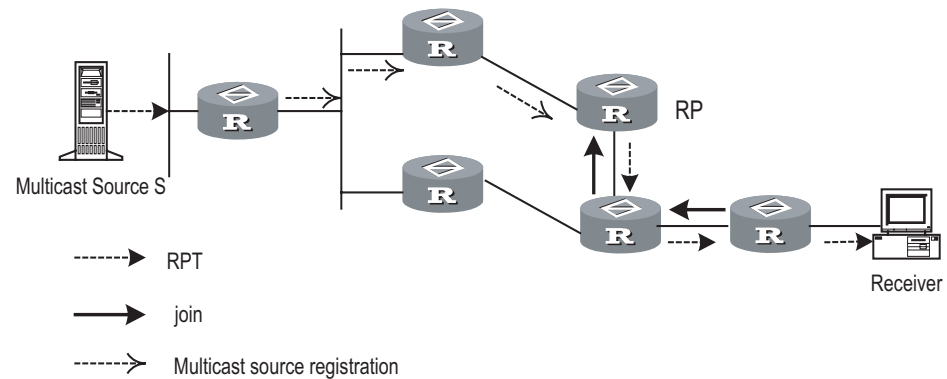
Build the RP shared tree (RPT)

When hosts join a multicast group G, the leaf routers that directly connect with the hosts send IGMP messages to learn the receivers of multicast group G. In this way, the leaf routers calculate the corresponding rendezvous point (RP) for multicast group G and then send join messages to the node of the next level toward the rendezvous point (RP).

Each router along the path between the leaf routers and the RP will generate (*, G) entries in the forwarding table, indicating that all packets sent to multicast group G are applicable to the entries no matter from which source they are sent. When the RP receives the packets sent to multicast group G, the packets will be

sent to leaf routers along the path built and then reach the hosts. In this way, an RP-rooted tree (RPT) is built as shown in Figure 8-1.

Figure 112 RPT schematic diagram



Multicast source registration

When multicast source S sends a multicast packet to the multicast group G, the PIM-SM multicast router directly connected to S will encapsulate the received packet into a registration packet and send it to the corresponding RP in unicast form. If there are multiple PIM-SM multicast routers on a network segment, the Designated Router (DR) will be responsible for sending the multicast packet.

Preparations before Configuring PIM-SM

Configuring candidate RPs

In a PIM-SM network, multiple RPs (candidate-RPs) can be configured. Each Candidate-RP (C-RP) is responsible for forwarding multicast packets with the destination addresses in a certain range. Configuring multiple C-RPs is to implement load balancing of the RP. These C-RPs are equal. All multicast routers calculate the RPs corresponding to multicast groups according to the same algorithm after receiving the C-RP messages that the BSR advertises.



CAUTION: One RP can serve multiple multicast groups or all multicast groups. Each multicast group can correspond to one unique RP at a time rather than multiple RPs.

Configuring BSRs

The BSR is the management core in a PIM-SM network. Candidate-RPs send announcement to the BSR, which is responsible for collecting and advertising the information about all candidate-RPs.



CAUTION: There can be only one BSR in a network but you can configure multiple candidate-BSRs. In this case, once a BSR fails, you can switch over to another BSR. A BSR is elected among the C-BSRs automatically. The C-BSR with the highest priority is elected as the BSR. If the priority is the same, the C-BSR with the largest IP address is elected as the BSR.

Configuring static RP

The router that serves as the RP is the core router of multicast routes. If the dynamic RP elected by BSR mechanism is invalid for some reason, the static RP can be configured to specify RP. As the backup of dynamic RP, static RP improves

network robustness and enhances the operation and management capability of multicast network.

PIM-SM Configuration

- 1 PIM-SM basic configuration includes:
 - Enabling Multicast
 - Enabling PIM-SM
 - Entering the PIM view
 - Configuring candidate-BSRs
 - Configuring candidate-RPs
 - Configuring static RP
- 2 PIM-SM advanced configuration includes:
 - Configuring the PIM-SM domain boundary
 - Configuring the sending interval for the Hello packets of the interface
 - Configuring the filtering of multicast source/group
 - Configuring the filtering of PIM neighbor
 - Configuring the maximum number of PIM neighbor on an interface
 - Configuring RP to filter the register messages
 - Limiting the range of legal BSR
 - Limiting the range of legal C-RP
 - Clearing multicast route entries from PIM routing table
 - Clearing PIM neighbor



CAUTION: At least one router in an entire PIM-SM domain should be configured with C-RPs and C-BSRs.

Enabling Multicast Refer to “Enabling Multicast Routing” “Enabling Multicast Routing”.

Enabling PIM-SM This configuration can be effective only after multicast is enabled.

Perform the following configuration in interface view.

Table 456 Enable PIM-SM

Operation	Command
Enable PIM-SM on an interface	pim sm
Disable PIM-SM on an interface	undo pim sm

Repeat this configuration to enable PIM-SM on other interfaces. Only one multicast routing protocol can be enabled on an interface at a time.

Once enabled PIM-SM on an interface, PIM-DM cannot be enabled on the same interface and vice versa.

Entering the PIM View Refer to “Entering the PIM View” “Entering the PIM View”.

Configuring the Time Intervals for Ports to Send Hello Packets In general, PIM-SM broadcasts Hello packets on the PIM-SM-enabled port periodically to detect PIM neighbors and determine the designated router (DR).

For details, refer to “Configuring the Time Intervals for Ports to Send Hello Packets” “Configuring the Time Intervals for Ports to Send Hello Packets”.

Configuring Candidate-BSRs In a PIM domain, one or more candidate BSRs should be configured. A BSR (Bootstrap Router) is elected among candidate BSRs. The BSR takes charge of collecting and advertising RP information.

The automatic election among candidate BSRs is described as follows:

One interface which has started PIM-SM must be specified when configuring the router as the candidate BSR.

At first, each candidate BSR considers itself as the BSR of the PIM-SM domain, and sends Bootstrap message by taking the IP address of the interface as the BSR address.

When receiving Bootstrap messages from other routers, the candidate BSR will compare the BSR address of the newly received Bootstrap message with that of itself. Comparison standards include priority and IP address. The bigger IP address is considered better when the priority is the same. If the priority of the former is higher, the candidate BSR will replace its BSR address and stop regarding itself as the BSR. Otherwise, the candidate BSR will keep its BSR address and continue to regard itself as the BSR.

Perform the following configuration in PIM view.

Table 457 Configure candidate-BSRs

Operation	Command
Configure a candidate-BSR	c-bsr Vlan-interface <i>Vlan-interface-number</i> <i>hash-mask-len</i> [<i>priority</i>]
Remove the candidate-BSR configured	undo c-bsr

Candidate-BSRs should be configured on the routers in the network backbone. By default, no BSR is set. The default priority is 0.



CAUTION: *One router can only be configured with one candidate-BSR. When a candidate-BSR is configured on another interface, it will replace the previous configuration.*

Configuring Candidate-RPs In PIM-SM, the shared tree built by multicast routing data is rooted at the RP. There is a mapping from a multicast group to an RP. A multicast group can be mapped to only one RP. Different multicast groups can be mapped to the same RP or different RPs.

Perform the following configuration in PIM view.

Table 458 Configure candidate-RPs

Operation	Command
Configure a candidate-RP	c-rp <i>interface-type interface-number</i> [group-policy <i>acl-number</i> priority <i>priority-value</i>]*
Remove the candidate-RP configured	undo c-rp { <i>interface-type interface-number</i> all }

When configuring RP, if the range of the served multicast group is not specified, the RP will serve all multicast groups. Otherwise, the range of the served multicast group is the multicast group in the specified range. It is suggested to configure Candidate RP on the backbone router.



CAUTION: Using the **group-policy** command on a candidate RP, you can configure only the permit rule. After the configuration of the permit rule, the RP only serves for groups included in the permit rule.

Configuring Static RP

To enhance network robustness, static RP serves as the backup of dynamic RP

Table 459 Configure static RP

Operation	Command	Remarks
Enter system view	system-view	-
Enter PIM view	pim	Required
Configure static RP	static-rp <i>rp-address</i> [<i>acl-number</i>]	Required



CAUTION:

- When the RP elected by BSR mechanism is effective, static RP does not work.
- All routers in the PIM domain must be configured with this command simultaneously, with the same RP address specified.
- The system supports up to ten different static RP addresses. When more than ten static RP addresses are configured, the system will give this prompt information: "Cannot config static-rp, exceeded static-rp limit 10".

Configuring the PIM-SM Domain Border

After the PIM-SM domain border is configured, bootstrap messages can not cross the border in any direction. In this way, the PIM-SM domain can be split.

Perform the following configuration in interface view.

Table 460 Configure the PIM-SM domain border

Operation	Command
Set the PIM-SM domain border	pim bsr-boundary
Remove the PIM-SM domain border configured	undo pim bsr-boundary

By default, no domain border is set.

After this configuration is performed, a bootstrap message can not cross the border but other PIM packets can. This configuration can effectively divide a network into domains using different BSRs.

Configuring the filtering of multicast source/group

Refer to “Configuring the Filtering of Multicast Source/Group” “Configuring the Filtering of Multicast Source/Group”.

Configuring the filtering of PIM neighbor

Refer to “Configuring the Filtering of PIM Neighbor” “Configuring the Filtering of PIM Neighbor”.

Refer to “Configuring the Maximum Number of PIM Neighbor on an Interface” “Configuring the Maximum Number of PIM Neighbor on an Interface”.

Configuring RP to Filter the Register Messages Sent by DR

In the PIM-SM network, the register message filtering mechanism can control which sources to send messages to which groups on the RP, i.e., RP can filter the register messages sent by DR to accept specified messages only.

Perform the following configuration in PIM view.

Table 461 Configure RP to filter the register messages sent by DR

Operation	Command
Configure RP to filter the register messages sent by DR	register-policy <i>acl-number</i>
Cancel the configured filter of messages	undo register-policy

If an entry of a source group is denied by the ACL, or the ACL does not define operation to it, or there is no ACL defined, the RP will send RegisterStop messages to the DR to prevent the register process of the multicast data stream.



CAUTION: Only the register messages matching the ACL permit clause can be accepted by the RP. Specifying an undefined ACL will make the RP deny all register messages.

Limiting the range of legal BSR

To prevent the legal BSR from being replaced maliciously in the network, you can limit the range of legal BSR. Other BSR messages beyond the range are not received by the router and thus ensure the BSR security.

Perform the following configuration in PIM view.

Table 462 Limit the range of legal BSR

Operation	Command
Set the limit legal BSR range	bsr-policy <i>acl-number</i>
Restore to the default setting	undo bsr-policy

For detailed information of **bsr-policy**, refer to the *3Com Switch 8800 Family Series Routing Switches Command Manual*.

Limiting the range of legal C-RP

To avoid C-RP spoofing, you can limit the range of legal C-RP and limit the groups that each C-RP servers.

Perform the following configuration in PIM view.

Table 463 Limit the range of legal C-RP

Operation	Command
Set the limit legal C-RP range	crp-policy <i>acl-number</i>
Restore to the default setting	undo crp-policy

For detailed information of **crp-policy**, refer to the *3Com Switch 8800 Family Series Routing Switches Command Manual*

Clearing multicast route entries from PIM routing table

Refer to “Clearing PIM Routing Table Entries” “Clearing PIM Routing Table Entries”.

Clearing PIM Neighbors

Refer to “Clearing PIM Neighbors” “Clearing PIM Neighbors”.

Displaying and Debugging PIM-SM

After the above configuration, execute the **display** command in any view to display the running of PIM-SM configuration, and to verify the effect of the configuration.

Execute the **debugging** command in user view for the debugging of PIM-SM.

Table 464 Display and debug PIM-SM

Operation	Command
Display the BSR information	display pim bsr-info
Display the RP information	display pim rp-info [<i>group-address</i>]
Enable the PIM-SM debugging	debugging pim sm { all mbr { alert fresh } verbose mrt msdp timer { assert bsr crpadv jp jpgdelay mrt probe spt } warning { recv send } { assert bootstrap crpadv jp reg regstop }
Disable the PIM-SM debugging	undo debugging pim sm { all mbr { alert fresh } verbose mrt msdp timer { assert bsr crpadv jp jpgdelay mrt probe spt } warning { recv send } { assert bootstrap crpadv jp reg regstop }

PIM-SM Configuration Example

Network requirements

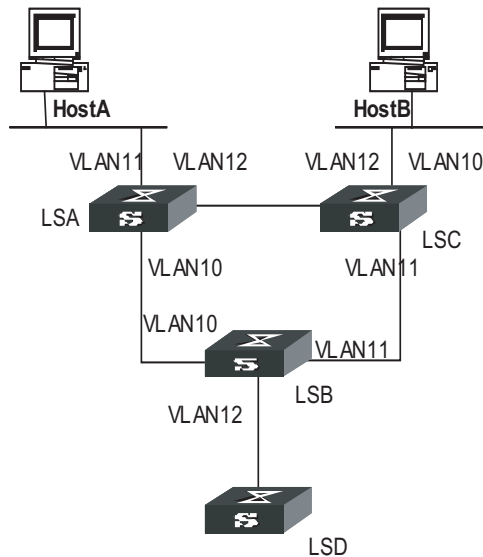
In actual network, we assume that the switches can intercommunicate and the IP address of each interface has been configured.

- LSA is connected to LSB through VLAN-interface10, connected to HostA through VLAN-interface11 and connected to LSC through VLAN-interface12.
- LSB is connected to LSA through VLAN-interface10, connected to LSC through VLAN-interface11 and connected to LSD through VLAN-interface12.
- LSC is connected to HostB through VLAN-interface10, connected to LSB through VLAN-interface11 and connected to LSA through VLAN-interface12.

Suppose that Host A is the receiver of the multicast group at 225.1.1.1. Host B begins transmitting data destined to 225.1.1.1. LSA receives the multicast data from Host B via LSB.

Network diagram

Figure 113 Network diagram for PIM-SM configuration



Configuration procedure

Configure LSA

Enable PIM-SM.

```

<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast routing-enable
[SW8800] vlan 10
[3Com-vlan10] port ethernet 2/1/2 to ethernet 2/1/3
[3Com-vlan10] quit
[SW8800] interface vlan-interface 10
[3Com-vlan-interface10] igmp enable
[3Com-vlan-interface10] pim sm
[3Com-vlan-interface10] quit
[SW8800] vlan 11
[3Com-vlan11] port ethernet 2/1/4 to ethernet 2/1/5
[3Com-vlan11] quit
[SW8800] interface vlan-interface 11
[3Com-vlan-interface11] igmp enable
[3Com-vlan-interface11] pim sm
[3Com-vlan-interface11] quit
[SW8800] vlan 12
[3Com-vlan12] port ethernet 2/1/6 to ethernet 2/1/7
[3Com-vlan12] quit
[SW8800] interface vlan-interface 12
[3Com-vlan-interface12] igmp enable
[3Com-vlan-interface12] pim sm
[3Com-vlan-interface12] quit
  
```

Configure LSB

Enable PIM-SM.

```
[SW8800] multicast routing-enable
[SW8800] vlan 10
[3Com-vlan10] port ethernet 2/1/2 to ethernet 2/1/3
[3Com-vlan10] quit
[SW8800] interface vlan-interface 10
[3Com-vlan-interface10] igmp enable
[3Com-vlan-interface10] pim sm
[3Com-vlan-interface10] quit
[SW8800] vlan 11
[3Com-vlan11] port ethernet 2/1/4 to ethernet 2/1/5
[3Com-vlan11] quit
[SW8800] interface vlan-interface 11
[3Com-vlan-interface11] igmp enable
[3Com-vlan-interface11] pim sm
[3Com-vlan-interface11] quit
[SW8800] vlan 12
[3Com-vlan12] port ethernet 2/1/6 to ethernet 2/1/7
[3Com-vlan12] quit
[SW8800] interface vlan-interface 12
[3Com-vlan-interface12] igmp enable
[3Com-vlan-interface12] pim sm
[3Com-vlan-interface12] quit
```

Configure the C-BSR.

```
[SW8800] pim
[3Com-pim] c-bsr vlan-interface 10 30 2
```

Configure the C-RP.

```
[SW8800] acl number 2000
[3Com-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255
[SW8800] pim
[3Com-pim] c-rp vlan-interface 10 group-policy 2000
```

Configure PIM domain border.

```
[SW8800] interface vlan-interface 12
[3Com-vlan-interface12] pim bsr-boundary
```

After VLAN-interface 12 is configured as domain border, the LSD will be excluded from the local PIM domain and cannot receive the BSR information transmitted from LSB any more.

Configure LSC.

Enable PIM-SM.

```
[SW8800] multicast routing-enable
[SW8800] vlan 10
[3Com-vlan10] port ethernet 2/1/2 to ethernet 2/1/3
[3Com-vlan10] quit
[SW8800] interface vlan-interface 10
[3Com-vlan-interface10] igmp enable
[3Com-vlan-interface10] pim sm
[3Com-vlan-interface10] quit
[SW8800] vlan 11
[3Com-vlan11] port ethernet 2/1/4 to ethernet 2/1/5
```

```
[3Com-vlan11] quit
[SW8800] interface vlan-interface 11
[3Com-vlan-interface11] igmp enable
[3Com-vlan-interface11] pim sm
[3Com-vlan-interface11] quit
[SW8800] vlan 12
[3Com-vlan12] port ethernet 2/1/6 to ethernet 2/1/7
[3Com-vlan12] quit
[SW8800] interface vlan-interface 12
[3Com-vlan-interface12] igmp enable
[3Com-vlan-interface12] pim sm
[3Com-vlan-interface12] quit
```



You should enable PIM-SM on all equal-cost routes if there are any.

MSDP Overview

Introduction No ISP would like to forward multicast traffic depending on the RP of competitors, though it has to obtain information from the source and distribute it among its members, regardless of the location of the multicast source RP. MSDP is proposed to solve this problem. Multicast source discovery protocol (MSDP) describes interconnection mechanism of multiple PIM-SM domains. It is used to discover multicast source information in other PIM-SM domains. MSDP allows the RPs of different domains to share the multicast source information, but all these domains must use PIM-SM as their intro-domain multicast routing protocol.

A RP configured with MSDP peer notifies all of its MSDP peers of the active multicast source message in its domain via SA (Source Active) message. In this way, multicast source information in a PIM-SM domain is transmitted to another PIM-SM domain.

MSDP peer relationship can be established between RPs in different domains or in a same domain, between a RP and a common router, or between common routers. The connection between MSDP peers is TCP connection.

MSDP makes a PIM-SM domain independent of the RP in another PIM-SM domain. After getting multicast source information in that domain, the receiver here can join directly to the SPT of the multicast source in that domain.

Another application of MSDP is Anycast RP. In a domain, configure a certain interface (usually Loopback interface) on different routers with a same IP address; designate these interfaces as C-RPs; and create MSDP peer relationship among them. After the unicast route convergence, the multicast source can select the nearest RP for registration, and the receiver can also select the nearest RP to add into its RPT. The RPs exchange individual registration source information via MSDP peers. Therefore, every RP knows all multicast sources of the entire domain; and every receiver on each RP can receive multicast data from all the multicast sources in the entire domain.

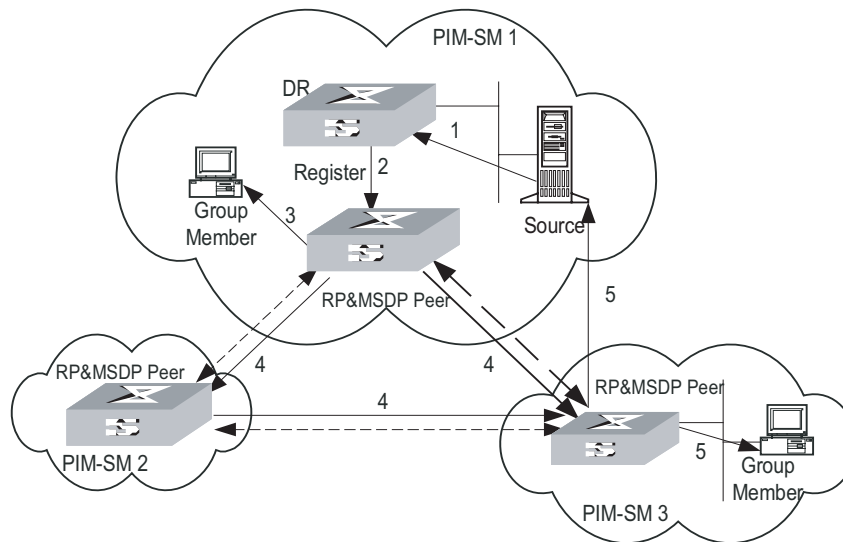
By initiating registration and RPT joining to the nearest RP, MSDP implements RP load sharing. Once an RP turns invalid, its original registered source and receivers will select another nearest RP, implementing redundant RP backup.

In addition, MSDP only accepts the SA messages from the correct paths and excludes redundant SA messages through RPF check mechanism, and prevents the flooding of SA messages among MSDP peers by configuring Mesh Group.

Working Principle Identifying multicast source and receiving multicast data

As shown in Figure 114, the RPs of PIM-SM domains 1, 2 and 3 establish peer relationship between them. Domain 3 contains a group member.

Figure 114 MSDP working principles (I)



When the multicast source in domain 1 sends data to the multicast group, the working process of the member in domain 3, from discovering the multicast source to receiving data from the source, includes the following:

The multicast source in PIM-SM domain 1 begins to send datagram.

The DR connected to the multicast source encapsulates the datagram into a Register packet and forward to the RP in domain 1.

The RP in domain 1 decapsulates the packet and forwards it along the RPT to all the members within the domain. The domain members can choose to take the path along SPT.

The RP in domain 1 generates an SA (Source Active) message for the MSDP peers (the RPs in PIM-SM domain 2 and domain 3). The SA message contains multicast source IP address, multicast group address and the address of the RP that generates the message. Besides, the RP in domain 1 encapsulates the first received multicast data into this SA message.

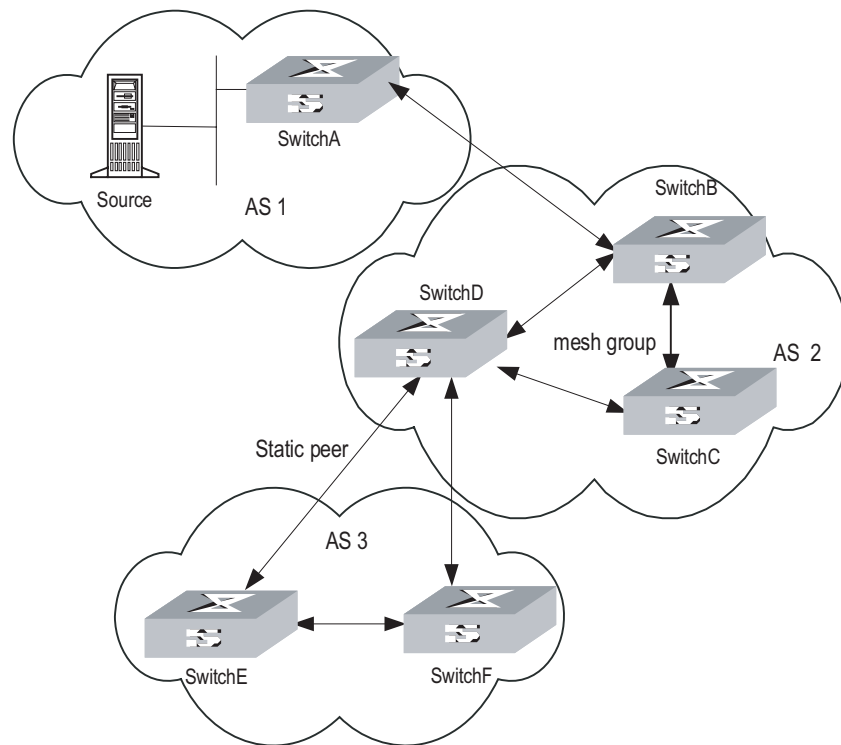
If there is any group member in the domain of an MSDP peer (in the figure, it is PIM-SM domain 3), the RP in this domain sends the multicast data encapsulated in the SA message to group members along the RPT and the join message to multicast source.

After the reverse forwarding path is created, the multicast source data is sent directly to the RP in domain 3, which then RP forwards the data along the RPT. In this case, the last hop router connected with the group member in domain 3 can choose whether to switch to SPT.

Message forwarding and RPF check between MSDP peers

As shown in Figure 115 “MSDP working principles (II)”, Switch A, Switch B, Switch C, Switch D, Switch E and Switch F belong to domain 1, domain 2 and domain 3 respectively. MSDP peer relationship is established between them, indicated with bi-directional arrows in the figure. Among them, Mesh Group is created among Switch B, Switch C and Switch D.

Figure 115 MSDP working principles (II)



The SA message forwarding and RPF check among these MSDP peers are illustrated as follows:

If the SA message is from a MSDP peer that is the RP of the multicast source as from Switch A to Switch B, it is received and forwarded to other peers.

If the SA message is from a MSDP peer that has only one peer as from Switch B to Switch A, it is received.

If the SA message is from a static RPF peer as from Switch D to Switch E, it is received and forwarded to other peers.

If the SA message is from a MSDP peer in Mesh Group as from Switch B to Switch D, it is received and forwarded to the peers outside the Mesh Group.

If the SA message is sent from a MSDP peer in a same domain, and the peer is the next hop along the optimal path to the RP in the domain of source, as in the case when the message is from Switch E to Switch F, it is received and forwarded to other peers.

If the SA message is sent from a MSDP peer in a different domain which is the next autonomous domain along the optimal path to the RP in the domain of source, as from Switch D to Switch F, it is received and forwarded to other peers.

For other SA messages, they are neither received nor forwarded.

Precautions for configuration

The router operating MSDP must also run BGP or MBGP. It is recommended to use the same IP address of the MSDP peer with that of the BGP peer or MBGP peer. If neither BGP nor MBGP is in operation, a static RPF peer should be configured.

MSDP Configuration

Basic configuration tasks of MSDP include

- Enable MSDP
- Configure MSDP peers

Advanced configuration tasks of MSDP include

- Configure static RPF peers
- Configure Originating RP
- Configure SA caching state
- Configure the maximum number of SA caching
- Request the source information of MSDP peers
- Control the source information created
- Control the source information forwarded
- Control the received source information
- Configure MSDP full connection group
- Configure the MSDP connection retry period
- Disable MSDP peers
- Clear MSDP connection, statistics and SA cache

Enabling MSDP

To configure MSDP, you must enable MSDP first.

Please perform the following configurations in system view.

Table 465 Enable MSDP

Operation	Command
Enable MSDP and enter MSDP view	msdp
Clear all MSDP configurations	undo msdp

Configuring MSDP Peers

To run MSDP, you need to configure MSDP peers locally.

Please perform the following configurations in MSDP view.

Table 466 Configure MSDP peers

Operation	Command
Configure MSDP peers	peer <i>peer-address</i> connect-interface <i>interface-type interface-number</i>
Remove MSDP peer configuration	undo peer <i>peer-address</i>
Add description to a MSDP peer	peer <i>peer-address</i> description <i>text</i>
Remove the description	undo peer <i>peer-address</i> description <i>text</i>

The command to add description is optional.

If the local router is also in BGP Peer relation with a MSDP peer, the MSDP peer and the BGP peer should use the same IP address.

Not any two routers between which MSDP peer relationship has been established must run BGP or MBGP, so long as they have a BGP or MBGP route between them. If no BGP or MBGP route exists between them, then you must configure static RPF peers.

Configuring Static RPF Peers

Please perform the following configurations in MSDP view.

Table 467 Configure static RPF peers

Operation	Command
Configure static RPF peers	static-rpf-peer <i>peer-address</i> [rp-policy <i>ip-prefix-name</i>]
Remove static RPF peer configuration	undo static-rpf-peer <i>peer-address</i>

By default, no static RPF peer is configured.



- The **peer** command must be configured before the configuration of **static-rpf-peer** command.
- If only one MSDP peer is configured via the peer command, the MSDP peer will be regarded as the static RPF peer.

To configure multiple static RPF peers at the same time, take any of the two methods:

- Using **rp-policy** parameters universally: Multiple static RPF peers take effect at the same time and SA messages are filtered by the RP addresses contained according to the configured prefix list. If multiple static RPF peers using the same **rp-policy** parameter are configured, any peer that receives an SA message will forward it to the other peers.
- Not using the **rp-policy** parameter universally: According to the configuration sequence, only the first static RPF peer whose connection state is UP is activated. All SA messages from the peer will be received and those from other static RPF peers will be discarded. Once the activated static RPF peer turns invalid (possibly out of configuration removed or connection interrupted), the following first static RPF peer with UP connection state according to the configuration sequence will assume its role.

Configuring Originating RP

During the creation of SA message, an MSDP peer can be configured to use the IP address of a specified interface as the RP address in its SA message.

Please perform the following configurations in MSDP view.

Table 468 Configure Originating RP

Operation	Command
Configure an MSDP peer to use the IP address of a specified interface as the RP address of its SA message	originating-rp <i>interface-type</i> <i>interface-number</i>
Remove the above operation	undo originating-rp

By default, the RP address in SA message is the one configured by PIM.

Configuring SA Caching State

When SA messages are cached on a router, the new join-in groups can directly access all the active sources and join to the corresponding source tree, instead of waiting for the arrival of the next SA message.

Please perform the following configurations in MSDP view.

Table 469 Configure SA caching state

Operation	Command
Configure SA caching state	cache-sa-enable
Disable SA caching state	undo cache-sa-enable

By default, the router caches the SA state, or rather the (S, G) entry when receiving an SA message.

Some memory is consumed as the join delay of groups is shortened by this configuration.

Configuring the Maximum Number of SA caching

To prevent DoS (Deny of Service) attacks, you can set the maximum number of SAs cached on the router.

Perform the following configuration in MSDP view.

Table 470 Configure the maximum number of SA caching

Operation	Command
Configuring the maximum number of SA caching	peer <i>peer-address</i> sa-cache-maximum <i>sa-limit</i>
Restore the default configuration	undo peer <i>peer-address</i> sa-cache-maximum

By default, the maximum number of SA caching is 2048.

Requesting Source Information of MSDP Peers

When a new group joins, the router will send a SA request message to the specified MSDP peer, and the MSDP peer will respond with the SA messages it caches. If the MSDP peer does not enable the SA caching, the configuration is invalid.

Please perform the following configurations in MSDP view.

Table 471 Request source information of MSDP peers

Operation	Command
Configure the router to send SA request message to the specified MSDP peer when receiving the join message of a group	peer <i>peer-address</i> request-sa-enable
Restore the default configuration	undo peer <i>peer-address</i> request-sa-enable

The SA request message sent by a local RP will get the immediate response about all active sources.

By default, the router does not send SA request message to its MSDP peer when receiving the join message of a group. Instead, it waits for the arrival of SA message of the next period.

Controlling the Source Information Created

Filtering the multicast routing entries imported

RP filters the registered sources to control the information of the active sources advertised in SA message. MSDP peers can be configured to only advertise the qualified (S, G) entries in the multicast routing table when creating SA messages, that is, to control the (S,G) entries imported from the multicast routing table to the domain.

Please perform the following configurations in MSDP view.

Table 472 Filter the multicast routing entries imported

Operation	Command
Advertise only the (S, G) entries permitted by the ACL	import-source [<i>acl acl-number</i>]
Remove the above configuration	undo import-source

By default, only intra-domain sources are advertised in SA messages.

If the import-source command without **acl** parameter is executed, no source is advertised in SA messages.

Filtering SA request messages

Please perform the following configurations in MSDP view.

Table 473 Filter SA request messages

Operation	Command
Filter all the SA request messages from a specified MSDP peer	peer <i>peer-address</i> sa-request-policy
Filter the SA request messages of the groups of a specified MSDP peer permitted by the basic ACL from	peer <i>peer-address</i> sa-request-policy <i>acl-number</i>
Remove the configuration of filtering SA request messages	undo peer <i>peer-address</i> sa-request-policy

By default, only the routers which caches SA messages can respond to SA request messages. Routers receive all SA request messages from its MSDP peers.

Multicast group addresses are described in ACL. If no ACL is specified, all SA request messages sent by the corresponding MSDP peer will be ignored. If an ACL is specified, only SA request messages of the groups permitted by the ACL will be processed.

Controlling the Source Information Forwarded

Controlling of source information also includes that of forwarding and receiving source information besides that of creating source information. The outbound filter or time to live (TTL) threshold of SA messages can be used to control the SA message forwarding. By default, all SA messages are forwarded to other MSDP peers.

Using MSDP outbound filter

MSDP outbound filter of are functional in:

- Filtering off all the (S, G) entries
- Forwarding only the SA messages permitted by the advanced ACL

Please perform the following configurations in MSDP view.

Table 474 Use MSDP outbound filter to control the source information forwarded

Operation	Command
Filter off all the SA messages to a specified MSDP peer	peer <i>peer-address</i> sa-policy export
Forward the SA messages permitted by the advanced ACL to a specified MSDP peer	peer <i>peer-address</i> sa-policy export acl <i>acl-number</i>
Remove the filtering over the source information forwarded	undo peer <i>peer-address</i> sa-policy export

Using TTL to filter SA messages with encapsulated data

An SA message with encapsulated data can reach the specified MSDP peer only when the TTL in its IP header is no less than the threshold. Therefore, the forwarding of SA messages with encapsulated data can be controlled by configuring the TTL threshold.

For example, you can set the TTL threshold for intra-domain multicast traffic as 10 if you wish to restrict SA messages with TTL less than or equal to 10 carrying encapsulated data from being propagated. If you set the TTL threshold greater than 10, then they can be propagated to outside.

Please perform the following configurations in MSDP view.

Table 475 Use TTL to filter SA messages with encapsulated data

Operation	Command
Filter off the multicast data encapsulated in the first SA message aiming at a specified MSDP peer	peer <i>peer-address</i> minimum-ttl <i>tth</i>
Remove the TTL threshold configuration	undo peer <i>peer-address</i> minimum-ttl

The default value of TTL threshold is 0.

Controlling the Received Source Information

Please perform the following configurations in MSDP view.

Table 476 Control the received source information

Operation	Command
Filter off the SA messages from a specified MSDP peer	peer <i>peer-address</i> sa-policy import
Receive the SA messages permitted by the advanced ACL from a specified MSDP peer	peer <i>peer-address</i> sa-policy import acl <i>acl-number</i>
Remove the filtering rule over received source information	undo peer <i>peer-address</i> sa-policy import

Similar to MSDP outbound filter in function, MSDP inbound filter controls the received SA messages. By default, the SA messages from all peers are accepted.

Configuring MSDP Mesh Group

Mesh Group is useful when full connection among MSDP peers is required but SA message flooding shall be prevented.

In a Mesh group, the SA messages from outside the group are forwarded to other members in the group, but the SA messages from peers inside the group will not be performed with Peer-RPF check or forwarded in the group. In this case, the overflow of SA messages is avoided and Peer-RPF is simplified, as BGP or MBGP is not required between MSDP peers.

Please perform the following configurations in MSDP view.

Table 477 Configure MSDP full connection group

Operation	Command
Configure an MSDP peer to be a member of an MSDP Mesh Group	peer <i>peer-address</i> mesh-group <i>name</i>
Delete that member from the Group	undo peer <i>peer-address</i> mesh-group <i>name</i>

If an MSDP peer is configured into different mesh groups, only the last configuration is valid.

Configuring the MSDP Connection Retry Period

Perform the following configurations in MSDP view.

Table 478 Configure the MSDP connection retry period

Operation	Command
Configuring the MSDP connection retry period	timer retry <i>seconds</i>
Restore the default value of MSDP connection retry interval	undo timer retry

By default, MSDP connection is retried at the interval of 30 seconds.

Shutting MSDP Peers Down

The session between MSDP peers can be cut off and re-activated as needed.

If a session between MSDP peers is cut off, the TCP connection will terminate with no retry effort, but the configuration information will be reserved.

Please perform the following configurations in MSDP view.

Table 479 Shut MSDP peers down

Operation	Command
Shut a specified MSDP peer down	shutdown <i>peer-address</i>
Turn the MSDP peer up	undo shutdown <i>peer-address</i>

By default, MSDP peer is enabled.

Clearing MSDP Connections, Statistics and SA Caching Configuration

Perform the following configurations in user view.

Table 480 Clear MSDP connections, statistics and SA caching configuration

Operation	Command
Clear a specified TCP connection and reset the counters of all MSDP information	reset msdp peer <i>peer-address</i>
Clear MSDP peer statistics	reset msdp statistics [<i>peer-address</i>]
Clear cached SA entries of MSDP	reset msdp sa-cache [<i>group-address</i>]

Displaying and Debugging MSDP

Displaying and Debugging MSDP

After the above configuration, execute **display** commands in any view to display the running information of MSDP and to verify the effect of the configuration.

Execute the **debugging** command in user view for the debugging of MSDP.

Table 481 Display and debug MSDP configuration

Operation	Command
Display the numbers of sources and groups of SA messages from a specified autonomous domain	display msdp sa-count [<i>as-number</i>]
Display the details of a MSDP peer	display msdp peer-status [<i>peer-address</i>]
Display the (S,G) state learnt from MSDP peer	display msdp sa-cache [<i>group-address</i> <i>source-address</i> <i>autonomous-system-number</i>] *
Display MSDP peer state	display msdp brief
Enable MSDP debugging	debugging msdp { all connect event packet source-active }



CAUTION: The **display msdp sa-count** command give output only after the **cache-sa-enable** command is executed.

Tracing the Transmission Path of SA Messages on the Network

The **msdp-tracert** command can be used in any view to trace the network path of multicast data from multicast source to destination receiver and locate faults.

Table 482 Trace the transmission path of SA messages on the network

Operation	Command
Trace the transmission path of SA messages on the network	msdp-tracert { <i>source-address</i> } { <i>group-address</i> } { <i>rp-address</i> } [max-hops <i>max-hops</i>] [next-hop-info] [sa-info] [peer-info] [skip-hops <i>skip-hops</i>]

Locating information loss and reducing configuration faults can be realized by tracing the network path of the specified (S, G, RP) entries. After the transmission path of SA messages is determined, the overflow of SA messages can be avoided by the correct configuration.

MSDP Configuration Examples

Configuring Static RPF Peers

Network requirements

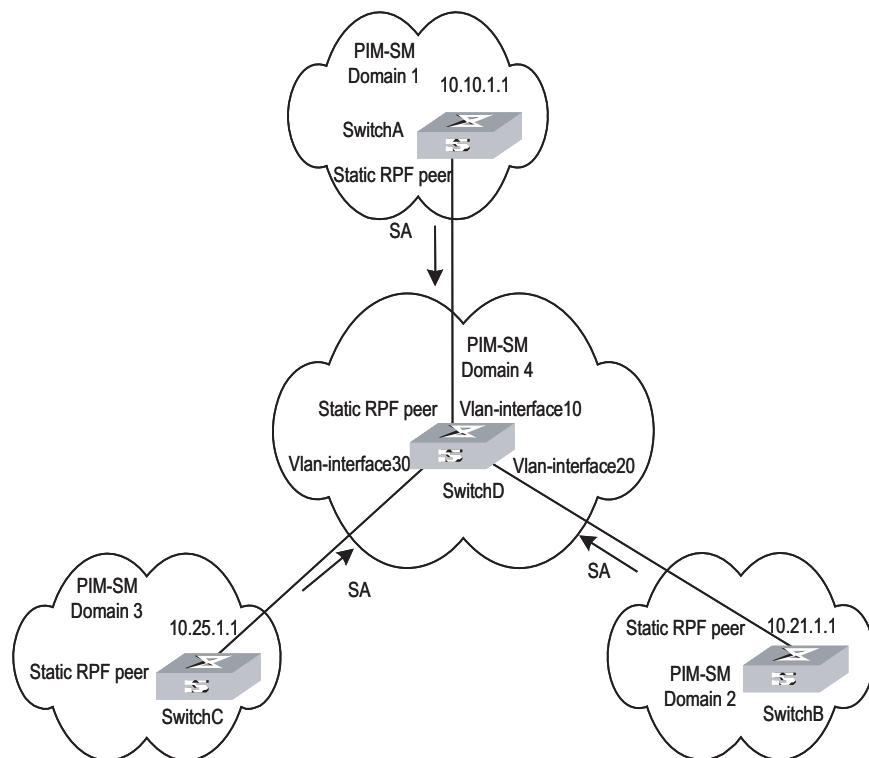
In the following network environment shown in Figure 9-3, four 3Com Switch 8800 Family series routing switches are in the different PIM-SM domains with no BGP or MBGP running among them.

To enable Switch D to receive the specified source information from PIM-SM domains 1, 2 and 3, you can configure static RPF peers with the parameter **rp-policy**.

After the configuration is complete, Switch D will only receive SA messages permitted by the corresponding filtering policy from its static RPF peers.

Network diagram

Figure 116 Configuring static RPF peers



Configuration procedure

The following configuration is made on Switch D.

```
# Configure Switch A to be a static RPF peer of Switch D.
```

```

<SwitchD> system-view
System View: return to User View with Ctrl+Z.
[SwitchD] ip ip-prefix list-a permit 10.10.0.0 16
[SwitchD] msdp
[SwitchD-msdp] peer 10.10.1.1 connect-interface Vlan-interface 10
[SwitchD-msdp] static-rpf-peer 10.10.1.1 rp-policy list-a
[SwitchD-msdp] quit

```

Configure Switch B to be a static RPF peer of Switch D.

```

[SwitchD] ip ip-prefix list-b permit 10.21.0.0 16
[SwitchD] msdp
[SwitchD-msdp] peer 10.21.1.1 connect-interface Vlan-interface 20
[SwitchD-msdp] static-rpf-peer 10.21.1.1 rp-policy list-b
[SwitchD-msdp] quit

```

Configure Switch C to be a static RPF peer of Switch D.

```

[SwitchD] ip ip-prefix list-c permit 10.25.0.0 16
[SwitchD] msdp
[SwitchD-msdp] peer 10.25.1.1 connect-interface Vlan-interface30
[SwitchD-msdp] static-rpf-peer 10.25.1.1 rp-policy list-c

```

Configuring Anycast RP Network requirements

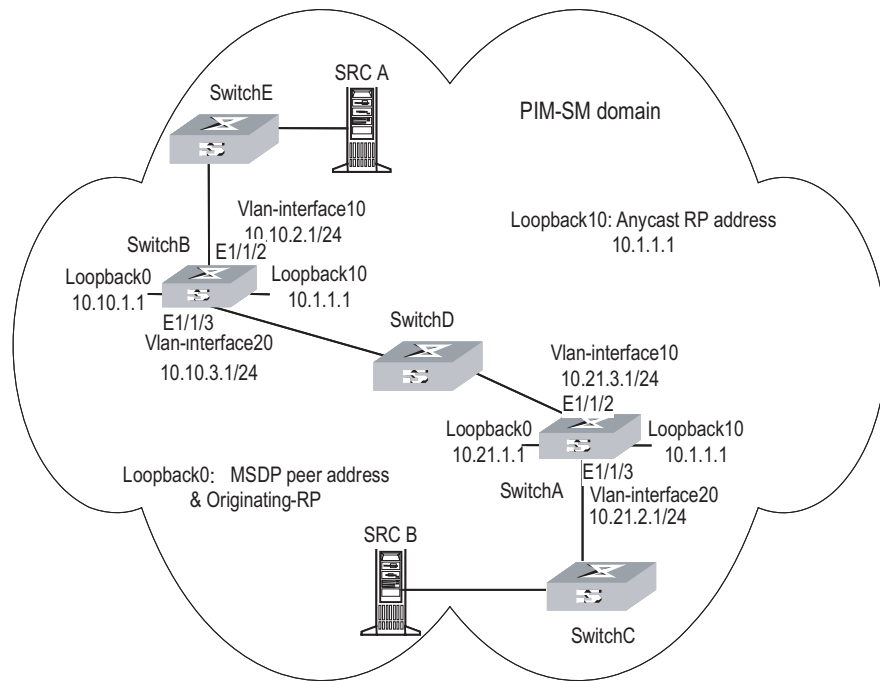
To configure Anycast RP in the PIM-SM domain, establish MSDP peer relationship between Switch A and Switch B; use the address of loopback0 on Switch A and Switch B to send SA messages outside; set Loopback10 interface on Switch A and Switch B as BSR/RP and configure the Anycast RP address. In this way, when a unicast group member joins, the switch directly connected to the host can originate a join message to the nearest RP in the topology.



This example focuses on the configuration of Switch A and Switch B. Configuration performed on Switch E, Switch D and Switch C is omitted as it mainly concerns enabling multicast and enabling PIM-SM on the interfaces.

Network diagram

Figure 117 Network diagram for Anycast RP configuration



Configuration procedure

1 Configure SwitchB:

Configure VLAN

```
<SwitchB> system-view
System View: return to User View with Ctrl+Z.
[SwitchB] vlan 10
[SwitchB-vlan10] port ethernet1/1/2
[SwitchB-vlan10] quit
[SwitchB] vlan 20
[SwitchB-vlan20] port ethernet1/1/3
[SwitchB-vlan20] quit
```

Enable multicast.

```
[SwitchB] multicast routing-enable
```

Configure the IP address of interface loopback0.

```
[SwitchB] interface loopback0
[SwitchB-LoopBack0] ip address 10.10.1.1 255.255.255.255
[SwitchB-LoopBack0] quit
```

Configure the IP address of interface loopback10 and enable IGMP and PIM-SM.

```
[SwitchB] interface loopback10
[SwitchB-LoopBack10] ip address 10.1.1.1 255.255.255.255
[SwitchB-LoopBack10] igmp enable
```

```
[SwitchB-LoopBack10] pim sm
[SwitchB-LoopBack10] quit
```

Configure the IP address of Vlan-interface10 and enable IGMP and PIM-SM.

```
[SwitchB] interface Vlan-interface10
[SwitchB-Vlan-interface10] ip address 10.10.2.1 255.255.255.0
[SwitchB-Vlan-interface10] igmp enable
[SwitchB-Vlan-interface10] pim sm
[SwitchB-Vlan-interface10] undo shutdown
[SwitchB-Vlan-interface10] quit
```

Configure the IP address of Vlan-interface20 and enable IGMP and PIM-SM.

```
[SwitchB] interface Vlan-interface20
[SwitchB-Vlan-interface20] ip address 10.10.3.1 255.255.255.0
[SwitchB-Vlan-interface20] igmp enable
[SwitchB-Vlan-interface20] pim sm
[SwitchB-Vlan-interface20] undo shutdown
[SwitchB-Vlan-interface20] quit
```

Configure OSPF

```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.10.2.0 0.255.255.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.10.3.0 0.255.255.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 10.10.1.1 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configure Switch A as its MSDP peer.

```
[SwitchB] msdp
[SwitchB-msdp] peer 10.21.1.1 connect-interface loopback 0
```

Configure Originating RP.

```
[SwitchB-msdp] originating-rp loopback0
[SwitchB-msdp] quit
```

Configure C-RP and BSR.

```
[SwitchB] pim
[SwitchB-pim] c-rp loopback 10
[SwitchB-pim] c-bsr loopback 10 30
```

2 Configure Switch A:

Configure VLAN

```
<SwitchA> system-view
System View: return to User View with Ctrl+Z.
[SwitchA] vlan 10
[SwitchA-vlan10] port ethernet1/1/2
[SwitchA-vlan10] quit
[SwitchA] vlan 20
```

```
[SwitchA-vlan20] port ethernet1/1/3
[SwitchA-vlan20] quit
```

Enable multicast.

```
[SwitchA] multicast routing-enable
```

Configure the IP address of interface loopback0.

```
[SwitchA] interface loopback0
[SwitchA-LoopBack0] ip address 10.21.1.1 255.255.255.255
[SwitchA-LoopBack0] quit
```

Configure the IP address of interface loopback10 and enable IGMP and PIM-SM.

```
[SwitchA] interface loopback10
[SwitchA-LoopBack10] ip address 10.1.1.1 255.255.255.255
[SwitchA-LoopBack10] igmp enable
[SwitchA-LoopBack10] pim sm
[SwitchA-LoopBack10] quit
```

Configure the IP address of interface Vlan-interface20 and enable IGMP and PIM-SM.

```
[SwitchA] interface Vlan-interface20
[SwitchA-Vlan-interface20] ip address 10.21.2.1 255.255.255.0
[SwitchA-Vlan-interface20] igmp enable
[SwitchA-Vlan-interface20] pim sm
[SwitchA-Vlan-interface20] undo shutdown
[SwitchA-Vlan-interface20] quit
```

Configure the IP address of Vlan-interface10 and enable IGMP and PIM-SM.

```
[SwitchA] interface Vlan-interface10
[SwitchA-Vlan-interface10] ip address 10.21.3.1 255.255.255.0
[SwitchA-Vlan-interface10] igmp enable
[SwitchA-Vlan-interface10] pim sm
[SwitchA-Vlan-interface10] undo shutdown
[SwitchA-Vlan-interface10] quit
```

Configure OSPF route.

```
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.21.2.0 0.255.255.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.21.3.0 0.255.255.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 10.21.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Configure Switch B as its MSDP peer.

```
[SwitchA] msdp
[SwitchA-msdp] peer 10.10.1.1 connect-interface loopback 0
```

Configure Originating RP.

```
[SwitchA-msdp] originating-rp loopback0
[SwitchA-msdp] quit
```

Configure C-RP and BSR.

```
[SwitchA] pim
[SwitchA-pim] c-rp loopback 10
[SwitchA-pim] c-bsr loopback 10 30
```

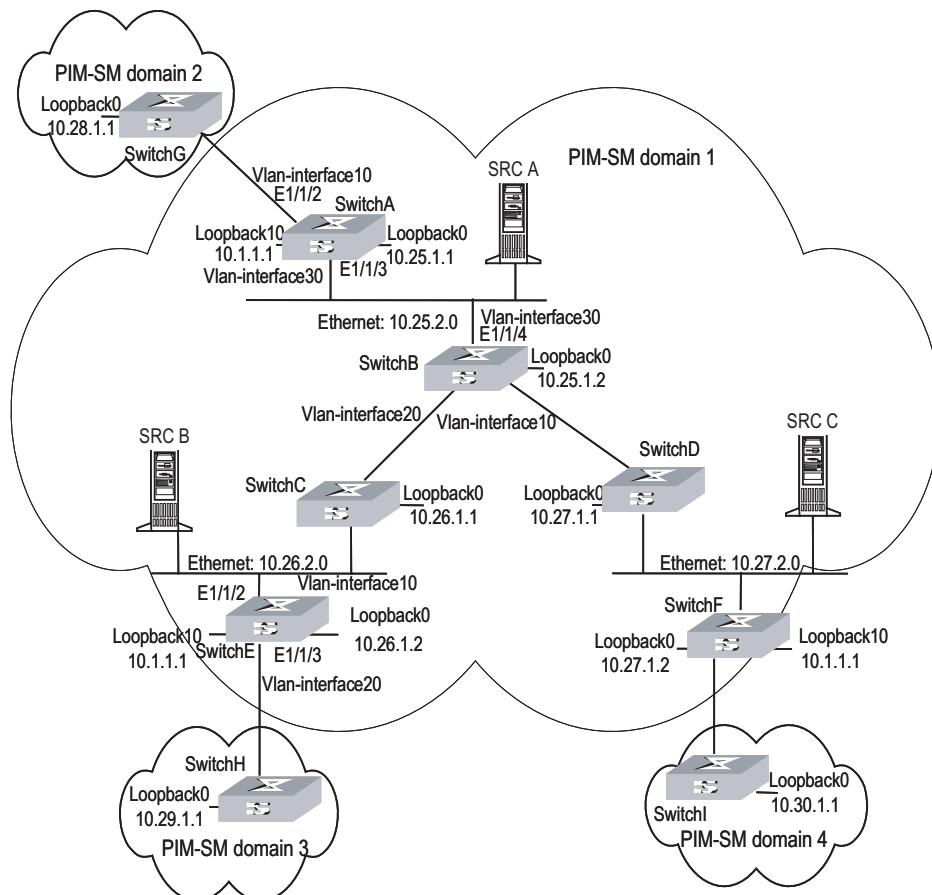
MSDP Integrated Networking

Network requirement

In the following network, enable MSDP and configure an Anycast RP in PIM-SM domain 1; establish MSDP peer relationship among RPs across PIM-SM domains; and use MBGP between domains. For the related commands, refer to 9.4 “MBGP Multicast Extension Configuration Example”.

Network diagram

Figure 118 MSDP integrated networking



Configuration procedure



The follow procedure details multicast configuration, but briefs router configuration.

1 Configure Switch A:

Configuring VLAN


```

<SwitchA> system-view
System View: return to User View with Ctrl+Z.
[SwitchA] vlan 10
[SwitchA-vlan10] port ethernet1/1/2
[SwitchA-vlan10] quit
[SwitchA] vlan 30
[SwitchA-vlan30] port ethernet1/1/3
[SwitchA-vlan30] quit

# Enable multicast.

[SwitchA] multicast routing-enable

# Configure the IP address of interface loopback0 and enable PIM-SM.

[SwitchA] interface loopback0
[SwitchA-LoopBack0] ip address 10.25.1.1 255.255.255.255
[SwitchA-LoopBack0] pim sm
[SwitchA-LoopBack0] quit

# Configure the IP address of interface loopback10 and enable PIM-SM.

[SwitchA] interface loopback10
[SwitchA-LoopBack10] ip address 10.1.1.1 255.255.255.255
[SwitchA-LoopBack10] pim sm
[SwitchA-LoopBack10] quit

# Configure the IP address of Vlan-interface30 and enable IGMP and PIM-SM.

[SwitchA] interface Vlan-interface30
[SwitchA-Vlan-interface30] ip address 10.25.2.3 255.255.255.0
[SwitchA-Vlan-interface30] igmp enable
[SwitchA-Vlan-interface30] pim sm
[SwitchA-Vlan-interface30] undo shutdown
[SwitchA-Vlan-interface30] quit

# Configure the IP address of Vlan-interface10 and enable IGMP and PIM-SM.

[SwitchA] interface Vlan-interface10
[SwitchA-Vlan-interface10] ip address 10.25.3.1 255.255.255.0
[SwitchA-Vlan-interface10] igmp enable
[SwitchA-Vlan-interface10] pim sm
[SwitchA-Vlan-interface10] undo shutdown
[SwitchA-Vlan-interface10] quit

# Configure OSPF

[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.25.2.0 0.255.255.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 10.25.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit

# Configure BGP.

```

```

[SwitchA] bgp 100
[SwitchA-bgp] undo synchronization
[SwitchA-bgp] group in internal
[SwitchA-bgp] peer 10.26.1.2 group in
[SwitchA-bgp] peer 10.27.1.2 group in
[SwitchA-bgp] peer in connect-interface loopback0
[SwitchA-bgp] ipv4-family multicast
[SwitchA-bgp-af-mul] peer in enable
[SwitchA-bgp-af-mul] peer 10.26.1.2 group in
[SwitchA-bgp-af-mul] peer 10.27.1.2 group in
[SwitchA-bgp-af-mul] peer in next-hop-local
[SwitchA-bgp-af-mul] quit
[SwitchA-bgp] group ex external
[SwitchA-bgp] peer 10.28.1.1 group ex as-number 200
[SwitchA-bgp] peer ex next-hop-local
[SwitchA-bgp] peer ex default-route-advertise
[SwitchA-bgp] ipv4-family multicast
[SwitchA-bgp-af-mul] peer ex enable
[SwitchA-bgp-af-mul] peer 10.28.1.1 group ex
[SwitchA-bgp-af-mul] peer ex next-hop-local
[SwitchA-bgp-af-mul] quit
[SwitchA-bgp] quit

```

Configure MSDP peer, Mess Group and Originating RP.

```

[SwitchA] msdp
[SwitchA-msdp] peer 10.28.1.1 connect-interface loopback 0
[SwitchA-msdp] peer 10.26.1.2 connect-interface loopback 0
[SwitchA-msdp] peer 10.27.1.2 connect-interface loopback 0
[SwitchA-msdp] peer 10.26.1.2 mesh-group net
[SwitchA-msdp] peer 10.27.1.2 mesh-group net
[SwitchA-msdp] originating-rp loopback0
[SwitchA-msdp] quit

```

Configuring C-RP and BSR.

```

[SwitchA] pim
[SwitchA-pim] c-rp loopback 10
[SwitchA-pim] c-bsr loopback 0 30

```

2 Configure Switch E:

Configuring VLAN

```

<SwitchE> system-view
System View: return to User View with Ctrl+Z.
[SwitchE] vlan 10
[SwitchE-vlan10] port ethernet1/1/2
[SwitchE-vlan10] quit
[SwitchE] vlan 20
[SwitchE-vlan20] port ethernet1/1/3
[SwitchE-vlan20] quit

```

Enable multicast.

```

[SwitchE] multicast routing-enable

```

Configure the IP address of interface loopback0 and enable PIM-SM.

```
[SwitchE] interface loopback0
[SwitchE-LoopBack0] ip address 10.26.1.2 255.255.255.255
[SwitchE-LoopBack0] pim sm
[SwitchE-LoopBack0] quit
```

Configure the IP address of interface loopback10 and enable PIM-SM.

```
[SwitchE] interface loopback10
[SwitchE-LoopBack10] ip address 10.1.1.1 255.255.255.255
[SwitchE-LoopBack10] pim sm
[SwitchE-LoopBack10] quit
```

Configure the IP address of Vlan-interface10 and enable IGMP and PIM-SM.

```
[SwitchE] interface Vlan-interface10
[SwitchE-Vlan-interface10] ip address 10.26.2.3 255.255.255.0
[SwitchE-Vlan-interface10] igmp enable
[SwitchE-Vlan-interface10] pim sm
[SwitchE-Vlan-interface10] undo shutdown
[SwitchE-Vlan-interface10] quit
```

Configure the IP address of Vlan-interface20 and enable IGMP and PIM-SM.

```
[SwitchE] interface Vlan-interface20
[SwitchE-Vlan-interface20] ip address 10.26.3.1 255.255.255.0
[SwitchE-Vlan-interface20] igmp enable
[SwitchE-Vlan-interface20] pim sm
[SwitchE-Vlan-interface20] undo shutdown
[SwitchE-Vlan-interface20] quit
```

Configuring OSPF

```
[SwitchE] ospf
[SwitchE-ospf-1] area 0
[SwitchE-ospf-1-area-0.0.0.0] network 10.26.2.0 0.255.255.255
[SwitchE-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.0
[SwitchE-ospf-1-area-0.0.0.0] network 10.26.1.2 0.0.0.0
[SwitchE-ospf-1-area-0.0.0.0] quit
[SwitchE-ospf-1] quit
```

Configure BGP.

```
[SwitchE] bgp 100
[SwitchE-bgp] undo synchronization
[SwitchE-bgp] group in internal
[SwitchE-bgp] peer 10.25.1.1 group in
[SwitchE-bgp] peer 10.27.1.2 group in
[SwitchE-bgp] peer in connect-interface loopback0
[SwitchE-bgp] ipv4-family multicast
[SwitchE-bgp-af-mul] peer in enable
[SwitchE-bgp-af-mul] peer 10.25.1.1 group in
[SwitchE-bgp-af-mul] peer 10.27.1.2 group in
[SwitchE-bgp-af-mul] peer in next-hop-local
[SwitchE-bgp-af-mul] quit
[SwitchE-bgp] group ex external
[SwitchE-bgp] peer 10.29.1.1 group ex as-number 300
[SwitchE-bgp] peer ex default-route-advertise
[SwitchE-bgp] peer ex ebgp-max-hop 255
```

```
[SwitchE-bgp] ipv4-family multicast
[SwitchE-bgp-af-mul] peer ex enable
[SwitchE-bgp-af-mul] peer 10.29.1.1 group ex
[SwitchE-bgp-af-mul] peer ex next-hop-local
[SwitchE-bgp-af-mul] quit
[SwitchE-bgp] quit
```

Configure MSDP peer, Mess Group and Originating RP.

```
[SwitchE] msdp
[SwitchE-msdp] peer 10.29.1.1 connect-interface loopback 0
[SwitchE-msdp] static-rpf-peer 10.29.1.1
[SwitchE-msdp] peer 10.25.1.1 connect-interface loopback 0
[SwitchE-msdp] peer 10.27.1.2 connect-interface loopback 0
[SwitchE-msdp] peer 10.25.1.1 mesh-group net
[SwitchE-msdp] peer 10.27.1.2 mesh-group net
[SwitchE-msdp] originating-rp loopback0
[SwitchE-msdp] quit
[SwitchE] ip route-static 10.29.1.1 255.255.255.0 Vlan-interface20
```

Configure C-RP and BSR.

```
[SwitchE] pim
[SwitchE-pim] c-rp loopback 10
[SwitchE-pim] c-bsr loopback 0 30
```



The configuration on the switches other than SwitchA and SwitchE is omitted here.

46

MBGP MULTICAST EXTENSION CONFIGURATION

MBGP Multicast Extension Overview

Introduction At present, the most widely used inter-domain unicast routing protocol is BGP-4. Because the multicast topology may be different from the unicast topology, BGP-4 must be modified in order to implement the transmission of inter-domain multicast routing information. Some routers in the network may only support unicast rather than multicast and may not forward multicast packets since the particular policy requires that. To construct inter-domain multicast routing trees, you need to know the unicast routing information as well as the information of multicast-supporting parts of the network, namely, the multicast network topology.

BGP-4 has been proved to be an effective and stable inter-domain unicast routing protocol. Therefore, it is more rational to enhance and extend the BGP-4 protocol than to construct a new protocol. RFC2858 provisions the multi-protocol extension method for BGP. The extended BGP (MBGP, also written as BGP-4+) can not only carry IPv4 unicast routing information but also the routing information of other network layer protocols (such as multicast, IPv6). Carrying multicast routing information is only one of the extended functions.

MBGP enables unicast and multicast routing information to be exchanged through the same process but stored in different routing tables. As MBGP is an enhanced version of BGP-4, all the common policies and configuration methods that BGP-4 supports can be applied to multicast.

This chapter describes mainly MBGP extension for multicast.

MBGP Extension Attributes for Multicast To make MBGP support multicast, RFC2858 defines two new route attributes in the UPDATE message: MP_REACH_NLRI (multiprotocol reachable NLRI) and MP_UNREACH_NLRI (multiprotocol unreachable NLRI). They are all optional non-transitive attributes, that is, routers that do not support MBGP can ignore the information in the attributes and not forward the attributes.

Among the information carried by MP_REACH_NLRI and MP_UNREACH_NLRI, AFI (Address Family Identifier) and SAFI (Subsequent Address Family Identifier) can identify for which address family the information is. SAFI is a complement to NLRI (Network Layer Reachability Information), with value 1 for the unicast mode of NLRI, and value 2 for the multicast mode of NLRI.

MP_REACH_NLRI attribute

MP_REACH_NLRI is an optional non-transitive attribute, and can be used to:

- Send the routing information of a new reachable protocol.
- Send the next hop information about the new protocol with the same coding mode as that of NLRI.
- Enable the router to report part or all of the SNPAs (Sub-network Points of Attachment) saved in the local system.

MP_UNREACH_NLRI attribute

The MP_UNREACH_NLRI is an optional non-transitive attribute that can be used for the purpose of withdrawing one or multiple unfeasible routes from service. It includes the following fields:

- AFI and SAFI.
- Withdrawn Routes: Contains one or multiple NLRIs, in which are the unreachable destination addresses.

An UPDATE packet that contains the MP_UNREACH_NLRI is not required to carry any other path attributes.

These two attributes enables MBGP to carry multi-protocol information. MSBP therefore supports both unicast and multicast by constructing different topology maps to implement appropriate policies. Besides, MBGP may construct different inter-domain routes for unicast and multicast under a same policy.

MBGP Operating Mode and Message Type

MBGP runs on a router in the following two modes:

- IBGP (Internal BGP)
- EBGP (External BGP)

MBGP running in an autonomous system is called IBGP; MBGP running across autonomous systems is called EBGP.

MBGP offers four types of messages:

- Open Message: the first message sent after the TCP connection is established.
- Notification Message: error notification message.
- Keepalive Message: Message used to check the validity of the connection.
- Update Message: the most important information in the MBGP system, used to exchange routing information among peers. It consists of three parts at the most: MP_UNREACH_NLRI, Path Attributes and MP_REACH_NLRI.

MBGP Multicast Extension Configuration

Basic configuration tasks of MBGP multicast extension include

- Enable MBGP multicast extension protocol
- Specify the network routes notified by the MBGP multicast extension

Advanced configuration tasks of MBGP multicast extension include

- Configure the MED value for an AS
- Compare MED values from different AS neighbor paths
- Configure local preference

- Configure MBGP timer
- Configure MBGP Peer (group)
- Configure MBGP route aggregation
- Configure an MBGP route reflector
- Configure the MBGP community attributes
- Configure the interaction between MBGP and IGP
- Define AS path list and routing policy
- Configure MBGP route filtering
- Reset BGP connections



Only configuration tasks in IPv4 multicast sub-address family view are detailed below. Other tasks configured in BGP or system view are only briefed. For the detailed configuration, refer to the BGP Configuration and IP Routing policy sections of the Routing Protocol part.

Enabling MBGP Multicast Extension Protocol

To enable the MBGP multicast extension protocol, enter the IPv4 multicast sub-address family view.

A router does not start receiving MBGP connection requests instantly after the MBGP multicast extension protocol is enabled. To activate a router to originate MBGP connection requests to neighboring routers, refer to the **neighbor** configuration. Perform the following configuration in BGP view.

Table 483 Enable MBGP multicast extension protocol

Operation	Command
Enter the MBGP multicast address family view	ipv4-family multicast
Remove the MBGP multicast address family view	undo ipv4-family multicast

By default, the system does not run the MBGP multicast extension protocol.

Specifying Network Routes Notified by MBGP Multicast Extension

The **network** command is used to specify the network routes to be advertised to MBGP peers, as well as the mask and route policy of this network route.

Perform the following configurations in IPV4 multicast sub-address family view.

Table 484 Specify network routes notified by MBGP multicast extension

Operation	Command
Configure the network routes to be advertised by the local MBGP	network <i>ip-address</i> [<i>address-mask</i>] [route-policy <i>route-policy-name</i>]
Remove the network routes to be advertised by the local MBGP	undo network <i>ip-address</i> [<i>address-mask</i>] [route-policy <i>route-policy-name</i>]

By default, no route is advertised by the local MBGP.

The **network** command advertises only the precisely matched route, the one with prefix and mask completely conforming to the configuration. If no mask is specified, match goes by the natural network segment.

Configuring the MED Value for an AS

The MED configured in BGP view is valid for both unicast and multicast.

For the details of this configuration, refer to "BGP Configuration" of the Routing Protocol part.

Comparing MED Values from Different AS Neighbor Paths

Do not use this configuration unless you are sure that different ASs adopt the same IGP and route selection method. The configuration in BGP view works both in unicast and multicast.

For the details of this configuration, refer to "BGP Configuration" of the Routing Protocol part.

Configuring Local Preference

Different local preference can be configured as a reference of the MBGP route selection. When an MBGP router gets routes with the same destination but different next hops through different neighbors, it will choose the route with the highest local preference.

The configuration works both in unicast and multicast.

For the details of this configuration, refer to "BGP Configuration" of the Routing Protocol part.

Configuring MBGP Timer

After a router establishes MBGP connection with a peer, it sends Keepalive messages to the peer periodically to check for the smooth connection. If the router does not receive a single Keepalive message or any other kind of message from the peer within the defined connection Holdtime, it will think the MBGP connection broken and exit, and will process the routing information received through this connection as appropriate. Therefore, the Keepalive message sending interval and MBGP connection Holdtime are two parameters of great importance in MBGP mechanism.

The configuration works both in unicast and multicast.

For the details of this configuration, refer to "BGP Configuration" of the Routing Protocol part.

Configuring MBGP Peer (Group)

The use of MBGP peer groups is to simplify configuration. When configuring MBGP peers, you can create and configure a peer group in BGP view, and then add the peers into the group, since all peers in a group have the same configuration with the group. Then, enable this peer group in IPv4 multicast sub-address family view and add peers to this peer group to create MBGP peers and an MBGP peer group. In conclusion, to create MBGP peers/peer groups, you must configure them successfully in BGP view first.



CAUTION: Configure the peer group under the guide of technical support engineers.

Creating a peer group with members

To configure a MBGP peer (group), configure a peer group in BGP view and add peers to this peer group. For details, refer to "BGP Configuration" in the Routing Protocol part.

Enabling a peer (group)

Please perform the following configurations in IPv4 multicast sub-address family view.

Table 485 Enable a peer (group)

Operation	Command
Enable the specified peer (group)	peer group-name enable
Disable the specified peer (group)	undo peer group-name enable

Adding an MBGP peer to the group

Please perform the following configurations in IPv4 multicast sub-address family view.

Table 486 Add an MBGP peer to the group

Operation	Command
Add an MBGP peer to the group	peer peer-address group group-name
Delete the MBGP peer	undo peer peer-address

Advertising MBGP community attributes to a peer (group)

Please perform the following configurations in IPv4 multicast sub-address family view.

Table 487 Configure to advertise the community attributes to a peer (group)

Operation	Command
Advertise the community attributes to a peer (group)	peer group-name advertise-community
Configure not to advertise the community attributes to a peer (group)	undo peer group-name advertise-community

By default, no community attribute is advertised to any peer (group).

Configuring a peer (group) as an MBGP route reflector client

Please perform the following configurations in IPv4 multicast sub-address family view.

Table 488 Configure a peer (group) as an MBGP route reflector client

Operation	Command
Configure a peer (group) as an MBGP route reflector client	peer group-name reflect-client
Remove the above configuration	undo peer group-name reflect-client

By default, there is no route reflector in an AS.

It is generally unnecessary to configure this command for a peer group. This command is reserved for the occasional compatibility with the network equipments of other vendors.

Configuring the local address as the next hop when advertising routes

This involves removing the next hop configuration in the routing information advertised to a peer (group) and configuring the local address as the next hop address. It is valid only for IBGP peers/peer groups.

Please perform the following configurations in IPV4 multicast sub-address family view.

Table 489 Configure the local address as the next hop when advertising routes

Operation	Command
Configure the local address as the next hop when advertising routing information	peer <i>group-name</i> next-hop-local
Remove the above configuration	undo peer <i>group-name</i> next-hop-local

Specifying the routing policy for a peer (group)

Please perform the following configurations in IPV4 multicast sub-address family view.

Table 490 Specify the routing policy for a peer (group)

Operation	Command
Configure routing policy for incoming packets	peer { <i>group-name</i> <i>peer-address</i> } route-policy <i>policy-name</i> import
Remove incoming policy configuration	undo peer { <i>group-name</i> <i>peer-address</i> } route-policy <i>policy-name</i> import
Configure routing policy for outgoing packets	peer <i>group-name</i> route-policy <i>policy-name</i> export
Remove outgoing policy configuration	undo peer <i>group-name</i> route-policy <i>policy-name</i> export

By default, no routing policy is specified for any peer (group).

Configuring IP-ACL-based route filtering policy for a peer (group)

Please perform the following configurations in IPV4 multicast sub-address family view.

Table 491 Configure IP-ACL-based route filtering policy for a peer (group)

Operation	Command
Configure filtering policy for incoming packets	peer { <i>group-name</i> <i>peer-address</i> } filter-policy <i>acl-number</i> import
Remove incoming policy configuration	undo peer { <i>group-name</i> <i>peer-address</i> } filter-policy <i>acl-number</i> import
Configure routing policy for outgoing packets	peer <i>group-name</i> filter-policy <i>acl-number</i> export
Remove outgoing policy configuration	undo peer <i>group-name</i> filter-policy <i>acl-number</i> export

By default, a peer (group) does not perform route filtering based on the IP ACL.

Configuring AS-path-list-based route filtering policy for a peer (group)

Please perform the following configurations in IPV4 multicast sub-address family view.

Table 492 Configuring the AS-path-list-based route filtering policy for a peer (group)

Operation	Command
Configure filtering policy for incoming packets	peer { <i>group-name</i> <i>peer-address</i> } as-path-acl <i>acl-number</i> import
Remove incoming policy configuration	undo peer { <i>group-name</i> <i>peer-address</i> } as-path-acl <i>acl-number</i> import
Configure routing policy for outgoing packets	peer { <i>group-name</i> <i>peer-address</i> } as-path-acl <i>acl-number</i> export
Remove outgoing policy configuration	undo peer { <i>group-name</i> <i>peer-address</i> } as-path-acl <i>acl-number</i> export

By default, a peer (group) does not perform route filtering based on the AS path list.

Configuring prefix-list-based route filtering policy for a peer (group)

Please perform the following configurations in IPv4 multicast sub-address family view.

Table 493 Configure prefix-list-based route filtering policy for a peer (group)

Operation	Command
Configure filtering policy for incoming packets	peer { <i>group-name</i> <i>peer-address</i> } ip-prefix <i>prefixname</i> import
Remove incoming policy configuration	undo peer { <i>group-name</i> <i>peer-address</i> } ip-prefix <i>prefixname</i> import
Configure routing policy for outgoing packets	peer { <i>group-name</i> } ip-prefix <i>prefixname</i> export
Remove outgoing policy configuration	undo peer <i>group-name</i> ip-prefix <i>prefixname</i> export

By default, a peer (group) does not perform route filtering based on the prefix list.

Configuring MBGP Route Aggregation

MBGP supports the manual aggregation of routes. Manual aggregation aggregates the local MBGP routes. A series of parameters can be configured during manual route aggregation.

Please perform the following configurations in IPv4 multicast sub-address family view.

Table 494 Configure MBGP route aggregation

Operation	Command
Configure the aggregation of local routes	aggregate <i>address mask</i> [as-set attribute-policy <i>route-policy-name</i> detail-suppressed origin-policy <i>route-policy-name</i> suppress-policy <i>route-policy-name</i>]*
Remove the aggregation of local routes	undo aggregate <i>address mask</i> [as-set attribute-policy <i>route-policy-name</i> detail-suppressed origin-policy <i>route-policy-name</i> suppress-policy <i>route-policy-name</i>]*

By default, MBGP does not aggregate local routes.

Configuring an MBGP Route Reflector

To ensure the interconnectivity among MBGP peers, it is necessary to establish fully-closed network among IBGP multicast peers. However, some internal MBGP

multicast networks are very large, and it costs a good sum to establish a fully-closed network.

Route reflector solves this problem. The core is to specify a router as the focus of the internal sessions. Multiple MBGP multicast routers can be peers of one central point, namely a multiple route reflector, which in turn creates peer relationship with other reflectors. The route reflector is the focus of other routers. The routers other than those reflectors are called clients. The clients are in peer with route reflects and exchange routing information with them. The route reflectors transfer (reflect) information between the clients in turn.

For the details of the principles and configurations, refer to "BGP Configuration" of the Routing Protocol part.

Configure MBGP Community Attributes

Within the MBGP, a community is a set of destinations with some characteristics in common. A community is not limited to a network or an AS has no physical boundary.

For details, refer to "BGP Configuration" in the Routing Protocol part.

Importing IGP Routing Information into MBGP

MBGP can advertise intra-area network information to other ASs. To this end, you can use MBGP to advertise the intra-area network information that local router gets through IGP routing protocol.

Please perform the following configurations in IPV4 multicast sub-address family view.

Table 495 Import IGP routing information

Operation	Command
Import IGP Routing Information into MBGP	import-route <i>protocol</i> [route-policy <i>policy-name</i>] [med <i>med-value</i>]
Delete the imported IGP routing information	undo import-route <i>protocol</i>

By default, MBGP does not import any route of other protocols.

Parameter *Protocol* specifies the source routing protocols of import, which can be direct, static, rip, isis, ospf, ospf-ase or ospf-nssa at present.

Defining AS Path List and Routing Policy

To configure AS path list and routing polity you need to:

- Configure the regular expression of autonomous systems (in system view);

The UPDATE information of MBGP contains an AS_PATH domain. The autonomous system paths for MBGP routing information exchange is recorded in this domain.

- Define the routing policy (in system view);
- Define matching rules (in routing policy view);
- Define value assigning rules (in routing policy view)

For the detailed configuration of regular expression of AS, refer to "BGP Configuration" of the Routing Protocol part. For other configurations, refer to the "IP Routing Policy Configuration" of the Routing Protocol part.

Configuring MBGP Route Filtering

The route filtering configuration of MBGP is the same as that of unicast BGP.

For details, refer to "BGP Configuration" of the Routing Protocol part.

Resetting BGP Connections

After changing the MBGP policy or protocol configuration, users must disconnect the present BGP connection to make the new configuration effective.

For details, refer to "BGP Configuration" of the Routing Protocol part.

Displaying and Debugging MBGP Configuration

After the above configuration, execute **display** commands in any view to display the running information of MBGP, and to verify the effect of the configuration.

Execute the **debugging** command in user view for the debugging of MBGP.

Table 496 Display and debug MBGP configuration

Operation	Command
Display an MBGP routing table	display bgp multicast routing-table [<i>ip-address</i> [<i>mask</i>]]
Display CIDR (classless inter-domain routing)	display bgp multicast routing-table cidr
Display the routing information about the specified MBGP community	display bgp multicast routing-table community [<i>aa:nn</i> no-export-subconfed no-advertise no-export]* [<i>whole-match</i>]
Display the routes permitted by the specified MBGP community list	display bgp multicast routing-table community-list <i>community-list-number</i> [<i>whole-match</i>]
Display the routes with inconsistent source autonomous systems	display bgp multicast routing-table different-origin-as
Display the routing information to or from a specified multicast neighbor	display bgp multicast peer [<i>peer-address</i>] [verbose]
Display the routing information advertised by MBGP	display bgp multicast network
Display the peer group information	display bgp multicast group [<i>group-name</i>]
Display the AS path information matching the AS regular expression	display bgp multicast routing-table regular-expression <i>as-regular-expression</i>
Disable/enable debugging MBGP UPDATE packets	[undo] debugging bgp mp-update [receive send] [verbose]

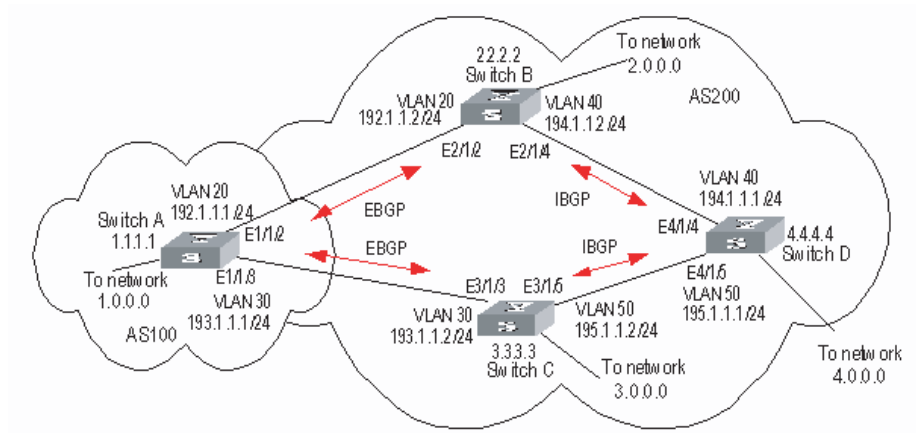
MBGP Multicast Extension Configuration Example

Network requirement

This example describes how the administrator uses the MBGP attributes to manage route selection. All switches are configured with MBGP. The IGP in AS200 uses OSPF. Switch A is AS100 and serves as the MBGP neighbor of Switch B and Switch C in AS200. Switch B and Switch C run IBGP for Switch D in AS200. Switch D is also in AS200.

Network diagram

Figure 119 Network diagram for MBGP path selection configuration



Configuration procedure

Configure Switch A:

```
<SwitchA> system-view
System View: return to User View with Ctrl+Z.
[SwitchA] vlan 20
[SwitchA-vlan20] port ethernet1/1/2
[SwitchA-vlan20] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ip address 192.1.1.1 255.255.255.0
[SwitchA-Vlan-interface20] quit
[SwitchA] vlan 30
[SwitchA-vlan30] port ethernet1/1/3
[SwitchA-vlan30] quit
[SwitchA] interface vlan-interface 30
[SwitchA-Vlan-interface30] ip address 193.1.1.1 255.255.255.0
[SwitchA-Vlan-interface30] quit
```

Enable MBGP.

```
[SwitchA] bgp 100
[SwitchA-bgp] ipv4-family multicast
```

Specify target network for MBGP.

```
[SwitchA-bgp-af-mul] network 1.0.0.0
[SwitchA-bgp-af-mul] network 2.0.0.0
[SwitchA-bgp-af-mul] quit
```

Configure peers relationship.

```
[SwitchA-bgp] bgp 100
[SwitchA-bgp] group a1 external
[SwitchA-bgp] peer 192.1.1.2 group a1 as-number 200
[SwitchA-bgp] group a2 external
[SwitchA-bgp] peer 193.1.1.2 group a2 as-number 200
[SwitchA-bgp] ipv4-family multicast
```

```
[SwitchA-bgp-af-mul] peer a1 enable
[SwitchA-bgp-af-mul] peer a2 enable
```

Configure the MED attribute of Switch A.

- Add an ACL on Switch A to permit network 1.0.0.0/8.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchA-acl-basic-2000] rule deny source any
```

- Define two routing policies: `set_med_50` and `set_med_100`, providing two MED values for network 1.0.0.0 (50 and 100 respectively).

```
[SwitchA] route-policy set_med_50 permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] apply cost 50
[SwitchA-route-policy] quit
[SwitchA] route-policy set_med_100 permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] apply cost 100
```

- Apply the routing policy `set_med_50` to the exported route updates of Switch C (193.1.1.2). Apply the routing policy `set_med_100` to the exported route updates of Switch B (192.1.1.2).

```
[SwitchA] bgp 100
[SwitchA-bgp] ipv4-family multicast
[SwitchA-bgp-af-mul] peer a2 route-policy set_med_50 export
[SwitchA-bgp-af-mul] peer a1 route-policy set_med_100 export
```

Configure Switch B:

```
<SwitchB> system-view
System View: return to User View with Ctrl+Z.
[SwitchB] vlan 20
[SwitchB-vlan20] port ethernet2/1/2
[SwitchB-vlan20] quit
[SwitchB] interface vlan-interface 20
[SwitchB-Vlan-interface20] ip address 192.1.1.2 255.255.255.0
[SwitchB-Vlan-interface20] quit
[SwitchB] vlan 40
[SwitchB-vlan40] port ethernet2/1/4
[SwitchB-vlan40] quit
[SwitchB] interface vlan-interface 40
[SwitchB-Vlan-interface40] ip address 194.1.1.2 255.255.255.0
[SwitchB-Vlan-interface40] quit
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
[SwitchB] bgp 200
[SwitchB-bgp] undo synchronization
[SwitchB-bgp] group b1 external
[SwitchB-bgp] peer 192.1.1.1.1 group b1 as-number 100
[SwitchB-bgp] group b2 internal
[SwitchB-bgp] peer 194.1.1.1.1 group b2
[SwitchB-bgp] peer 195.1.1.1.2 group b2
```

```
[SwitchB-bgp] ipv4-family multicast
[SwitchB-bgp-af-mul] peer b1 enable
[SwitchB-bgp-af-mul] peer b2 enable
```

Configure Switch C:

```
<SwitchC> system-view
System View: return to User View with Ctrl+Z.
[SwitchC] vlan 30
[SwitchC-vlan30] port ethernet3/1/3
[SwitchC-vlan30] quit
[SwitchC] interface vlan-interface 30
[SwitchC-Vlan-interface30] ip address 193.1.1.2 255.255.255.0
[SwitchC-Vlan-interface30] quit
[SwitchC] vlan 50
[SwitchC-vlan50] port ethernet3/1/5
[SwitchC-vlan50] quit
[SwitchC] interface vlan-interface 50
[SwitchC-Vlan-interface50] ip address 195.1.1.2 255.255.255.0
[SwitchC-Vlan-interface50] quit
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
[SwitchC] bgp 200
[SwitchC-bgp] undo synchronization
[SwitchC-bgp] group c1 external
[SwitchC-bgp] peer 193.1.1.1 group c1 as-number 100
[SwitchC-bgp] group c2 internal
[SwitchC-bgp] peer 194.1.1.2 group c2
[SwitchC-bgp] peer 195.1.1.1 group c2
[SwitchC-bgp] ipv4-family multicast
[SwitchC-bgp-af-mul] peer c1 enable
[SwitchC-bgp-af-mul] peer c2 enable
```

Configure the local preference attribute of Switch C.

- Add ACL 2000 on Switch C to permit network 1.0.0.0.

```
[SwitchC] acl number 2000
[SwitchC-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchC-acl-basic-2000] quit
```

- Define the routing policy named "localpref". Set the local preference for the routes matching ACL 2000 to 200, and otherwise, to 100.

```
[SwitchC] route-policy localpref permit node 10
[SwitchC-route-policy] if-match acl 2000
[SwitchC-route-policy] apply local-preference 200
[SwitchC-route-policy] quit
[SwitchC] route-policy localpref permit node 20
[SwitchC-route-policy] apply local-preference 100
```

- Apply this routing policy to the inbound traffic from BGP neighbor 193.1.1.1 (Switch A).


```
[SwitchC] bgp 200
[SwitchC-bgp] ipv4-family multicast
[SwitchC-bgp-af-mul] peer 193.1.1.1 route-policy localpref import
```

Configure Switch D:

```
<SwitchD> system-view
System View: return to User View with Ctrl+Z.
[SwitchD] vlan 40
[SwitchD-vlan40] port ethernet4/1/4
[SwitchD-vlan40] quit
[SwitchD] interface vlan-interface 40
[SwitchD-Vlan-interface40] ip address 194.1.1.1 255.255.255.0
[SwitchD-Vlan-interface40] quit
[SwitchD] vlan 50
[SwitchD-vlan50] port ethernet4/1/5
[SwitchD-vlan50] quit
[SwitchD] interface vlan-interface 50
[SwitchD-Vlan-interface50] ip address 195.1.1.1 255.255.255.0
[SwitchD-Vlan-interface50] quit
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 4.0.0.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
[SwitchD] bgp 200
[SwitchD-bgp] undo synchronization
[SwitchD-bgp] group d1 internal
[SwitchD-bgp] peer 194.1.1.2 group d1
[SwitchD-bgp] peer 195.1.1.2 group d1
[SwitchD-bgp] ipv4-family multicast
[SwitchD-bgp-af-mul] peer d1 enable
```

To make the configuration effective, you need to use the **reset bgp all** command on all MBGP neighbors.

47

MPLS ARCHITECTURE



The 3Com Switch 8800 Family Series Routing Switches (hereinafter referred to as Switch 8800 Family series) running MPLS can serve as routers. Routers mentioned in this manual can be either a router in common sense, or a layer 3 Ethernet switch running MPLS.

MPLS (Multiprotocol Label Switching) encapsulates network layer packets with short and fixed-length labels. As the name implies, it supports multiple protocols, such as IP, IPv6, and IPX. And it allows a device to make forwarding decision based on the labels attached to the received packets without going through the complex routing table lookup procedures with IP. MPLS brings together the advantages of the connectionless control with IP and the connection-oriented forwarding with ATM. In addition to the support from IP routing and control protocols, its powerful and flexible routing functions allows it to accommodate to various emerging applications.

MPLS Overview

MPLS (Multiprotocol Label Switching) encapsulates network layer packets with short and fixed-length labels. As the name implies, it supports multiple protocols, such as IP, IPv6, and IPX. And it allows a device to make forwarding decision based on the labels attached to the received packets without going through the complex routing table lookup procedures with IP. MPLS brings together the advantages of the connectionless control with IP. In addition to the support from IP routing and control protocols, its powerful and flexible routing functions allows it to accommodate to various emerging applications.

MPLS was initially proposed to accelerate the packet forwarding on routers, but it has been widely used in Traffic Engineering (TE), Virtual Private Network (VPN), and other aspects, and is becoming one of the most important standards on large scale IP networks.

MPLS Basic Concepts

FEC Forwarding Equivalence Class (FEC) is an important concept in MPLS. MPLS is actually a kind of classify-and-forward technology. It categorizes packets with the same forwarding strategy (same destination addresses, same forwarding routes and same QoS levels) into one class, which is called a FEC. Generally, the FEC classification is based on network layer address. Packets of the same FEC are processed in the same way in MPLS network.

Label **Label definition**

A label is a locally significant short identifier with fixed length, which is used to identify a FEC. When reaching at MPLS network ingress, packets are divided into

different FECs, based on their FECs, different labels are encapsulated into the packets. Later forwarding is based on these labels.

Label structure

The structure of the label is shown in Figure 120.

Figure 120 Label structure



Label is located between the link layer header and the network layer packet, with the length of four bytes. A label contains four fields:

Label: label value, 20 bits.

Exp: three bits, reserved, used for COS.

S: one bit, MPLS supports hierarchical label structure, namely multi-layer label. Value 1 refers to the label of bottom layer.

TTL: eight bits, with the same meaning as TTL in IP packet.

Label operations

1 Label mapping

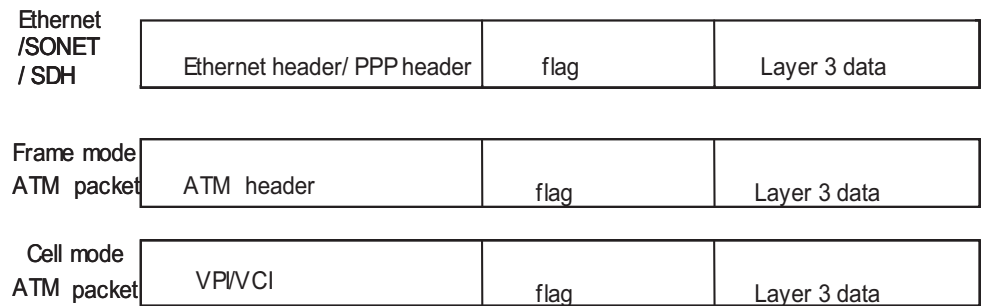
There are two types of label mapping: label mapping at ingress routers, and label mapping in MPLS domain.

The first type of mapping is implemented at Ingress label switching routers (LSR). The Ingress LSRs group the incoming packets into multiple FECs based on certain principles, and then map corresponding labels to these FECs and record the mapping results into the label information base (LIB). In simple words, label mapping is to assign a label to a FEC.

The second type is also called incoming label mapping (ILM), that is, to map each input label to a series of next hop label forwarding entries (NHLFE). The packets are forwarded along the paths based on the mapping results.

2 Label encapsulation

Figure 121 illustrates label encapsulation in different media:

Figure 121 Label position in packet

In Ethernet packets and PPP packets, label stack lies between layer 2 header and layer 3 data, acting like a shim.

3 Label assignment and distribution

Label distribution refers to the process of creating a corresponding label switching path (LSP) for a FEC.

In the MPLS architecture, the decision to bind a particular label to a particular FEC is made by downstream LSR; after making the decision, the downstream LSR notifies the upstream LSR. That is to say, the label is assigned by the downstream LSR, and the assigned label is distributed from downstream to upstream.

Two label distribution modes are available in MPLS: downstream unsolicited (DU) mode and downstream on demand (DoD) mode.

- For a specific FEC, if LSR originates label assignment and distribution even without receiving label request message from upstream, it is in DU mode.
- For a specific FEC, if LSR begins label assignment and distribution only after receiving label request message from upstream, it is in DoD mode.

The upstream and downstream which have adjacency relation in-label distribution should reach agreement on label distribution mode.

To distribute labels to its peer, the LSR can use Label Distribution Protocol (LDP) messages or make the labels carried on other routing protocol messages.



Upstream and downstream are just on a relative basis: For a packet forwarding process, the transmit router serves as upstream LSR and receive router serves as downstream LSR. Currently, the Switch 8800 Family series adopt the DU label distribution mode.

4 Label assignment control mode

There are two modes to control the assignment and distribution of labels: independent mode and ordered mode.

In independent control mode, each LSR can send label mapping messages to the LSRs it connects to at anytime.

In ordered control mode, a LSR can send label mapping messages to upstream only when it receives a specific label mapping messages of the next hop of a FEC or the LSR serves as LSP (Label Switching Path) egress node.



Currently, the Switch 8800 Family series adopt the ordered label control mode.

5 Label retention mode

There are two label-retention modes: liberal label retention mode and conservative label retention mode.

Suppose there are two LSRs: Ru and Rd. For a specific FEC, if LSR Ru has received the label binding from LSR Rd, in case Rd is not the next hop of Ru and Ru saves this binding, then it is the liberal label retention. And if Ru discards this binding, then it is the conservative label retention mode.

In case it is required that LSR is capable of adapting route variation rapidly, you can use the liberal label retention mode. In case it is required that a few labels are saved in LSR, you can use the conservative label retention mode.



Currently, the Switch 8800 Family series adopt the liberal label retention mode.

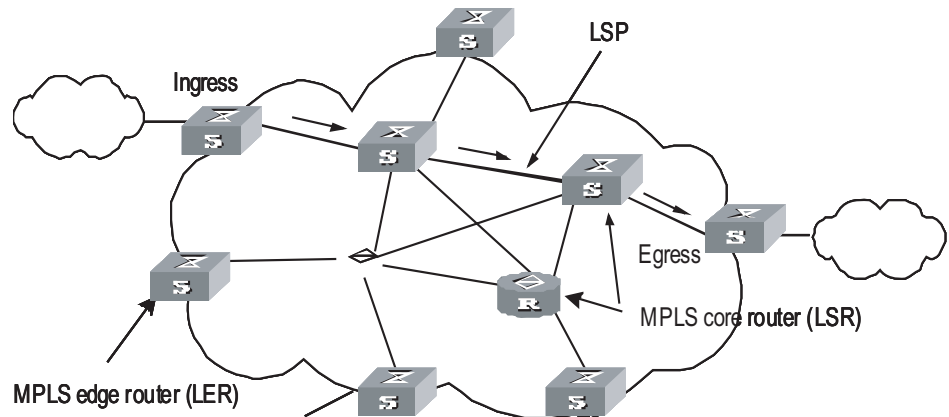
LDP Label distribution protocol (LDP) is the signaling control protocol in MPLS, which controls binding labels and FECs between LSRs and coordinates a series of procedures between LSRs.

MPLS Architecture

MPLS Network Structure The basic composing unit of MPLS network is LSR (Label Switching Router). It runs MPLS control protocol and L3 routing protocol, exchanges routing messages with other LSRs and create the routing table, maps FECs with IP packet headers, binds FECs with labels, distributes label binding messages, establishes and maintains label forwarding table.

The network consisting of LSRs is called MPLS domain. The LSR that is located at the edge of the domain is called edge LSR (LER, Labeled Edge Router). It connects an MPLS domain with a non-MPLS domain or with another MPLS domain, classifies packets, distributes labels (as ingress LER) and distracts labels (as egress LER). The ingress LER is termed as ingress and egress LER as egress.

The LSR that is located inside the domain is called core LSR, which provides functions such as label swapping and label distribution. The labeled packets are transmitted along the LSP (Label Switched Path) composed of a series of LSRs.

Figure 122 MPLS basic principle

Forwarding Labeled Packets

At the ingress, the packets entering the network are classified into FECs according to their characteristics. Usually, packets are classified into FECs according to the IP address prefix or host address. Packets in the same FEC pass through the same path (that is, LSP) in MPLS area. LSR assigns a short label of fixed length for the incoming FEC packet, and then forwards it through the corresponding interface.

On the LSR along the LSP, the mapping table of the import/export labels has been established (the element of this table is referred to as Next Hop Label Forwarding Entry (NHLFE)). When the labeled packet arrives, LSR only needs to find the corresponding NHLFE from the table according to the label and replace the original label with a new one, and then forwards the labeled packet. This process is called Incoming Label Map (ILM).

At the ingress, MPLS specifies a FEC for a specific packet, and the following routers only need to forward the packet by label switching, therefore this method is much simpler than general network layer forwarding and increases the forwarding speed.

Establishing LSP

Actually, the establishment of LSP refers to the process of binding FEC with the label, and then advertising this binding to the adjacent LSR on LSP. This process is implemented through LDP, which regulates the message in interactive processing and message structure between LSRs as well as routing mode.

LDP working process

Through sending Hello message periodically, an LSR finds its neighbor and then establish LDP session with the newly discovered adjacent LSR. By LDP session, the adjacent LSRs advertise such information as label switching mode, label space, session Keepalive timer value to each other. LDP session is a TCP connection, which needs to be maintained through LDP message. In case there is not any other LDP message during the time period specified by the session Keepalive timer value, and then it is necessary to send session Keepalive message to maintain the existence of LDP session. Figure 123 illustrates the diagram of LDP label distribution.

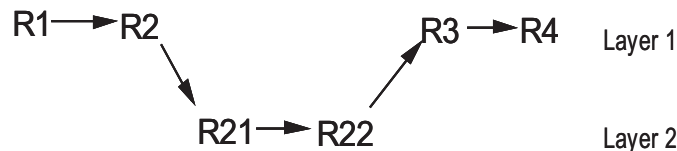
The path vector method refers to that the path information is recorded in the message bound with the forwarding label, and, for every hop, the corresponding router checks if its ID is contained in this record. If not, the router adds its ID into the record; and if yes, it indicates that a loop presents and the process for establishing LSP is terminated.

LSP Tunnel and Hierarchy

LSP tunnel

MPLS supports LSP tunnel technology. On an LSP path, LSR Ru and LSR Rd are both the upstream and the downstream for each other. However, the path between LSR Ru and LSR Rd may not be part of the path provided by routing protocol. MPLS allows establishing a new LSP path $\langle Ru R1 \dots Rn Rd \rangle$ between LSR Ru and LSR Rd, and LSR Ru and LSR Rd are respectively the starting point and ending point of this LSP. The LSP between LSR Ru and LSR Rd is referred to as the LSP tunnel, which avoids the traditional encapsulated tunnel on the network layer. If the route along which the tunnel passes and the route obtained hop by hop from routing protocol is consistent, this tunnel is called hop-by-hop routing tunnel. And if the two routes are not consistent, then the tunnel of this type is called explicit routing tunnel.

Figure 124 LSP tunnel



As shown in Figure 124, LSP $\langle R2 R21 R22 R3 \rangle$ is a tunnel between R2 and R3.

Multi-layer label stack

In MPLS, a packet may carry multiple labels which are in the form of stack. Operations to the stack follow the "last in first out" principle and it is always the labels at the top of the stack that decide how to forward packets. Pushing label indicates to add a label into a outgoing packet, then the depth of the label stack is the former one plus 1, and the current label of the packet changes to the newly added one; popping a label indicates to remove a label form a packet, then the depth of the packet is the former one minus 1, and the current label of the packet changes to the label of its underlayer.

Multiple-layer label stack is used in LSP tunnel. When a packet travels in LSP tunnel, there will be multiple layers for the label of the packet. Then, at the ingress and egress of each tunnel, it is necessary to implement pushing and popping operation for the label stack. For each pushing operation, the label will be added with one layer. And there is no depth limitation for the label stack from MPLS.

The labels are organized according to the principle of "last in first out" in the label stack, and MPLS processes the labels beginning from the top of the stack.

If the depth of the label stack for a packet is m , it indicates that the label at the bottom of that stack is level 1 label, and the label at the top of the stack is level m label. A packet with no label can be regarded as a packet with empty label stack, that is, the depth of its label stack is 0.

MPLS and Other Protocols (Routing Protocols)

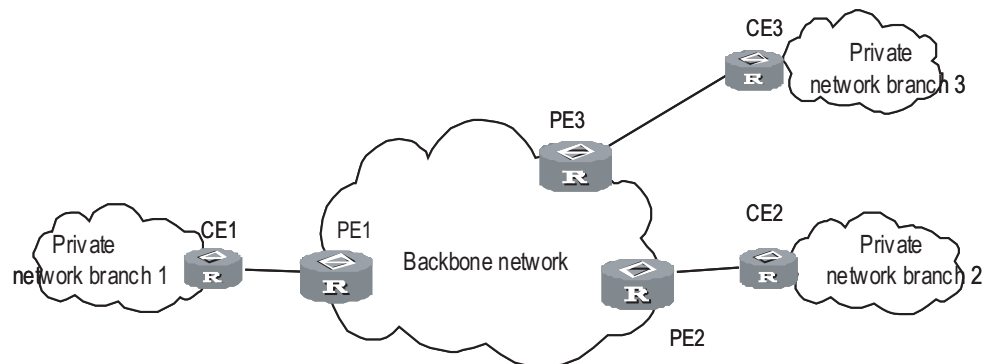
When LDP establishes LSP in hop-by-hop mode, the next hop is determined by using the information, which is usually collected by such routing protocols as IGP, BGP in each LSR route forwarding table, on the way. However, LDP just uses the routing information indirectly, rather than associates with various routing protocols directly.

On the other hand, although LDP is the special protocol for implementing label distribution, it is not the sole protocol for label distribution. The existing protocols such as BGP, RSVP, after being extended, can also support MPLS label distribution. For some MPLS applications, it is also necessary to extend some routing protocols. For example, the application of MPLS VPN requires extending the BGP protocol, thus the BGP protocol can propagate VPN routing information.

MPLS Application (MPLS-based VPN)

To transmit data stream of private network on public network, traditional VPN uses tunnel protocols like GRE, L2TP, and PPTP. LSP itself is a tunnel on public network, so there are obvious advantages to implement VPN by MPLS. MPLS VPN connects the geographically different branches of private network by using LSP, forming a united network. MPLS VPN also supports the interconnection between different VPNs.

Figure 125 MPLS-Based VPN



The basic structure of MPLS-based VPN is shown in Figure 125. CE is the customer edge device, and it may either be a router or a switch, or perhaps a host. PE is a service provider edge router, which is located on the backbone network. PE is responsible for the management of VPN customers, establishing LSP connection between various PEs, route allocation among different branches of the same VPN customer.

Usually the route allocation between PEs is implemented by using extended BGP. MPLS VPN supports the IP address multiplexing between different branches and the interconnection between different VPNs. Compared with traditional route, it is necessary to add branch and VPN identifier information in VPN route. So, it is necessary to extend BGP so as to carry VPN routing information.

48

MPLS BASIC CAPABILITY CONFIGURATION

MPLS Basic Capability Overview

Basic MPLS forwarding functions includes LDP session establishment and LSP path maintenance.

The typical configuration procedure for enabling basic MPLS functions on a routing switch is as follows:

- 1 Configure LSR ID
- 2 Enable MPLS
- 3 Enable LDP
- 4 Enter VLAN interface view and enable MPLS and LDP on the interface

Then the routing switch can provide MPLS forwarding and LDP signaling functions.

If you want to modify the default parameters or enable some special functions, for example, manually creating LSP or explicit route, you can configure according to the methods in configuration list. For some complicated functions, configuration combination may be required.

MPLS Configuration

The following sections describe the required configuration tasks for MPLS basic capability:

- “Defining MPLS LSR ID”
- “Enabling MPLS and Entering MPLS View”

The following sections describe the optional configuration tasks for MPLS basic capability:

- “Configuring the Topology-Driven LSP Setup Policy”
- “Configuring an LSP Setup Policy”
- “Configuring Static LSP”

Defining MPLS LSR ID

Before configuring any other MPLS command, it is necessary to first configure the LSR ID. This ID is usually in IP address format and must be unique in the domain.

Perform the following configuration in the system view.

Table 497 Define MPLS LSR ID

Operation	Command
Define LSR ID	mpls lsr-id <i>ip-address</i>
Delete LSR ID	undo mpls lsr-id

By default, LSR ID is not defined.

Enabling MPLS and Entering MPLS View

In system view, you can first enable MPLS globally and enter MPLS view using the **mpls** command. Then you can directly enter MPLS view after using the **mpls** command in system view.

Use the **mpls** command in VLAN interface view to enable MPLS on the VLAN interface.

Table 498 Enter MPLS view

Operation	Command
Enable MPLS globally and enter MPLS view (system view)	mpls
Enable MPLS on a VLAN interface (VLAN interface view)	mpls
Disable MPLS globally or on a VLAN interface (system or VLAN interface view)	undo mpls

By default, MPLS is not enabled.

Configuring the Topology-Driven LSP Setup Policy

It refers to specifying filtering policy as all or ip-prefix.

Perform the following configuration in MPLS view.

Table 499 Configure the topology-driven LSP setup policy

Operation	Command
Configure the topology-Driven LSP setup policy	lsp-trigger { all ip-prefix <i>ip-prefix</i> }
Use the default value, which only allows 32-bit IP to trigger LSP.	undo lsp-trigger { all ip-prefix <i>ip-prefix</i> }

Configuring an LSP Setup Policy

When a Label Mapping event is received, use the IP address prefix filtering policy to control the acceptance of label binding.

Table 500 Configure an LSP setup policy

Operation	Command
Configure an LSP setup policy	mpls ldp label-accept <i>ip-prefix-name</i>
Cancel the LSP setup policy configured	undo mpls ldp label-accept <i>ip-prefix-name</i>

Perform the following configurations in system view.

Table 501 Configure the advertisement of local distribution labels

Operation	Command
Configure the advertisement of local distribution labels	mpls ldp label-advertise <i>fec-ip-prefix</i> [<i>lsp-ip-prefix</i>] [swap-only]

Table 501 Configure the advertisement of local distribution labels

Operation	Command
Cancel the configuration of the advertisement of local distribution labels	undo mpls ldp label-advertise { <i>fec-ip-prefix</i> all }

By default, the labels of all destination addresses are advertised to all LDP peers.

Configuring Static LSP

You can manually set an LSR to be a node along an LSP, and place a limit on the traffic over the LSP. Depending on the position in an MPLS domain, an LSR along an LSP can be the ingress node, an intermediate node (also called transit node), or the egress node. Note that an LSP operates normally only after all the LSRs along the LSP have been properly configured.

Perform the following configuration in MPLS view.

Table 502 Set the local LSR to a node on a specified LSP

Operation	Command
Set the current LSR to the ingress node of the specified LSP	static-lsp ingress <i>lsp-name</i> { destination <i>dest-addr</i> { <i>addr-mask</i> <i>mask-length</i> } I2vpn } nexthop <i>next-hop-addr</i> } out-label <i>out-label-value</i>
Cancel the ingress node setting of the specified LSP	undo static-lsp ingress <i>lsp-name</i>
Set the current LSR to an intermediate node along the specified LSP	static-lsp transit <i>lsp-name</i> [I2vpn] incoming-interface <i>interface-type interface-number</i> in-label <i>in-label-value</i> nexthop <i>next-hop-addr</i> out-label <i>out-label-value</i>
Cancel the intermediate node setting of the specified LSP	undo static-lsp transit <i>lsp-name</i>
Set the current LSR to the egress node of the specified LSP	static-lsp egress <i>lsp-name</i> [I2vpn] incoming-interface <i>interface-type interface-number</i> in-label <i>in-label-value</i>
Cancel the egress node setting of the specified LSP	undo static-lsp egress <i>lsp-name</i>

LDP Configuration

The following sections describe the required LDP configuration tasks for MPLS basic capability:

- “Enabling LDP protocol”
- “Enabling LDP on a VLAN interface”

The following sections describe the optional LDP configuration tasks for MPLS basic capability:

- “Configuring Remote-Peer for Extended Discovery Mode”
- “Configuring session parameters”

Enabling LDP protocol

To configure LDP, first enable LDP.

Perform the following configuration in the system view.

Table 503 Enable/disable LDP view

Operation	Command
Enable LDP protocol	mpls ldp
Disable LDP	undo mpls ldp

By default, LDP is disabled.

Enabling LDP on a VLAN interface

To make the VLAN interface support LDP, you must enable LDP function on the interface in VLAN interface mode. After enabling the LDP function, the interface then sets up session. It begins to set up LSP if in topology-driven mode.

Disabling LDP function on interface causes the break of all LDP session in VLAN interface, and all the LSP based on those sessions are deleted. So you must use this command with cautiously.

Perform the following configuration in the interface view.

Table 504 Enable/disable LDP on an interface

Operation	Command
Enable LDP function on an interface	mpls ldp enable
Disable LDP function on an interface	mpls ldp disable

By default, the interface LDP function is disabled.

Configuring Remote-Peer for Extended Discovery Mode

The Remote-peer configuration is mainly used for extended discovery mode so that this LSR can establish sessions with LSRs that are not directly connected with it at the link layer.

Enter Remote-peer view

Perform the following configuration in the system view.

Table 505 Enter Remote-peer view

Operation	Command
Enter Remote-peer view	mpls ldp remote-peer <i>index</i>
Delete the corresponding Remote-peer	undo mpls ldp remote-peer <i>index</i>

There is no default remote-peer.

Configuring an address for the Remote-peer

You can specify the address of any LDP-enabled interface on the Remote-peer or the address of the Loopback interface on the LSR that has advertised the route as the address of the Remote-peer.

Perform the following configuration in the Remote-peer view.

Table 506 Configure a Remote-peer address

Operation	Command
Configure a remote-peer address	remote-ip <i>remoteip</i>

remoteip: the IP address of the Remote-peer. It should be the ID of the peer LSR.

Configuring session parameters

Configuring session hold-time

The LDP entity on the interface sends Hello packets periodically to find out LDP peer, and the established sessions must also maintain their existence by periodic message (if there is no LDP message, then Keepalive message must be sent).



There are two types of LDP sessions: Basic and Remote. Basic session can be established only on two direct-connect switches, while Remote session can be on two switches which are not directly connected. You can only configure Basic sessions in VLAN interface view and Remote sessions in remote-peer view.



CAUTION: *Modifying the holdtime parameter results in re-establish the original session, as well as the LSP over this session. Here the session refers to Basic session, but not Remote session.*

Configure Basic session hold-time in VLAN interface view.

Table 507 Configure Basic session hold-time

Operation	Command
Configure session hold-time	mpls ldp timer { session-hold session-holdtime hello hello-holdtime }
Return to the default value	undo mpls ldp timer { session-hold hello }

By default, the *session-holdtime* is 60 seconds and *hello-holdtime* is 15 seconds.

Configure Remote session hold-time in Remote-peer view.

Table 508 Configure Remote session hold-time

Operation	Command
Configure session hold-time	mpls ldp timer { targeted-session-hold targeted-hello } {holdtime interval }
Return to the default value	undo mpls ldp timer { targeted-session-hold targeted-hello }

By default, **targeted-session-hold** *holdtime* is 60 seconds, and the interval is 24 seconds; **targeted-hello** *holdtime* is 45 seconds and the interval is 13 seconds.

Configuring Hello transport-address

The transport-address discussed here refers to the address carried in the transport address TLV in Hello messages. Generally, you can configure the transport-address to the MPLS LSR ID of the current LSR, but you can also configure the transport-address to other address flexibly as required by some applications.

Perform the following configuration in VLAN interface view.

Table 509 Configure Hello transport-address

Operation	Command
Configure Hello transport-address	mpls ldp transport-ip { interface ip-address }

Table 509 Configure Hello transport-address

Operation	Command
Return to the default Hello transport-address	undo mpls ldp transport-ip

Transport-address defaults to the MPLS LSR ID of the current LSR.

If there are multiple links connecting two neighboring LSRs, all the LDP-enabled interfaces on the links connecting LSR and its neighbor must have the same transport address. You are recommended to use the same interface address for all of them, that is, LSR-ID.

Configuring LDP Loop Detection Control

Enabling loop detection

You can enable or disable the loop detection function during LDP signaling process. The loop detection includes maximum hop count mode and path vector mode.

The maximum hop count method refers to that the hop-count information is contained in the message bound with the forwarding label, and the value pluses one for each hop. When the value exceeds the threshold value, it is considered that a loop presents, and the process for establishing LSP is terminated.

The path vector method refers to that the path information is recorded in the message bound with the forwarding label, and, for every hop, the corresponding router checks if its ID is contained in this record. If not, the router adds its ID into the record; and if yes, it indicates that a loop presents and the process for establishing LSP is terminated. When this method is used, if the defined maximum value is exceeded, it is considered that a loop happens and the LSP establishment fails.

Perform the following configuration in the system view.

Table 510 Enable loop detection

Operation	Command
Enable loop detection	mpls ldp loop-detect
Disable loop detection	undo mpls ldp loop-detect

By default, the loop detection is disabled.

Setting the maximum hop count for loop detection

When maximum hop count mode is adopted for loop detection, the maximum hop-count value can be defined. And if the maximum value is exceeded, it is considered that a loop happens and the LSP establishment fails.

Perform the following configuration in the system view.

Table 511 Set the maximum hop count for loop detection

Operation	Command
Set maximum hop count for loop detection	mpls ldp hops-count <i>hop-number</i>
Return to the default maximum hop count	undo mpls ldp hops-count

The maximum hop count of loop detection is 32 by default.

Setting the maximum hop count in path vector mode

When path vector mode is adopted for loop detection, it is also necessary to specify the maximum value of LSP path. In this way, when one of the following conditions is met, it is considered that a loop happens and the LSP establishment fails.

- The record of this LSR already exists in the path vector recording table.
- The path hop count exceeds this maximum value.

Perform the following configuration in the system view.

Table 512 Set the maximum hop count in path vector mode

Operation	Command
Set the maximum hop count in path vector mode	mpls ldp path-vectors <i>pv-number</i>
Return to the default maximum hop count in path vector mode	undo mpls ldp path-vectors

The maximum of the maximum hop count of path vector is 32 by default.

Configuring LDP Authentication Mode Between Every Two Routers

Perform the following configuration in VLAN interface view or Remote-peer view.

Table 513 Configure LDP authentication mode (between every two routers)

Operation	Command
Configure LDP authentication Mode	mpls ldp password [cipher simple] <i>password</i>
Remove LDP authentication	undo mpls ldp password

Displaying and Debugging MPLS Basic Capability

Displaying and Debugging MPLS

Displaying static LSPs

After accomplishing the configuration tasks mentioned previously, you can execute the **display** command in any view to view the running state of a single or all the static LSPs and thus to evaluate the effect of the configurations.

Table 514 Display the static LSP information

Operation	Command
Display the static LSP information	display mpls static-lsp [include <i>text</i> verbose]

Displaying the MPLS statistics information or LSP information of all ports or a single VLAN interface

After finishing the configurations above, execute the **display** command in any view to view the MPLS statistics information or LSP information of all ports or a single VLAN interface. You can verify the effect of the configuration by checking the information on display.

Table 515 Display statistics information of static LSP

Operation	Command
Displaying the MPLS statistics information or LSP information of all ports or a single VLAN interface	display mpls statistics { interface { <i>Vlan-interface</i> all } lsp { <i>lsp-Index</i> all <i>lsp-name</i> }

Displaying MPLS-enabled interfaces

After accomplishing the configuration tasks mentioned previously, you can execute the **display** command in any view to view the information related to the MPLS-enabled interfaces and thus to evaluate the effect of the configurations.

Table 516 Display information of the MPLS-enabled interfaces

Operation	Command
Display information of the MPLS-enabled interfaces	display mpls interface

Displaying MPLS LSP information

Execute the following commands in any view to display the information related to MPLS LSP.

Table 517 Display the information about MPLS LSP

Operation	Command
Display the information about MPLS LSP	display mpls lsp [include <i>text</i> verbose]

Debugging MPLS

You may execute the **debugging** command in user view to debug the information concerning all interfaces with MPLS function enabled.

As enabling debugging may affect the router performance, you are recommended to use this command when necessary. Execute the **undo** form of this command to disable the corresponding debugging.

Table 518 Enable/disable debugging for MPLS

Operation	Command
Enable debugging for MPLS LSP	debugging mpls lspm { agent all event ftn interface packet policy process vpn }
Disable debugging for MPLS LSP	undo debugging mpls lspm { agent all event ftn interface packet policy process vpn }

Trap information of MPLS

This command is used to enable the trap function of MPLS during an LSP/LDP setup process.

Perform the following configuration in system view.

Table 519 Enable the trap function of MPLS

Operation	Command
Enable the LDP Trap function of MPLS	snmp-agent trap enable ldp
Disable the LDP Trap function of MPLS	undo snmp-agent trap enable ldp
Enable the LSP Trap function of MPLS	snmp-agent trap enable lsp

Table 519 Enable the trap function of MPLS

Operation	Command
Disable the LSP Trap function of MPLS	undo snmp-agent trap enable lsp

Displaying and Debugging LDP

LDP display commands

Comware provides abundant MPLS monitoring commands for monitoring states of LSRs, LDP sessions, interfaces and peers. These commands are the powerful debugging and diagnosing tools.

After accomplishing the configuration tasks described earlier, you can execute the **display** command in any view to view the running state of LDP and thus to evaluate the effect of the configurations.

Table 520 Display LDP

Operation	Command
Display LDP information	display mpls ldp
Display buffer information for LDP	display mpls ldp buffer-info
Display LDP-enabled interface information	display mpls ldp interface
Display LDP saved label information	display mpls ldp lsp
Display information on all peers of LDP session	display mpls ldp peer
Display information of the remote-peers in the LDP sessions	display mpls ldp remote
Display states and parameters of LDP sessions	display mpls ldp session

LDP debugging commands

Execute **debugging** command in user view for the debugging of various messages related to LDP

Table 521 Enable/disable debugging for MPLS LDP

Operation	Command
Enable debugging for MPLS LDP	debugging mpls ldp { all main advertisement session pdu notification remote filter } [interface <i>interface-type</i> <i>interface-number</i>]
Disable debugging for MPLS LDP	undo debugging mpls ldp { all main advertisement session pdu notification remote filter } [interface <i>interface-type</i> <i>interface-number</i>]

Use the **mpls ldp reset-session** command in VLAN interface to reset a specific LDP session on the VLAN interface.

Table 522 Reset LDP

Operation	Command
Reset a specific LDP session on the VLAN interface (VLAN interface view)	mpls ldp reset-session <i>peer-address</i>

Typical MPLS Configuration Example

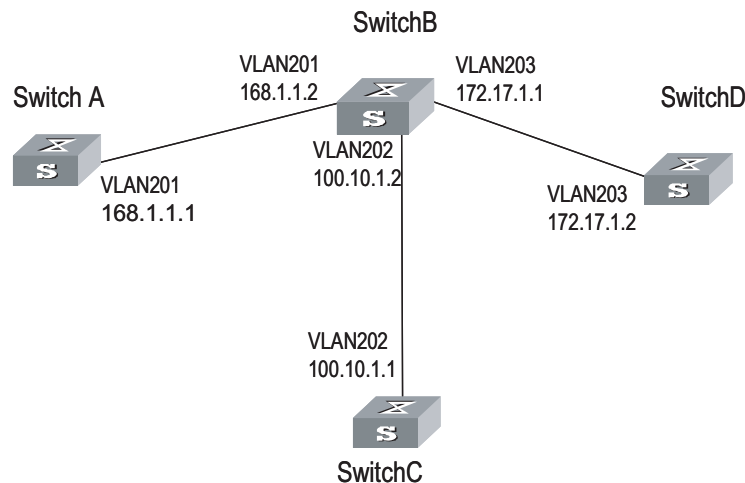
Network requirements

Figure 126 illustrates a network with four switches, which connects to each other through Ethernet.

The four switches all support MPLS, and LSP can be established between any two switches with the routing protocol OSPF. LDP establishes LSP by using routing information of OSPF.

Network diagram

Figure 126 Network diagram



Configuration procedure

1 Configure Switch A

Configure LSR ID and enable MPLS and LDP.

```
[SW8800] mpls lsr-id 168.1.1.1
[SW8800] mpls
[3Com-mpls] quit
[SW8800] mpls ldp
```

Configure IP address and enable MPLS and LDP for VLAN interface 201.

```
[SW8800] vlan 201
[3Com-vlan201] port gigabitethernet 2/1/1
[3Com-vlan201] quit
[SW8800] interface Vlan-interface 201
[3Com-Vlan-interface201] ip address 168.1.1.1 255.255.0.0
[3Com-Vlan-interface201] mpls
[3Com-Vlan-interface201] mpls ldp enable
[3Com-Vlan-interface201] mpls ldp transport-ip interface
```

Enable OSPF on the interface connecting Switch A with Switch B.

```
[SW8800] Router id 168.1.1.1
[SW8800] ospf
[3Com-ospf-1] area 0
[3Com-ospf-1-area-0.0.0.0] network 168.1.0.0 0.0.255.255
```

2 Configure Switch B

Configure LSR ID and enable MPLS and LDP.

```
[SW8800] mpls lsr-id 172.17.1.1
[SW8800] mpls
[3Com-mpls] quit
[SW8800] mpls ldp
```

Configure IP address and enable MPLS and LDP for VLAN interface 201.

```
[SW8800] vlan 201
[3Com-vlan201] port gigabitethernet 2/1/1
[3Com-vlan201] quit
[SW8800] interface vlan-interface 201
[3Com-Vlan-interface201] ip address 168.1.1.2 255.255.0.0
[3Com-Vlan-interface201] mpls
[3Com-Vlan-interface201] mpls ldp enable
[3Com-Vlan-interface201] mpls ldp transport-ip interface
```

Configure IP address and enable MPLS and LDP for VLAN interface 203.

```
[SW8800] vlan 203
[3Com-vlan203] port gigabitethernet 2/1/3
[3Com-vlan203] quit
[SW8800] interface vlan-interface 203
[3Com-Vlan-interface203] ip address 172.17.1.1 255.255.0.0
[3Com-Vlan-interface203] mpls
[3Com-Vlan-interface203] mpls ldp enable
[3Com-Vlan-interface203] mpls ldp transport-ip interface
```

Configure IP address and enable MPLS and LDP for VLAN interface 202.

```
[SW8800] vlan 202
[3Com-vlan202] port gigabitethernet 2/1/2
[3Com-vlan202] quit
[SW8800] interface Vlan-interface 202
[3Com-Vlan-interface202] ip address 100.10.1.2 255.255.255.0
[3Com-Vlan-interface202] mpls
[3Com-Vlan-interface202] mpls ldp enable
[3Com-Vlan-interface202] mpls ldp transport-ip interface
[3Com-Vlan-interface202] quit
```

Enable OSPF on the interfaces respectively connecting Switch B with Switch A, Switch D and Switch C.

```
[SW8800] Router id 172.17.1.1
[SW8800] ospf
[3Com-ospf-1] area 0
[3Com-ospf-1-area-0.0.0.0] network 168.1.0.0 0.0.255.255
[3Com-ospf-1-area-0.0.0.0] network 172.17.0.0 0.0.255.255
[3Com-ospf-1-area-0.0.0.0] network 100.10.1.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] quit
```

3 Configure Switch C

Configure LSR ID and enable MPLS and LDP.

```
[SW8800] mpls lsr-id 100.10.1.1
[SW8800] mpls
[3Com-mpls] quit
[SW8800] mpls ldp
```

Configure IP address and enable LDP and MPLS for VLAN interface 202.

```
[SW8800] vlan 202
[3Com-vlan202] port gigabitethernet 2/1/1
[3Com-vlan202] quit
[SW8800] interface Vlan-interface 202
[3Com-Vlan-interface202] ip address 100.10.1.1 255.255.255.0
[3Com-Vlan-interface202] mpls
[3Com-Vlan-interface202] mpls ldp enable
[3Com-Vlan-interface202] quit
```

Enable OSPF on the interface connecting Switch C with Switch B.

```
[SW8800] Router id 100.10.1.1
[SW8800] ospf
[3Com-ospf-1] area 0
[3Com-ospf-1-area-0.0.0.0] network 100.10.1.0 0.0.0.255
```

4 Configure Switch D

Configure LSR ID and enable MPLS and LDP.

```
[SW8800] mpls lsr-id 172.17.1.2
[SW8800] mpls
[3Com-mpls] quit
[SW8800] mpls ldp
```

Configure IP address and enable MPLS and LDP for VLAN interface 203.

```
[SW8800] vlan 203
[3Com-vlan203] port gigabitethernet 2/1/3
[3Com-vlan203] quit
[SW8800] interface vlan-interface 203
[3Com-Vlan-interface203] ip address 172.17.1.2 255.255.0.0
[3Com-Vlan-interface203] mpls
[3Com-Vlan-interface203] mpls ldp enable
```

Enable OSPF on the interface connecting Switch D with Switch B.

```
[SW8800] Router id 172.17.1.2
[SW8800] ospf
[3Com-ospf-1] area 0
[3Com-ospf-1-area-0.0.0.0] network 172.17.0.0 0.0.255.255
```

Troubleshooting MPLS Configuration

Symptom: Session cannot be setup with the peer after LDP is enabled on the interface.

Troubleshooting:

Cause 1: Loop detection configuration is different at the two ends.

Solution: Check loop detection configuration at both ends to see if one end is configured while the other end is not (this will result in session negotiation failure).

Cause 2: Local machine cannot get the route to peer LSR ID, so TCP connection cannot be set up and session cannot be established.

Solution: The default address for session transfer is MPLS LSR ID. The local machine should issue the LSR ID route (often the Loopback address) and lean the peer LSR ID route.

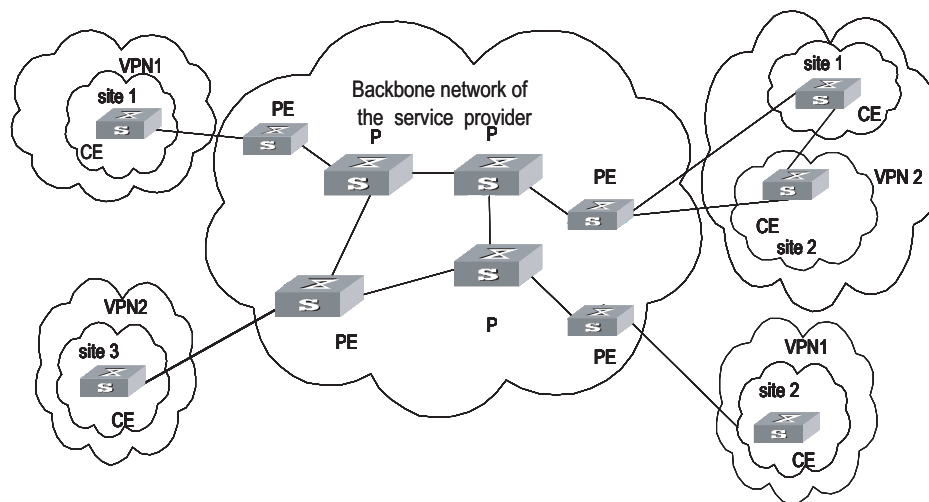
BGP/MPLS VPN Overview

Traditional VPN, for which layer 2 tunneling protocols (L2TP, L2F and PPTP, and so on.) or layer 3 tunnel technology (IPSec, GRE and so on.) is adopted, is a great success and is therefore widely used. However, along with the increase of the size of VPNs, the deficiency of traditional VPN in such aspects as expansibility and manageability becomes more and more obvious. In addition, QoS (Quality of Service) and security are also the difficult problem for traditional VPN.

Using the MPLS technology, service providers can implement the IP-based VPN services easily and enable their networks to meet the expansibility and manageability requirement for VPN. The VPN constructed by using MPLS also provides the possibility for the implementation of value-added service. Multiple VPNs can be formed from a single access point, and each VPN represents a different service, making the network able to transmit services of different types in a flexible way.

Product currently provides comparatively complete BGP/MPLS VPN networking capabilities:

- Address isolation, allowing the overlap of address of different VPNs and public networks.
- Supporting MBGP advertising VPN routing information through public network, establishing BGP/MPLS VPN.
- Forwarding VPN data stream over MPLS LSP.
- Providing MPLS VPN performance monitoring and fault detecting tools.

BGP/MPLS VPN Model BGP/MPLS VPN model**Figure 127** MPLS VPN model

As shown in Figure 127, MPLS VPN model contains three parts: CE, PE and P.

- CE (Customer Edge) device: It is a composing part of the customer network, which is usually connected with the service provider directly through an interface. It may be a router or a switch which cannot sense the existence of VPN.
- PE (Provider Edge) router: It is the Provider Edge router, namely the edge device of the provider network, which connects with your CE directly. In MPLS network, PE router processes all the operations for VPN. PE needs to possess MPLS basic forwarding capability.
- P (Provider) router: It is the backbone router in the provider network, which is not connected with CE directly. P router needs to possess MPLS basic forwarding capability.

The classification of CE and PE mainly depends on the range for the management of the provider and the customer, and CE and PE are the edges of the management ranges.

Nested BGP/MPLS VPN model

In a basic BGP/MPLS VPN model, the PEs are in the network of the service provider and are managed by the service provider.

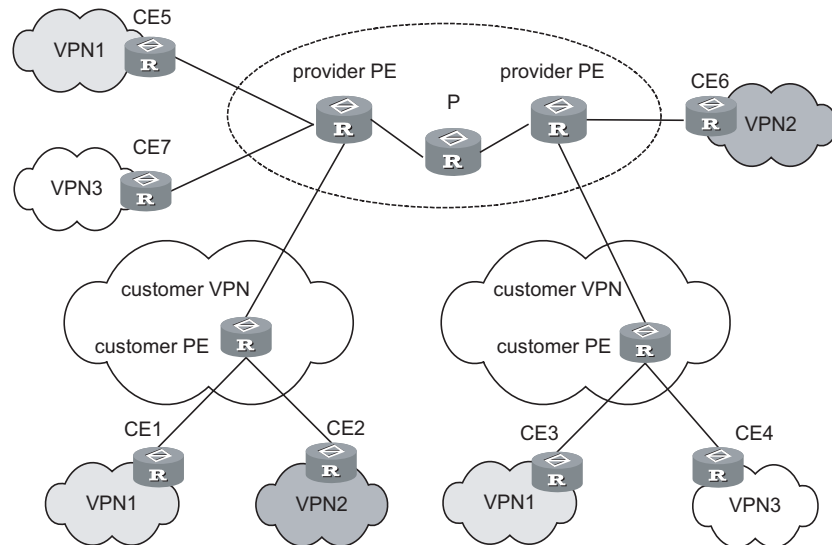
When a VPN user wants to subdivide the VPN into multiple VPNs, the traditional solution is to configure these VPNs directly on the PEs of the service provider. This solution is easy to implement, but has the following disadvantages: the number of the VPNs carried on PEs may increase rapidly; the operator may have to perform more operations when required by a user to adjust the relation between the user's internal VPNs. These disadvantages not only increase the network operating cost, but also bring relevant management and security issues.

The nested VPN is a better solution. Its main idea is to transfer VPNv4 route between PE and CE of common BGP MPLS/VPN such that user themselves can

manage their internal VPN division, and the service provider can be saved from participating into users' internal VPN management.

The following figure shows the network model for nested VPN:

Figure 128 Network model for nested BGP/MPLS VPN



Basic concepts in BGP/MPLS VPN

1 VPN-instance

VPN-instance is an important concept in VPN routing in MPLS. In an MPLS VPN implementation, each site corresponds to a specific VPN-instance on PE (their association is implemented by binding VPN-instance to the VALN interface). If subscribers on one site belong to multiple VPNs, then the corresponding VPN-instance includes information about all these VPNs.

Specifically, such information should be included in VPN-instance: label forwarding table, IP routing table, the interfaces bound with VPN-instance, and the management information (RD, route filtering policy, member interface list, and so on). It includes the VPN membership and routing rules of this site.

PE is responsible for updating and maintaining the relationship between VPN-instance and VPN. To avoid data leakage from the VPN and illegal data entering into the VPN, each VPN-instance on the PE has an independent set of routing table and label forwarding table, in which the forwarding information of the message is saved

2 MBGP

MBGP (multiprotocol extensions for BGP-4, see RFC2283) propagates VPN membership information and routes between PE routers. It features backward compatibility: It not only supports traditional IPv4 address family, but also supports other address families, for example, VPN-IPv4 address family. MP-BGP ensures that VPN private routes are only advertised within VPNs, as well as implementing communication between MPLS VPN members.

3 VPN-IPv4 address

VPN is just a private network, so it can use the same IP address to indicate different sites. But the IP address is supposed as unique when MP-BGP advertises CE routes between PE routers, so routing errors may occur for the different meaning in two systems. The solution is to switch IPv4 addresses to VPN-IPv4 address to generate globally unique addresses before advertising them, so PE routers is required to support MP-BGP.

A VPN-IPv4 address consists of 12 bytes, and the first eight bytes represent the RD (Route Distinguisher), which are followed by a 4-byte IPv4 address. The service providers can distribute RD independently. However, their special AS (Autonomous System) number must be taken as a part of the RD. After being processed in this way, even if the 4-byte IPv4 address contained in VPN-IPv4 address has been overlapped, the VPN-IPv4 address can still maintain globally unique. RD is only used within the carrier network to differentiate routes. When the RD is 0, a VPN-IPv4 address is just a IPv4 address in general sense.

The route received by PE from CE is the IPv4 route that needs to be redistributed into VPN-instance routing table, and in this case a RD needs to be added. It is recommended that the same RD be configured for all routes from the same user site.

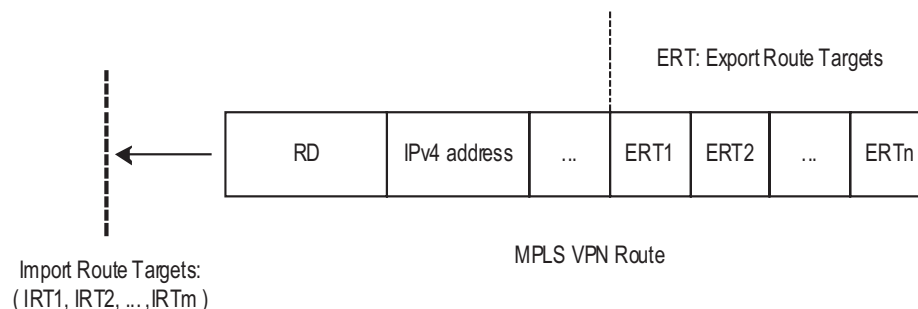
VPN Target attribute

VPN Target attribute is one of the MBGP extension community attributes and is used to limit VPN routing information advertisement. It identifies the set of sites that can use some route, namely by which Sites this route can be received, and the PE router can receive the route transmitted by which Sites. The PE routers connected with the site specified in VPN Target can all receive the routes with this attribute.

For PE routers, there are two sets of VPN Target attributes: one of them, referred to as Export Targets, is added to the route received from a direct-connect site in advertising local routes to remote PE routers. And the other one, known as Import Targets, is used to decide which routes can be imported into the routing table of this site in receiving routes from remote PE routers.

When matching the VPN Target attribute carried by the route to filter the routing information received by the PE router, if the export VPN target set of the received route contains identical items with the import VPN target set of the local end, the route is imported into the VPN routing table and then advertised to the connected CE . Otherwise, the route will be rejected.

Figure 129 Route filtering through matching VPN Target attribute





The routes for other VPNs will not appear in the VPN's routing table by using VPN Target attribute to filter routing information received at PE router, so the CE-transmitted data will only be forwarded within the VPN.

BGP/MPLS VPN Implementation

BGP/MPLS VPN works on this principle: It uses BGP to propagate VPN private routing information on carrier backbone network, and uses MPLS to forward VPN service traffic.

The following are introductions to BGP/MPLS implementation from two aspects: advertising VPN routing information and forwarding VPN packets.

Advertising VPN routing information

Routing information exchange has the following four types:

1 Between CE and PE

A PE router can learn routing information about the CE connected to it through static route, RIP (supporting multi-instance), OSPF (supporting multi-instance) or EBGP, and imports it in a vpn-instance.

2 Between ingress PE and egress PE

The ingress PE router uses MP-BGP to send information across public network: It advertises routing information learned from CE to the egress PE router (with MPLS label) and learns the CE routing information learned at the egress PE router.

The internal connectivity among the VPN internal nodes is ensured through enabling IGP (for example, RIP and OSPF) or configuring static routes on the PEs.

3 LSP setup between PEs

LSPs must be set up between PEs for VPN data traffic forwarding with MPLS LSP. The PE router which receives packets from CE and create label protocol stack is called Ingress LSR, while the BGP next hop (Egress PE router) is Egress LSR. Using LDP to create fully connected LSPs among PEs.

4 Between PE and CE

A CE can learn remote VPN routes from the PE connected through static routes, RIP, OSPF or EBGP.

With above-mentioned steps, reachable routes can be established between CEs, for transmission of VPN private routing information over public network.

Forwarding VPN packets

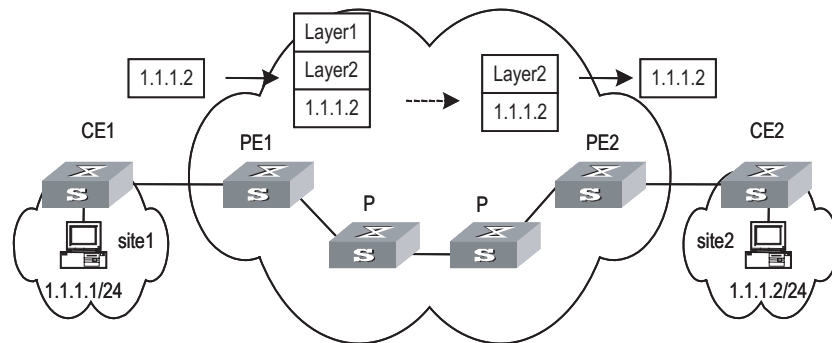
On the ingress PE, two-layer label stack is formed for each VPN packet:

Interior-layer label, also called MPLS label, is at the bottom of the label stack and distributed by M-BGP when the egress PE advertises routing information (in VPN forwarding table) to ingress GE. When VPN packets from public network reach the CE, they can be forwarded from the designated interface to the designated CE or site by searching for the target MPLS forwarding table according to the labels contained.

Exterior-layer label, known as LSP initialization label, distributed by MPLS LDP, is at the top of the label stack and indicates an LSP from the ingress PE to egress PE. By the switching of exterior-layer label, VPN packets can be forwarded along the LSP to the peer PE.

Figure 130 illustrates the details:

Figure 130 Forwarding VPN packets



- 1 Site 1 sends an IPv4 packet with the destination address 1.1.1.2 of to CE1. CE1 looks up the IP routing table for a matched entry and sends the packet to PE1 according to the matched entry.
- 2 Depending on the interface the packet reaches and the destination of it, PE1 looks up the VPN-instance entry to obtain interior-layer label, exterior-layer label, BGP next hop (PE2), and output interfaces. After the establishment of labels, PE1 forwards MPLS packets to the first P of LSP through output interface.
- 3 Each P router on LSP forwards MPLS packets using exterior-layer label to the penultimate-hop router, namely the P router before PE2. The penultimate-hop router extracts the exterior-layer and sends MPLS packet to PE2.
- 4 PE2 looks up in the MPLS forwarding table according to the interior-layer label and destination address to determine the egress interface for labeling operation and the packet. It then extracts the interior-layer label and forwards through the egress interface the IPv4 packet to CE2.
- 5 CE2 looks up in the routing table and sends the packet in normal IPv4 packet forwarding mode to the site2.

Nested BGP/MPLS VPN Implementation

When implementing a nested BGP/MPLS VPN, pay attention to the following items:

- No address overlap is allowed between user's internal sub-VPNs.
- To ensure the VPN routing information is correctly advertised over the backbone network, the VPN-Targets of the user VPN and the internal sub-VPNs cannot be overlapped and must be specified by the service provider.
- The provider PE and the customer PE must be directly connected and cannot exchange VPNv4 route in Multihop-EBGP mode.

Before configuring a nested BGP/MPLS VPN, you must complete the following tasks:

- Configuring IGP on the MPLS backbone network (including provider PE and P routers) to implement the IP connectivity on the backbone network.

- Configuring basic MPLS capability on the MPLS backbone network.
- Configuring MPLS LDP and setting up LDP LSP on the MPLS backbone network.
- Configuring BGP on the MPLS backbone network (create IBGP peers between provider PEs).
- Configuring basic MPLS capability on user-end network (including customer PEs).

Hierarchical BGP/MPLS VPN Implementation

As PE is required to aggregate multiple VPN routes on a BGP/MPLS VPN, it is prone to forming a bottleneck in a large-scale deployment or in the case that PE capacity is small. To solve the problem, 3Com Corporation introduced the HoVPN (Hierarchy of VPN, Hierarchical BGP/MPLS VPN) solution.

Hierarchical BGP/MPLS VPN divides an MPLS VPN into several MPLS VPNs in a hierarchical network structure. Each VPN takes on a role depending on its level. There are high performance requirements in routing and forwarding on the PEs at the higher level of MPLS VPN, because they are primarily used for connecting the backbone networks and providing access service for huge VPN clients. However, such requirements are relatively low for PEs at the lower level of the network as they primarily function to access the VPN clients at the edges. Congruous with the IP network model, HoVPN model improves the scalability of BGP/MPLS VPN, and hence allows lower-layer MPLS VPNs comprising low-end equipment to provide MPLS VPN accessing and interconnect through the high-end MPLS VPN backbone.

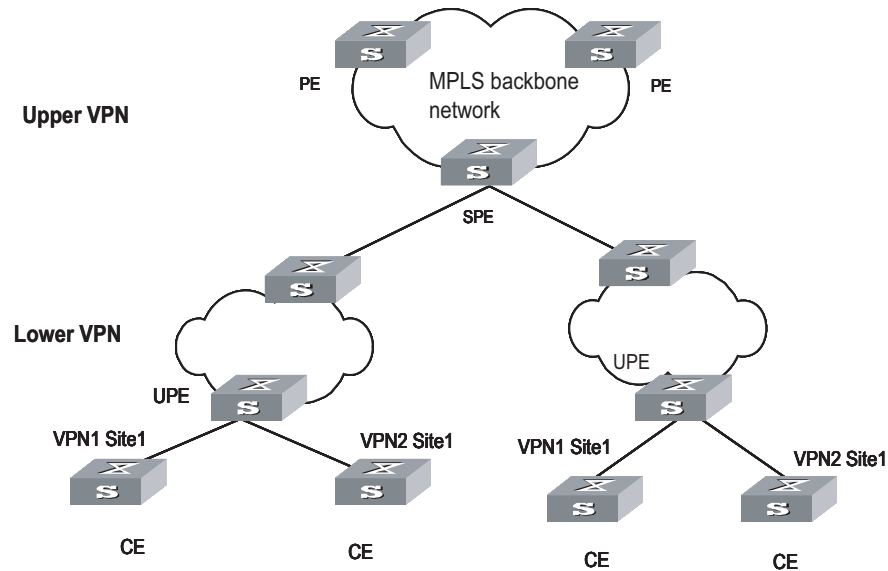
As shown in Figure 131, the PEs directly connected with user devices are called UPE (underlayer PE or user-end PE); the devices in the core network connected with the UPEs are called SPE (superstratum PE or service-provider-end PE).

Hierarchical PEs have the same appearance as that of the traditional PEs and can coexist with other PEs in the same MPLS network.

UPEs are responsible for user access; they only maintain the routes of directly connected VPN sites, but not that of the remote sites. SPEs, however, are responsible for the maintenance and advertisement of VPN routes; they maintain all the routes of the VPNs connected by their UPEs, including the routes in both local and remote sites.

UPE and SPE are relative concepts. In a multi-layer PE architecture, an upper layer PE is an SPE for its lower layer PE, and a lower layer PE is an UPE for its upper layer PE.

The MBGP runs between SPE and UPE can be either MP-IBGP or MP-EBGP, depending on whether the SPE and the UPE are in the same AS.

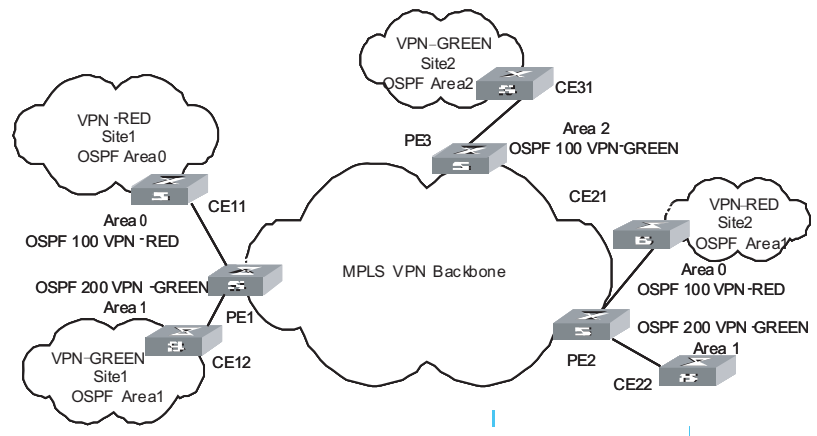
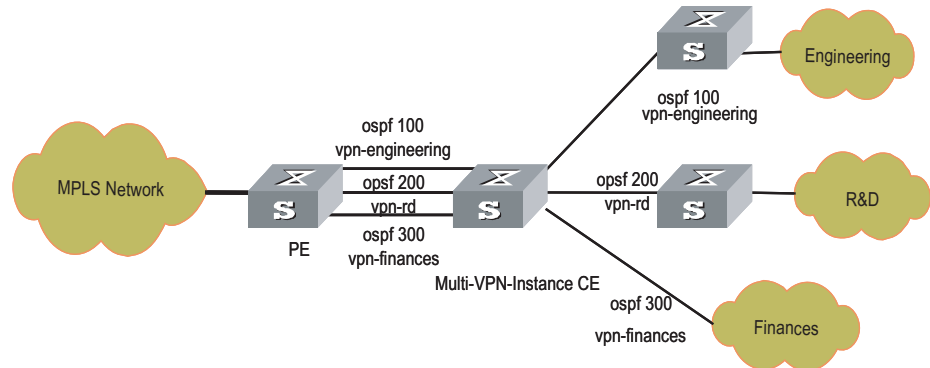
Figure 131 Hierarchical BGP/MPLS VPN

Introduction to OSPF Multi-instance

As one of the most popular IGP routing protocols, OSPF is used as an internal routing protocol in many VPNs. Using OSPF on PE-CE links brings convenience to you because in this case CE routers only need to support OSPF protocol, without the need of supporting other protocols, and network administrator only have to know the OSPF protocol. If you want to transform conventional OSPF backbone into BGP/MPLS VPN, using OSPF between PE and CE can simplify this transform process.

Therefore IETF raised two new OSPF VPN extension drafts, to provide a complete solution to SPPF problems in BGP/MPLS VPN application when OSPF is used as PE-CE routing protocol. In this case, PE router must be able to run multiple OSPF instances, each of which corresponds to one VPN instance, owns an individual interface, routing table, and sends VPN routing information over MPLS network using BGP/OSPF interaction.

If supporting OSPF multi-instance, one router can run multiple OSPF processes, which can be bound to different VPN instances. In practice, you can create one OSPF instance for each service type. OSPF multi-instance can fully isolate different services in transmission, which can solve security problems with low cost to meet the needs of customers. Generally, OSPF multi-instance is run on PEs; The CE running OSPF multi-instance in the LAN is called multi-VPN-instance CE. At present, isolation of LAN services implements by VLAN function of the switch. OSPF Multi-VPN-Instance CE provides schemes of services isolation implemented on routers.

Figure 132 OSPF multi-instance application in MPLS/BGP VPN PE**Figure 133** Multi-VPN-instance CE application in conventional LAN

Introduction to Multi-Role Host

The VPN attribute of the packets from a CE to its PE lies on the VPN bound with the ingress interface. This, in fact determines that all the CEs forwarded by the PE through the same ingress interface belong to the same VPN; but in actual network environments, a CE may need to access multiple VPNs through one physical interface. Though you can configure different logical interfaces to meet this need, this compromised method brings additional configuration burden and has limitation in actual use.

To resolve this problem, the idea of multi-role host is generated. Specifically to say, this idea is to differentiate the accesses to different VPNs through configuring policy routing based on IP addresses, and transmit downstream data flow from PE to CE by configuring static routing. The static routing under multi-role host circumstance is different from common hosts; it is implemented by specifying an interface of another VPN as the egress interface through a static route in a VPN; and thus allowing one logical interface to access multiple VPNs.

BGP/MPLS VPN Configuration

Configuring Various Kinds of Routers

Implementing BGP/MPLS VPN functions requires the following procedures in general: Configure basic information on PE, CE and P; establish the logical or

physical link with IP capabilities from PE to PE; advertise and update VPN network information.

CE router

The configuration on CE is relative simple. Only static route, RIP, OSPF or EBGp configuration is needed for VPN routing information exchange with the PE connected, MPLS configuration is not needed.

PE router

The configuration on PE is relative complex. After the configuration, the PE implements MPLS/BGP VPN core functions.

The following sections describe the configuration tasks on a PE device:

- "Configuring basic MPLS capability"
- "Defining BGP/MPLS VPN site"
- "Configuring PE-CE route exchanging"
- "Configuring PE-PE route exchanging"

P router

The configuration on P device is relative simple. The main task is to configure MPLS basic capacity on the P device to support LDP and MPLS forwarding.

The following are detailed configurations.

Configuring CE Router

As a customer-side device, only basic configuration is required on a CE router, for routing information exchange with PE router. Currently route switching modes available include static route, RIP, OSPF, EBGp, and so on.

Creating static route

If you select static route mode for CE-PE route switching, you should then configure a private static route pointing to PE on CE.

Perform the following configuration in the system view.

Table 523 Create/delete a static route in VPN instance routing table

Operation	Command
Create a specified VPN-instance static route	ip route-static <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-name</i> <i>gateway-address</i> } [preference <i>preference-value</i>] [reject blackhole]
Delete a specified VPN-instance static route	undo ip route-static <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-name</i> <i>gateway-address</i> } [preference <i>preference-value</i>]

By default, the preference value for a static route is 60. You can also specify preference for a static route.

Configuring RIP

If you select RIP mode for CE-PE route switching, you should then configure RIP on CE. For detailed RIP configuration steps, see the RIP configuration part in routing

protocol in *3Com Switch 8800 Family Series Routing Switches Operation Manual Volume I*.

Configuring OSPF

If you select OSPF mode for CE-PE route switching, you should then configure OSPF on CE. For configuring OSPF, see the routing protocol part in *3Com Switch 8800 Family Series Routing Switches Operation Manual Volume II*.

You must configure OSPF multi-instance to isolate services of different VPNs on CE router, which is now called Multi-VPN-Instance CE.

You can bind OSPF processes with VPN with the following command in OSPF view.

Table 524 Configure the router as multi-VPN-instance CE

Operation	Command
Configure the router as multi-VPN-instance CE	vpn-instance-capability simple
Remove the configuration	undo vpn-instance-capability

Configuring EBGp

If you select BGP mode for CE-PE route switching, you should then configure EBGp peer, import direct-connect route, static route and other IGP routes, for BGP to advertise VPN routes to PE.

Configuring PE Router

Configuring basic MPLS capability

It includes configuring MPLS LSR ID, enable MPLS globally and enable MPLS in the corresponding VLAN interface view.

Refer to Chapter 2 MPLS Basic Capacity Configuration for details.

Defining BGP/MPLS VPN site

1 Create VPN-instance and enter VPN-instance view

The VPN instance is associated with a site. The VPN membership and routing rules of a site is configured in the corresponding VPN instance.

This command is used to create a new VPN-instance and enter the VPN-instance view, or directly enter the VPN-instance view if the VPN-instance already exists.

Perform the following configuration in the system view.

Table 525 Create a VPN-instance and enter VPN-instance view

Operation	Command
Create a VPN-instance and enter VPN-instance view	ip vpn-instance <i>vpn-instance-name</i>
Delete a VPN-instance	undo ip vpn-instance <i>vpn-instance-name</i>

By default, no VPN-instance is defined.

1 Configure RD for the vpn-instance

After PE router is configured with RD, when a VPN route learned from CE is imported into BGP, BGP attaches the RD in front of the IPv4 address. Then the general IPv4 address which may overlaps between several VPN IPv4 addresses in the VPN is turned into a globally unique VPN IPv4 address and thus ensure the correct routing in the VPN.

Perform the following configuration in VPN-instance view.

Table 526 Configure RD for the VPN-instance

Operation	Command
Configure RD for the VPN-instance	route-distinguisher <i>route-distinguisher</i>

The parameter in the above command has no default value. A VPN-instance works only when a RD is configured for it. Other parameters for a VPN-instance cannot be configured before configuring a RD for it.

To modify the RD, you must first delete the VPN-instance and reconfigure it.

2 Configure VPN-instance description

Perform the following configuration in VPN-instance view

Table 527 Configure VPN-instance description

Operation	Command
Configure VPN-instance description	description <i>vpn-instance-description</i>
Delete VPN-instance description	undo description

3 Configure VPN-target attribute for the VPN-instance

VPN-target attribute, a BGP extension community attribute, controls advertisement of VPN routing information.

The following is the advertisement controlling process of VPN routing information:

- When BGP is imported into a VPN route learned at CE, it associates a VPN-target extension community attribute list for the route. Usually the list is the VPN-instance output routing attribute list which is associated with CE.
- VPN instance defines input routing attribute list according to the **import-extcommunity** in VPN-target, defines the acceptable route range and import it.
- VPN instance modifies VPN-target attributes for the routes to be advertised, according to the **export-extcommunity** in VPN-target.

Like an RD, an extension community includes an ASN plus an arbitrary number or an IP address plus an arbitrary number. There are two types of formats:

The first one is related to autonomous system number (ASN), in the form of 16-bit ASN (can be 0 here): 32-bit user-defined number, for example, 100:1.

The second one is related to IP address, in the form of 32-bit IP address (can be 0.0.0.0 here): 16-bit user-defined number, for example, 172.1.1.1:1.

Perform the following configuration in the VPN-instance view.

Table 528 Create VPN-target extended community for the VPN-instance

Operation	Command
Configure VPN-target extended community for the VPN-instance	vpn-target <i>vpn-target-extcommunity</i> [import-extcommunity export-extcommunity both]
Delete the specified VPN-target attribute from the VPN-target attribute list associated with the VPN-instance	undo vpn-target <i>vpn-target-extcommunity</i> [import-extcommunity export-extcommunity both]

By default, the value is **both**. In general all Sites in a VPN can be interconnected, and the **import-extcommunity** and **export-extcommunity** attributes are the same, so you can execute the command only with the **both** option.

Up to 16 VPN-targets can be configured with a command, and up to 20 *vpn-targets* can be configured for a VPN-instance.

4 Limit the maximum number of routes in a VPN-instance

This command is used to limit the maximum number of routes for a VPN-instance so as to avoid too many routes imported from a Site.

Perform the following configuration in the VPN-instance view.

Table 529 Limit the maximum number of routes in the VPN-instance

Operation	Command
Limit the maximum number of routes in the VPN-instance	routing-table limit <i>integer</i> { <i>alarm-integer</i> syslog-alert }
Remove the maximum number limitation	undo routing-table limit

Integer is in the range of 1 to 65536 and *alarm-integer* is in the range of 1 to 100.



*Changing the maximum route limit for VPN-instance will not affect the existing routing table. To make the new configuration take effect immediately, you should rebuild the corresponding routing protocol or perform **shutdown/undo shutdown** operation on the corresponding interface.*

5 Configure vlan-id larger than 1024 on the fast Ethernet port of Trunk type (Optional)

Configure *vlan-id* larger than 1024, with the range of MPLS/VPN VLANs allowed to pass the port from *vlan-id* to *vlan-id* + 1023

Perform the following configuration in Ethernet port view.

Table 530 Configure the vlan-id range of MPLS/VPN VLANs allowed

Operation	Command
Configure the <i>vlan-id</i> range of MPLS/VPN VLANs allowed to pass Trunk fast Ethernet ports	port trunk mpls vlan from <i>vlan-id</i> [to] <i>vlanid</i>
Remove the configured <i>vlan-id</i> range of MPLS/VPN VLANs allowed to pass Trunk fast Ethernet ports	undo port trunk mpls

By default, the *vlan-id* range of MPLS/VPN VLANs is from 0 to 1023, and the default value of *vlan-id* is 0. The value range of *vlan-id* is from 1 to 3071.

**CAUTION:**

- This command can only be executed on Trunk ports, and MPLS/VPN-enabled VLANs and VLANs out of the configured range are excluded..
- Set the VPN range for the cards and set the range of MPLS/VPN VLAN *vlan-id* on the interface of the card to 1 to 4094.

Perform the following configuration in system view.

Table 531 Configure the MPLS/VPN VLAN *vlan-id* range for the card

Operation	Command
Enable the 4K VPN-range for the card	vlan vpn-range slot <i>slot-number</i> enable
Disable the 4K VPN-range for the card	undo vlan vpn-range slot <i>slot-number</i> enable

**CAUTION:**

- This command is actually effective for only the first 12 ports on the card. When you configure MPLS/VPN VLAN *vlan-id* on subsequent ports, only the MPLS/VPN VLAN range enabled for one VLAN will take effect. If you remove MPLS/VPN configuration from an active port, no subsequent port will take effect automatically either, and you have to reconfigure the ports to update their states.
- Restart the card after issuing a command or its corresponding undo command to ensure that the configuration takes effect.
- After you cancel card configuration, if the VLAN configured on a port exceeds 1K, which is the default value, the configuration will be deleted automatically.
- In aggregation mode, VPN-range configuration will not be synchronized automatically and you can manually make/remove the configuration on an individual port.
- Set the VPN range for the ports and set the range of MPLS/VPN VLAN *vlan-id* on the ports to 1 to 4094.

Perform the following configuration in Ethernet interface view.

Table 532 Configure the MPLS/VPN VLAN *vlan-id* range for the interface

Operation	Command
Enable the 4K vpn-range for the interface	port vpn-range share-mode enable

Table 532 Configure the MPLS/VPN VLAN vlan-id range for the interface

Operation	Command
Disable the 4K vpn-range for the interface	undo port vpn-range share-mode enable

**CAUTION:**

- Ports supporting this function stop supporting the application of ACL rules.
- Associate interface with VPN-instance

VPN instance is associated with the direct-connect Site through interface binding. When the packets from the Site reach the PE router through the interface bound, then the PE can look routing information (including next hop, label, egress interface, and so on.) up in the corresponding VPN-instance.

This command can associate a VPN-instance with an interface.

Perform the following configuration in VLAN interface view.

Table 533 Associate interface with VPN-instance

Operation	Command
Associate interface with VPN-instance	ip binding vpn-instance <i>vpn-instance-name</i>
Remove the association of the interface with VPN-instance	undo ip binding vpn-instance <i>vpn-instance-name</i>



CAUTION: As executing the **ip binding vpn-instance** command on an interface will delete the IP address of the interface, you must configure the IP address of the interface after executing that command when you bind the interface with a VPN-instance.

Configuring PE-CE route exchanging

These route exchanging modes are available between PE and CE: static route, RIP, OSPF, EBGp.

1 Configure static route on PE

You can configure a static route pointing to CE on PE for it to learn VPN routing information from CE.

Perform the following configuration in the system view.

Table 534 Create/Delete static route in VPN-instance routing table

Operation	Command
Create the static route of a specific VPN-instance	ip route-static vpn-instance <i>vpn-instance-name1</i> <i>vpn-instance-name2</i> ... <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-name</i> [vpn-instance <i>vpn-nexthop-name</i> <i>vpn-nexthop-address</i>] } [preference <i>preference-value</i> public] [reject blackhole]
Delete a static route of a specific VPN-instance	undo ip route-static vpn-instance <i>vpn-instance-name1</i> <i>vpn-instance-name2</i> ... <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-name</i> [vpn-instance <i>vpn-nexthop-name</i> <i>vpn-nexthop-address</i>] } [preference <i>preference-value</i> public] [reject blackhole]

By default, the preference value for a static route is 60. You can also specify another preference for the static route you are configuring.

2 Configure RIP multi-instance

If you select RIP mode for CE-PE route switching, you should then specify running environment for RIP instance on PE. With this command, you can enter RIP view and import and advertise RIP instance in the view.

Perform the following configuration in the RIP view.

Table 535 Configure PE-CE RIP instance

Operation	Command
Create PE-CE RIP instance	ipv4-family [unicast] vpn-instance <i>vpn-instance-name</i>
Delete PE-CE RIP instance	undo ipv4-family [unicast] vpn-instance <i>vpn-instance-name</i>

Then configuring RIP multi-instance to import IBGP route.

For details about RIP configuration, see RIP configuration section in Routing Protocol of this manual.

3 Configure OSPF multi-instance on PE

If you select OSPF mode for CE-PE route switching, you should then configure OSPF multi-instance on PE. Other configurations, such as MPLS basic configuration, VPN-instance configuration, do not change. Noted that when OSPF routes and direct-connect routes are imported in the VPN instance address family view, BGP routes should also be imported into OSPF. Here only introduces OSPF multi-instance configuration in detail.

First step: Configure OSPF process.

Perform the following configuration in the system view.

Table 536 Configure OSPF process

Operation	Command
Configure an OSPF process	ospf <i>process-id</i> [router-id <i>router-id-number</i>] [vpn-instance <i>vpn-instance-name</i>]
Delete an OSPF process	undo ospf <i>process-id</i>

By default, the process index is 1.



CAUTION: An OSPF process can only belong to one VPN instance, while one VPN instance may contain multiple OSPF processes. By default, an OSPF process belongs to public network.

Step 2: Configure Domain ID

The Domain ID is used to identify an OSPF autonomous system (AS), and the same OSPF domain must have the same Domain ID. One process can be configured with only one Domain ID; different processes can be configured with the same Domain ID or different Domain IDs.

Perform the following configuration in the OSPF view.

Table 537 Configure Domain ID

Operation	Command
Configure Domain ID	domain-id { <i>id-number</i> <i>id-addr</i> }
Return to the default value	undo domain-id

By default, *id-number* is 0 and *id-addr* is 0.0.0.0.

It is recommended that all OSPF instances in a VPN are configured with either the same domain ID or the default value.



CAUTION: The configured value will not take effect until the command **reset ospf** is executed.

Step 3: Configure tag for imported VPN route (optional)

If a VPN Site links to multiple PEs, routing ring may present when the routes learned by MPLS/BGP are received by another PE router in being advertised by category-5/-7 LSA of a PE to the VPN Site. To solve this problem, you should configure Route-tag. It is recommended to configure identical Route-tag for the PEs in the same VPN.

Perform the following configuration in the OSPF view.



CAUTION: The configured Route-tag will not take effect until the command **reset ospf** is executed.

Table 538 Configure tag for imported VPN route

Operation	Command
Configure tag for imported VPN route	route-tag <i>tag-number</i>
Return to the default value	undo route-tag

tag-number is used to identify Tag value; by default, the first two bytes are fixed, that is, 0xD000, and the last two bytes is AS number of local BGP. For example, the AS number of local BGP is 100, and then its default tag value is 3489661028 in decimal notation. This value is an integer ranging from 0 to 4294967295.

Step 4: Configure Sham-link (optional)

Sham-links are required between two PEs when Backdoor links (that is, the OSPF links that do not pass through the MPLS backbone network) exist between the two PEs and data is expected to be transported over the MPLS backbone. A Sham-link between two PEs is considered as a link in OSPF domain. Its source and destination addresses are both the Loopback interface address with 32-bit mask, but this Loopback interface should be bound to a VPN instance and direct routes must be imported into BGP by BGP. OSPF processes of the VPN cannot directly import the routes of the Loopback interface (so the **import direct** command cannot be executed in an OSPF processes of VPN); instead, an OSPF process can only advertise the route indirectly by importing a BGP route.

Perform the following configuration in the OSPF area view.

Table 539 Configure Sham-link

Operation	Command
Configure Sham-link	sham-link <i>source-addr destination-addr</i> [cost <i>cost-value</i>] [simple <i>password</i> md5 <i>keyid key</i>] [dead <i>seconds</i>] [hello <i>seconds</i>] [retransmit <i>seconds</i>] [trans-delay <i>seconds</i>]
Delete a Sham-link	undo sham-link <i>source-addr destination-addr</i>

By default, the cost value is 1, dead value is 40 seconds, hello value is 10 seconds, retransmit value is 5 seconds and trans-delay value is 1 second.

4 Configure EBGP on PE

If you select EBGP between PE and CE, you should configure a neighbor for each VPN in VPN instance address family sub-view, and import IGP route of CE.

Step 1: Configure peer group

Configuring peer group in VPN instance address family view.

Table 540 Configure peer group

Operation	Command
Configure a peer group	group <i>group-name</i> [internal external]
Delete the specified peer group	undo group <i>group-name</i>

By default, the peer group is configured as internal. When BGP mode is used for PE-CE route switching, they often belong to different ASs, so you should configure EBGP peer as external.

Step 2: Configure AS number for a specific neighbor and add group member to a peer group

When EBGP mode is used for PE-CE route switching, you should configure AS number for a specific neighbor for every CE VPN-instance.

Perform the following configuration in VPN instance address family view.

Table 541 Configure AS number for a specific neighbor

Operation	Command
Configure AS number for a specific neighbor	peer { <i>group-name</i> [<i>peer-address</i> group <i>group-name</i>] } as-number <i>as-number</i>
Delete the AS number of a specific neighbor	undo peer { <i>group-name</i> [<i>peer-address</i> group <i>group-name</i>] } as-number <i>as-number</i>

Step 3: Activate peer (group)

By default, BGP neighbor is active while MBGP neighbor is inactive. You should activate MBGP neighbor in VPNv4 sub-address family view.

Perform the following configuration in VPNv4 sub-address family view.

Table 542 Activate/deactivate peer (group)

Operation	Command
Activate the peer (group)	peer group-name enable
Deactivate the peer (group)	undo peer group-name enable

Step 4: Configure MBGP to import VPN route of direct-connect CE

To advertise correct VPN route over public network to other PEs with which BGP adjacency has been created, a PE must import the VPN routing information of the direct-connect CE into its MBGP routing table.

For example, if a static route is used between PE and CE, PE must import a static route in VPN-instance address family sub-view of MBGP (**import-route static**). If RIP is run between PE and CE, PE must import an RIP route in VPN-instance view of MBGP (**import-route rip**). If BGP is run between PE and CE, MBGP imports a direct-connect route.

Perform the following configuration in VPN instance address family sub-view.

Table 543 Import IGP route

Operation	Command
Import IGP route	import-route protocol [<i>process-id</i>] [med med]
Remove IGP route import	undo import-route protocol

Step 5: Configure BGP as asynchronous.

Perform the following configuration in VPN instance address family sub-view.

Table 544 Configure BGP asynchronous with IGP

Operation	Command
Configure BGP asynchronous with IGP	undo synchronization

By default, BGP is in asynchronous mode.

Step 6: Permit route loop configuration in Hub&Spoke networking (optional)

Generally speaking, PE-CE configuration is completed after you specify the AS number of neighbor; for the rest configuration, you can keep the system default values.

In the case of standard BGP, BGP tests routing loop via AS number to avoid generating routing loop. In the case of Hub&Spoke networking, however, PE carries the AS number of the local autonomous system when advertising the routing information to CE, if EBGP is run between PE and CE. Accordingly, the updated routing information will carry the AS number of the local autonomous system when route update is received from CE. In this case, PE will not accept the route update information.

This phenomenon can be avoided by executing the **peer allow-as-loop** command, which makes the PE still receives the route update information containing the local AS number from CE.

Perform the following configuration in IPv4 instance sub-address family view.

Table 545 Configure to allow/disable routing loop

Operation	Command
Configure to allow routing loop	peer { <i>group-name</i> <i>peer-address</i> } allow-as-loop <i>asn-limit</i>
Configure to disable routing loop	undo peer { <i>group-name</i> <i>peer-address</i> } allow-as-loop <i>asn-limit</i>

By default, the received route update information is not allowed to generate loop information.

Step 7: Configure BGP features.

Configuring PE-PE route exchanging

To exchange VPN-IPv4 routing information between PEs, you should configure MP-IBGP on PEs.

Perform the following configuration in BGP view or PVN instance address family sub-view.

1 Configure IBGP

These steps are often required.

Step 1: Configure BGP as asynchronous.

Step 2: Configure BGP neighbor.

Note that BGP adjacency is established through Loopback interface and the sub-net mask must be 32 bits.

Step 3: Permit BGP session over any operable TCP interface.

In general, BGP uses the best local address in TCP connection. To keep TCP connection available even when the interface involved fails, you can perform the following configuration to permit BGP session over any interface through which TCP connection with the peer can be set up. The command here is usually executed together with the Loopback interface.

Perform the following configuration in VPNv4 sub-address family view.

Table 546 Permit BGP session over any operable TCP interface

Operation	Command
Permit BGP session over any operable TCP interface	peer { <i>peer-address</i> <i>group-name</i> } connect-interface { <i>interface-type</i> <i>interface-number</i> }
Use the best local address for TCP connection	undo peer { <i>peer-address</i> <i>group-name</i> } connect-interface

BGP creates BGP adjacency to the peer end using specific interfaces, which is usually the loopback interface. Because this interface is always in the up state, thus it reduces the strike brought by network shock.

2 Configure MP-IBGP

Step 1: Enter protocol address family view.

Perform the following configuration in BGP view.

Table 547 Configure VPNv4 address family

Operation	Command
Enter VPNv4 sub-address family view	ipv4-family vpnv4 [unicast]
Delete VPNv4 sub-address family view configuration	undo ipv4-family vpnv4 [unicast]

Step 2: Activate the peer (group).

By default, BGP neighbor is active while MBGP neighbor is inactive. You must enable MBGP neighbor in VPNv4 sub-address family view.

Table 548 Enable/disable IBGP peer group

Operation	Command
Enable a peer group	peer group-name enable
Disable a specific peer group	undo peer group-name enable

Step 3: Configure the local address as the next hop in route advertisement (optional).

Since the default value is no configuration, you must show clearly to add in this configuration command when configuring MBGP of PE-PE.

Perform the following configuration in VPNv4 sub-address family view.

Table 549 Configure the local address as the next hop in route advertisement

Operation	Command
Configure the local address as the next hop in route advertisement	peer { group-name } next-hop-local
Remove the configuration	undo peer { group-name } next-hop-local

Step 4: Transfer BGP update packet without AS number (optional)

Perform the following configuration in VPNv4 sub-address family view.

Table 550 Transfer BGP update packet without AS number

Operation	Command
Transfer BGP update packet without AS number	peer group-name public-as-only
Transfer BGP update packet with AS number	undo peer group-name public-as-only



*In the above-mentioned configuration steps, the **public-as-only** keyword is required for configuring EBGP and alliance, but not for configuring IBGP.*

Step 5: Advertise default route to the peer (group)

This command adds a default route which uses local address as the next hop on the PE SPE (system processing engine)

Perform the following configuration in VPNv4 sub-address family view.

Table 551 Advertise default route to the peer (group)

Operation	Command
Advertise default route to the peer (group)	peer <i>ip-address</i> default-route-advertise vpn-instance <i>vpn-instance name</i>
Remove to advertise default route to the peer (group)	undo peer <i>ip-address</i> default-route-advertise vpn-instance <i>vpn-instance name</i>

Step 6: Configure BGP neighbor as the User-end PE (UPE) of BGP/MPLS VPN

This command is only used for UPE of BGP/MPLS VPN.

Configure the following commands in the VPNv4 sub-address family view.

Table 552 Configure BGP neighbor as the UPE of BGP/MPLS VPN

Operation	Command
Configure BGP neighbor as the UPE of BGP/MPLS VPN	peer <i>peer-address</i> upe
Disable the configuration	undo peer <i>peer-address</i> upe

Configuring P Router

P router does not maintain VPN routes, but do keep connection with public network and coordinate with PE in creating LSPs. These configurations are required on P router:

Step 1: Configure MPLS basic capacity and enable LDP on the interfaces connecting P router to PE router, for forwarding MPLS packets. See "MPLS Basic Capability Configuration".

Step 2: Enable OSPF protocol at the interfaces connecting P router to PE router and import direct-connect routes. See "OSPF" part in "Routing Protocol" for details.

Displaying and Debugging BGP/MPLS VPN

Displaying VPN address information from BGP table

After the above configuration, execute **display** command in any view to display the running of the VPNv4 information in BGP database configuration, and to verify the effect of the configuration.

Table 553 Display VPN address information from BGP table

Operation	Command
Display VPN address information from BGP table	display bgp vpnv4 { all route-distinguisher <i>rd-value</i> vpn-instance <i>vpn-instance-name</i> } { group network peer routing-table }

Displaying IP routing table associated with VPN-instance

After the above configuration, you can execute **display** command in any view to display the corresponding information in the IP routing tables related to VPN-instance, and to verify the effect of the configuration.

Table 554 Display IP routing table associated with VPN-instance

Operation	Command
Display IP routing table associated with VPN-instance	display ip routing-table vpn-instance <i>vpn-instance-name</i> [<i>ip-address</i>] [verbose] [statistics]

Displaying VPN-instance related information

After the above configuration, executing the **display** command in any view can display the VPN-instance related information, including its RD, description, the interfaces associated with it, and so on. You can view the information to verify the configuration effect.

Table 555 Display VPN-instance related information

Operation	Command
Display the VPN-instance related information, including its RD, description, the interfaces associated with it, and so on.	display ip vpn-instance [<i>vpn-instance-name</i>] [verbose]

Debugging information concerning processing BGP

Execute **debugging** command in user view for the debugging of the related vpn-instance information.

Table 556 Enable the debugging for processing BGP

Operation	Command
Enable the debugging for processing BGP	debugging bgp { all event normal } { keepalive mp-update open packet update route-refresh update } [receive send] [verbose]
Disable the debugging	undo debugging bgp { { all event normal keepalive mp-update open packet update route-refresh } [receive send verbose] } { all event normal update }

Displaying MPLS L3VPN-LSP information

Table 557 Display MPLS L3VPN-LSP information

Operation	Command
Display MPLS L3VPN LSP information	display mpls l3vpn-lsp [verbose] include <i>text</i>
Display MPLS L3VPN LSP VPN-instance information	display mpls l3vpn-lsp [vpn-instance <i>vpn-instance-name</i>] [transit egress ingress] [include <i>text</i> verbose]

Displaying Sham-link

Table 558 Display Sham-link

Operation	Command
Display Sham-link	display ospf [<i>process-id</i>] sham-link

Typical BGP/MPLS VPN Configuration Example

Integrated BGP/MPLS VPN Configuration Example

Network requirements

- VPNA includes CE1 and CE3; VPNB includes CE2 and CE4.
- Subscribers in different VPNs cannot access each other. The VPN-target attribute for VPNA is 111:1 and that for VPNB is 222:2.
- The PEs and P are 3Com switches supporting MPLS, and CEs are common layer 3 switches.

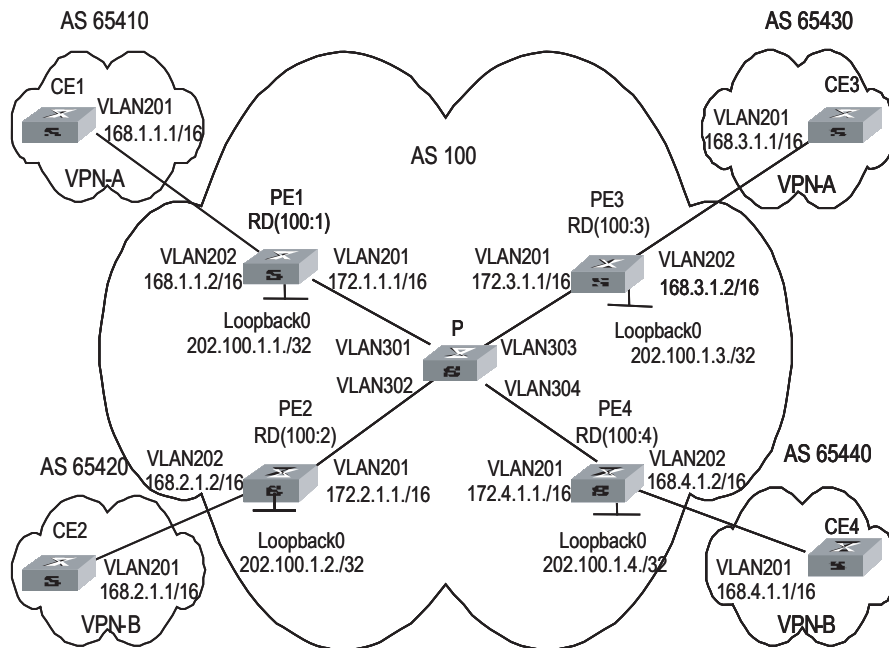


The configuration in this case is focused on:

- Configure EBGP to exchange VPN routing information between CEs and PEs.
- Configure OSPF for inter-PE communication between PEs.
- Configure MP-IBGP to exchange VPN routing information between PEs.

Network diagram

Figure 134 Network diagram for integrated BGP/MPLS VPN



Configuration procedure

The following are the configuration introduction to PE, CE and P switches.

1 Configure CE1.

Configure CE1 and PE1 as EBGP neighbors, import direct-connect routes and static routes to import intra-CE1 VPN routes into BGP and advertise to PE1. CE1 connects to PE1 through interface Gigabitethernet 2/1/1.

```
[CE1] vlan 201
[CE1-vlan201] port gigabitethernet 2/1/1
```



```
[CE1-vlan201] quit
[CE1] interface Vlan-interface 201
[CE1-Vlan-interface201] ip address 168.1.1.1 255.255.0.0
[CE1-Vlan-interface201] quit
[CE1] bgp 65410
[CE1-bgp] group 168 external
[CE1-bgp] peer 168.1.1.2 group 168 as-number 100
[CE1-bgp] import-route direct
[CE1-bgp] import-route static
```



The configuration on the other three CE switches (CE2 to CE4) is similar to that on CE1, the details are omitted here.

2 Configure PE1

Configure vpn-instance for VPNA on PE1, as well as other associated attributes to control advertisement of VPN routing information.

```
[PE1] ip vpn-instance vpna
[PE1-vpn-vpna] route-distinguisher 100:1
[PE1-vpn-vpna] vpn-target 111:1 both
[PE1-vpn-vpna] quit
```

Configure PE1 and CE1 as MP-EBGP neighbors, import CE1 VPN routes learned into MBGP VPN-instance address family.

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] group 168 external
[PE1-bgp-af-vpn-instance] peer 168.1.1.1 group 168 as-number 65410
[PE1-bgp-af- vpn-instance] quit
[PE1-bgp] quit
```

Bind the VLAN interface connecting PE1 and CE1 to the VPNA. Note that you should first configure association between the VLAN interface and VPN-instance, and then configure the IP address of the VLAN interface.

```
[PE1] vlan 202
[PE1-vlan202] port gigabitethernet 2/1/2
[PE1-vlan202] quit
[PE1] interface Vlan-interface 202
[PE1-Vlan-interface202] ip binding vpn-instance vpna
[PE1-Vlan-interface202] ip address 168.1.1.2 255.255.0.0
[PE1-Vlan-interface202] quit
```

Configure Loopback interface. (For PE, the IP address for Loopback interface must be a host address with 32-bit mask, to prevent the route is aggregated and then LSP cannot process correctly interior-layer labels.)

```
[PE1] interface loopback0
[PE1-LoopBack 0] ip address 202.100.1.1 255.255.255.255
[PE1-LoopBack 0] quit
```

Configure MPLS basic capacity and enable MPLS and LDP on VLAN interface connecting PE1 and P. Create LSP and achieve MPLS packet forwarding.

```

[PE1] mpls lsr-id 202.100.1.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1] vlan 201
[PE1-vlan201] port gigabitethernet 2/1/1
[PE1-vlan201] quit
[PE1] interface Vlan-interface 201
[PE1-Vlan-interface201] ip address 172.1.1.1 255.255.0.0
[PE1-Vlan-interface201] mpls
[PE1-Vlan-interface201] mpls ldp enable
[PE1-Vlan-interface201] quit

```

Enable OSPF on the interface connecting PE1 and P and on the Loopback interface, import direct-connect routes. Achieve inter-PE communication.

```

[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[PE1-ospf-1-area-0.0.0.0] network 202.100.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] import-route direct
[PE1-ospf-1] quit

```

Set up MP-IBGP adjacency between PEs to exchange inter-PE VPN routing information and activate MP-IBGP peer in VPNv4 sub-address family view.

```

[PE1] bgp 100
[PE1-bgp] group 202 internal
[PE1-bgp] peer 202.100.1.3 group 202
[PE1-bgp] peer 202.100.1.3 connect-interface loopback0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 202 enable
[PE1-bgp-af-vpn] peer 202.100.1.3 group 202
[PE1-bgp-af-vpn] quit
[PE1-bgp] quit

```

3 Configure P:

Configure MPLS basic capacity, enable LDP on the interfaces connecting P and PE for MPLS packet forwarding.

```

[P] mpls lsr-id 172.1.1.2
[P] mpls
[P-mpls] quit
[P] mpls ldp
[P] interface loopback0
[P-LoopBack 0] ip address 172.1.1.2 255.255.255.255
[P-LoopBack 0] quit
[P] vlan 301
[P-vlan301] port gigabitethernet 3/1/1
[P-vlan301] quit
[P] interface Vlan-interface 301
[P-Vlan-interface301] ip address 172.1.1.2 255.255.0.0
[P-Vlan-interface301] mpls
[P-Vlan-interface301] mpls ldp enable
[P-Vlan-interface301] quit
[P] vlan 302

```

```

[P-vlan302] port gigabitethernet 3/1/2
[P-vlan302] quit
[P] interface Vlan-interface 302
[P-Vlan-interface302] ip address 172.2.1.2 255.255.0.0
[P-Vlan-interface302] mpls
[P-Vlan-interface302] mpls ldp enable
[P-Vlan-interface302] quit
[P] vlan 303
[P-vlan303] port gigabitethernet 3/1/3
[P-vlan303] quit
[P] interface Vlan-interface 303
[P-Vlan-interface303] ip address 172.3.1.2 255.255.0.0
[P-Vlan-interface303] mpls
[P-Vlan-interface303] mpls ldp enable
[P-Vlan-interface303] quit
[P] vlan 304
[P-vlan304] port gigabitethernet 3/1/4
[P-vlan304] quit
[P] interface Vlan-interface 304
[P-Vlan-interface304] ip address 172.4.1.2 255.255.0.0
[P-Vlan-interface304] mpls
[P-Vlan-interface304] mpls ldp enable
[P-Vlan-interface304] quit

```

Enable OSPF protocol on the interfaces connecting P and PE, import direct-connect route to achieve inter-PE communication.

```

[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.255.255
[P-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.255.255
[P-ospf-1-area-0.0.0.0] network 172.3.1.0 0.0.255.255
[P-ospf-1-area-0.0.0.0] network 172.4.1.0 0.0.255.255
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] import-route direct

```

4 Configure PE3



The configuration on PE3 is similar to that on PE1, you should pay more attention to VPN routing attribute setting on PE3 to get information about how to control advertisement of a same VPN routing information (with same VPN-target) over MPLS network.

Create VPN-instance for VPNA on PE3, configure correlative attributes to control advertisement of VPN routing information.

```

[PE3] ip vpn-instance vpna
[PE3-vpn-vpna] route-distinguisher 100:3
[PE3-vpn-vpna] vpn-target 111:1 both
[PE3-vpn-vpna] quit

```

Set up MP-EBGP adjacency between PE3 and CE3, import intra-CE3 VPN routes learned into MBGP VPN-instance address family.

```

[PE3] bgp 100
[PE3-bgp] ipv4-family vpn-instance vpna
[PE3-bgp-af-vpn-instance] import-route direct
[PE3-bgp-af-vpn-instance] group 168 external

```

```
[PE3-bgp-af-vpn-instance] peer 168.3.1.1 group 168 as-number 65430
[PE3-bgp-af-vpn-instance] quit
[PE3-bgp] quit
```

Bind the interface connecting PE3 and CE3 to VPNA.

```
[PE3] vlan 202
[PE3-vlan202] port gigabitethernet 2/1/2
[PE3-vlan202] quit
[PE3] interface Vlan-interface 202
[PE3-Vlan-interface202] ip binding vpn-instance vpna
[PE3-Vlan-interface202] ip address 168.3.1.2 255.255.0.0
[PE3-Vlan-interface202] quit
```

Configure Loopback interface

```
[PE3] interface loopback0
[PE3-LoopBack 0] ip address 202.100.1.3 255.255.255.255
[PE3-LoopBack 0] quit
```

Configure MPLS basic capacity and enable MPLS and LDP on VLAN interface connecting PE3 and P. Creates LSP and achieve MPLS packet forwarding.

```
[PE3] mpls lsr-id 202.100.1.3
[PE3] mpls
[PE3-mpls] quit
[PE3] mpls ldp
[PE3] vlan 201
[PE3-vlan201] interface gigabitethernet 2/1/1
[PE3-vlan201] quit
[PE3] interface Vlan-interface 201
[PE3-Vlan-interface201] ip address 172.3.1.1 255.255.0.0
[PE3-Vlan-interface201] mpls
[PE3-Vlan-interface201] mpls ldp enable
[PE3-Vlan-interface201] quit
```

Enable OSPF on the interface connecting PE3 and P and the Loopback interface, import direct-connect routes.

```
[PE3] ospf
[PE3-ospf-1] area 0
[PE3-ospf-1-area-0.0.0.0] network 172.3.0.0 0.0.255.255
[PE3-ospf-1-area-0.0.0.0] network 202.100.1.3 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] import-route direct
[PE3-ospf-1-area-0.0.0.0] import-route direct
```

Set up MP-IBGP adjacency between PEs to exchange inter-PE VPN routing information.

```
[PE3] bgp 100
[PE3-bgp] group 202 internal
[PE3-bgp] peer 202.100.1.1 group 202 as-number 100
[PE3-bgp] peer 202.100.1.1 connect-interface loopback0
[PE3-bgp] ipv4-family vpnv4
[PE3-bgp-af-vpn] peer 202 enable
```

```
[PE3-bgp-af-vpn] peer 202.100.1.1 group 202
[PE3-bgp-af-vpn] quit
```

5 Configure PE2 and PE4

The configuration of PE2 and PE4 is similar to that of PE1 and PE3. The details are omitted here.

Extranet Configuration Example

Network requirements

Company A and Company B are located at City A and City B respectively. Their headquarters is located at City C. They respectively own VPN1 and VPN2.

In this case, VPN function is provided by MPLS. There are some shared resources at the City C for the two VPNs. All subscribers in both VPNs can access the shared resources, but VPN subscribers in City A and City B cannot access each other.

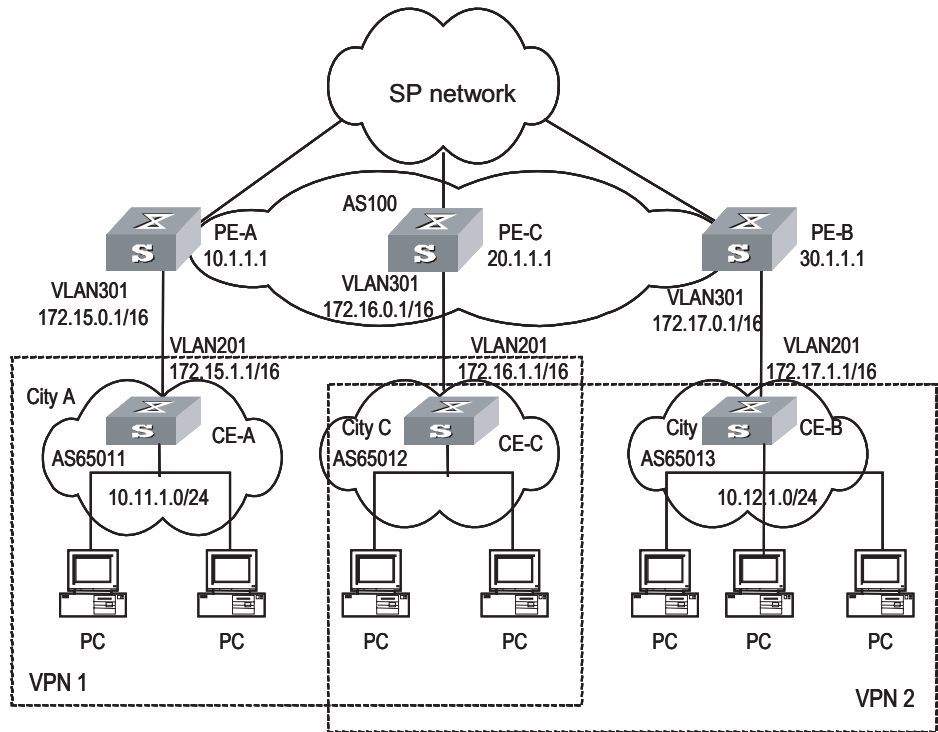
The two companies cannot use identical IP addresses, for they share the same VPN-instance at PE-C.



In the case the configuration is focused on controlling access authority of VPN subscribers at different cities by configuring different VPN-target attributes at different PEs.

Network diagram

Figure 135 Network diagram for Extranet



Configuration procedure

This configuration procedure has omitted configurations between PE and P, and configurations on CEs. For these details refer to the former example.

1 Configure PE-A:

Configure VPN-instance 1 for VPN1 on PE-A, so that it can send and receive VPN routing information of VPN-target 111:1.

```
[PE-A] ip vpn-instance vpn-instance 1
[PE-A-vpn-1] route-distinguisher 100:1
[PE-A-vpn-1] vpn-target 111:1 both
[PE-A-vpn-1] quit
```

Set up MP-EBGP adjacency between PE-A and CE-A, import intra-CE-A VPN routes learned into MBGP VPN-instance address family.

```
[PE-A] bgp 100
[PE-A-bgp] ipv4-family vpn-instance vpn-instance1
[PE-A-bgp-af-vpn-instance] import-route direct
[PE-A-bgp-af-vpn-instance] import-route static
[PE-A-bgp-af-vpn-instance] group 172 external
[PE-A-bgp-af-vpn-instance] peer 172.15.1.1 group 172 as-number 65011
[PE-A-bgp-af-vpn-instance] quit
[PE-A-bgp] quit
```

Bind VPN-instance1 with the interface of VLAN301 which connects CE-A.

```
[PE-A] vlan 301
[PE-A-vlan301] port gigabitethernet 3/1/1
[PE-A-vlan301] quit
[PE-A] interface Vlan-interface 301
[PE-A-Vlan-interface301] ip binding vpn-instance vpn-instance1
[PE-A-Vlan-interface301] ip address 172.15.0.1 255.255.0.0
[PE-A-Vlan-interface301] quit
```

Configure Loopback interface

```
[PE-A] interface loopback 0
[PE-A-LoopBack0] ip address 10.1.1.1 255.255.255.255
[PE-A-LoopBack0] quit
```

Configure MPLS basic capacity.

```
[PE-A] mpls lsr-id 10.1.1.1
[PE-A] mpls
[PE-A-mpls] quit
[PE-A] mpls ldp
```

Set up MP-IBGP adjacency between PEs to exchange inter-PE VPN routing information and activate MP-IBGP peer in VPNv4 sub-address family view.

```
[PE-A] bgp 100
[PE-A-bgp] group 20 internal
[PE-A-bgp] peer 20.1.1.1 group 20
[PE-A-bgp] peer 20.1.1.1 connect-interface loopback 0
[PE-A-bgp] ipv4-family vpnv4
```

```
[PE-A-bgp-af-vpn] peer 20 enable
[PE-A-bgp-af-vpn] peer 20.1.1.1 group 20
[PE-A-bgp-af-vpn] quit
```

2 Configure PE-C.

Create a VPN-instance 2 on PE-C, so that it can send and receive VPN routing information of VPN-target 111:1 and 222:2.

```
[PE-C] ip vpn-instance vpn-instance 2
[PE-C-vpn-2] route-distinguisher 100:2
[PE-C-vpn-2] vpn-target 111:1 both
[PE-C-vpn-2] vpn-target 222:2 both
[PE-C-vpn-2] quit
```

Set up MP-EBGP adjacency between PE-C and CE-C, import intra-CE-C VPN routes learned into MBGP VPN-instance address family.

```
[PE-C] bgp 100
[PE-C-bgp] ipv4-family vpn-instance vpn-instance2
[PE-C-bgp-af-vpn-instance] import-route direct
[PE-C-bgp-af-vpn-instance] import-route static
[PE-C-bgp-af-vpn-instance] group 172 external
[PE-C-bgp-af-vpn-instance] peer 172.16.1.1 group 172 as-number 65012
[PE-C-bgp-af-vpn-instance] quit
[PE-C-bgp] quit
```

Bind VPN-instance2 with the interface of VLAN301 which connects CE-C.

```
[PE-C] vlan 301
[PE-C-vlan301] port gigabitethernet 3/1/1
[PE-C-vlan301] quit
[PE-C] interface Vlan-interface 301
[PE-C-Vlan-interface301] ip binding vpn-instance vpn-instance2
[PE-C-Vlan-interface301] ip address 172.16.0.1 255.255.0.0
[PE-C-Vlan-interface301] quit
```

Configure Loopback interface

```
[PE-C] interface loopback 0
[PE-C-LoopBack0] ip address 20.1.1.1 255.255.255.255
[PE-C-LoopBack0] quit
```

Configure MPLS basic capacity.

```
[PE-C] mpls lsr-id 20.1.1.1
[PE-C] mpls
[PE-C-mpls] quit
[PE-C] mpls ldp
```

Set up MP-IBGP adjacency between PEs to exchange inter-PE VPN routing information and activate MP-IBGP peer in VPNv4 sub-address family view.

```
[PE-C] bgp 100
[PE-C-bgp] group 10
[PE-C-bgp] peer 10.1.1.1 group 10
[PE-C-bgp] peer 10.1.1.1 connect-interface loopback 0
[PE-C-bgp] group 30
```

```
[PE-C-bgp] peer 30.1.1.1 group 30
[PE-C-bgp] peer 30.1.1.1 connect-interface loopback 0
[PE-C-bgp] ipv4-family vpnv4
[PE-C-bgp-af-vpn] peer 10 enable
[PE-C-bgp-af-vpn] peer 10.1.1.1 group 10
[PE-C-bgp-af-vpn] peer 30 enable
[PE-C-bgp-af-vpn] peer 30.1.1.1 group 30
[PE-C-bgp-af-vpn] quit
```

3 Configure PE-B:

Create VPN-instance 3 for VPN2 on PE-B, so that it can send and receive VPN routing information of VPN-target 222:2.

```
[PE-B] ip vpn-instance vpn-instance 3
[PE-B-vpn-3] route-distinguisher 100:3
[PE-B-vpn-3] vpn-target 222:2 both
[PE-B-vpn-3] quit
```

Set up MP-EBGP adjacency between PE-B and CE-B, import intra-CE-B VPN routes learned into MBGP VPN-instance address family.

```
[PE-B] bgp 100
[PE-B-bgp] ipv4-family vpn-instance vpn-instance3
[PE-B-bgp-af-vpn-instance] import-route direct
[PE-B-bgp-af-vpn-instance] import-route static
[PE-B-bgp-af-vpn-instance] group 172 external
[PE-B-bgp-af-vpn-instance] peer 172.17.1.1 group 172 as-number 65013
[PE-B-bgp-af-vpn-instance] quit
[PE-B-bgp] quit
```

Bind VPN-instance3 with the interface of VLAN301 which connects to CE-B.

```
[PE-B] vlan 301
[PE-B-vlan301] port gigabitethernet 3/1/1
[PE-B-vlan301] quit
[PE-B] interface Vlan-interface 301
[PE-B-Vlan-interface301] ip binding vpn-instance vpn-instance3
[PE-B-Vlan-interface301] ip address 172.17.0.1 255.255.0.0
[PE-B-Vlan-interface301] quit
```

Configure Loopback interface

```
[PE-B] interface loopback 0
[PE-B-LoopBack0] ip address 30.1.1.1 255.255.255.255
[PE-B-LoopBack0] quit
```

Configure MPLS basic capacity.

```
[PE-B] mpls lsr-id 30.1.1.1
[PE-B] mpls
[PE-B-mpls] quit
[PE-B] mpls ldp
```

Set up MP-IBGP adjacency between PEs to exchange inter-PE VPN routing information and activate MP-IBGP peer in VPNv4 sub-address family view.


```
[PE-B] bgp 100
[PE-B-bgp] group 20
[PE-B-bgp] peer 20.1.1.1 group 20
[PE-B-bgp] peer 20.1.1.1 connect-interface loopback 0
[PE-B-bgp] ipv4-family vpnv4
[PE-B-bgp-af-vpn] peer 20 enable
[PE-B-bgp-af-vpn] peer 20.1.1.1 group 20
[PE-B-bgp-af-vpn] quit
```

Hub&Spoke Configuration Example

Network requirements

Hub&Spoke networking is also called central server networking. The Site in the center is called Hub-Site, while the one not in the center is called Spoke-Site. The Hub-Site knows the routes to all other Sites in the same VPN, and the Spoke-Site must send its traffic first to the Hub-Site and then to the destination. Hub-Site is the central node of Spoke-Sites.

A bank has a headquarters network and subsidiary networks, and it requires that the subsidiaries cannot directly exchange data with each other, but they can exchange data through the headquarters network which provides uniform control. In this case, Hub&Spoke networking topology is used: CE2 and CE3 are spoke-sites, while CE1 is a hub-site in the bank data center. CE1 controls communication between CE2 and CE3.

- Set up IBGP adjacency between PE1 and PE2 or PE1 and PE3, but not between PE2 and PE3, that is, VPN routing information cannot be exchanged between PE2 and PE3.
- Create two VPN-instances on PE1, import VPN routes of VPN-target 100:11 and 100:12, set VPN-target for VPN routes advertised as 100:2.
- Create a VPN-instance on PE2, import VPN routes of VPN-target 100:2, set VPN-target for VPN routes advertised as 100:11.
- Create a VPN-instance on PE3, import VPN routes of VPN-target 100:2, set VPN-target for VPN routes advertised as 100:12.

Then PE2 and PE3 can only learn their neighbor's routes through PE1.

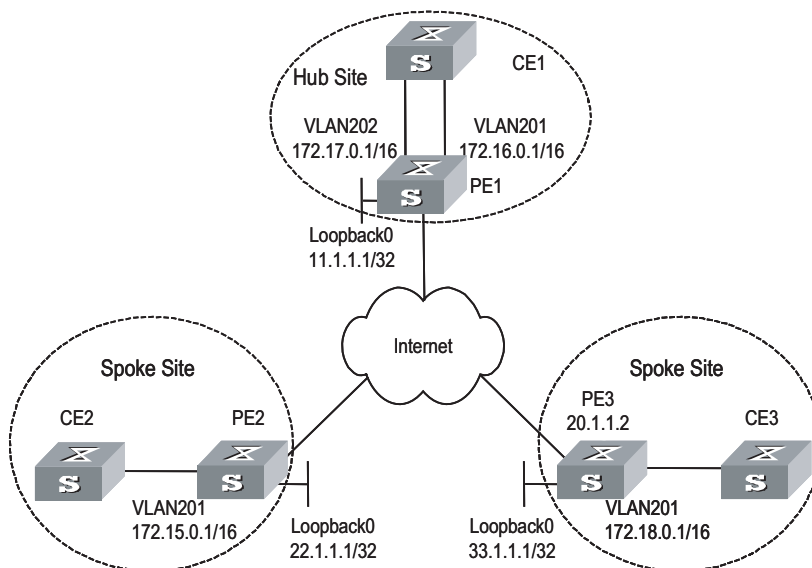


In this case the configuration is focused on four points:

- Route advertisement can be controlled by VPN-target settings on different PEs.
- Routing loop is permitted only once, so that PE can receive route update messages with AS number included from CE.
- In Hub&Spoke networking, VPN-target of VPN-instance (VPN-instance3) which is used to release route on the PE1 cannot be the same with any VPN-target of VPN-instance (VPN-instance2) which is used to import route on PE1.
- In Hub&Spoke networking, route-distinguisher rd2 (100:3) of VPN-instance which is used to release route on the PE1 cannot be the same with the route-distinguisher rd1 (100:1) or rd4 (100:4) of corresponding VPN-instances on each PE2 and PE3; rd 1 and rd4 can be the same or not.

Network diagram

Figure 136 Network diagram for Hub&Spoke



Configuration procedure



The following contents are omitted in this case: MPLS basic capacity configuration between PEs, configuration between PE and P, configuration between CEs. For the details refer to “Integrated BGP/MPLS VPN Configuration Example”.

1 Configure PE1

Configure two VPN-instances on PE1, set specified VPN-target for the routes received from PE2 and PE3.

```
[PE1] ip vpn-instance vpn-instance2
[PE1-vpn-vpn-instance2] route-distinguisher 100:2
[PE1-vpn-vpn-instance2] vpn-target 100:11 import-extcommunity
[PE1-vpn-vpn-instance2] vpn-target 100:12 import-extcommunity
[PE1-vpn-vpn-instance2] quit
[PE1] ip vpn-instance vpn-instance3
[PE1-vpn-vpn-instance3] route-distinguisher 100:3
[PE1-vpn-vpn-instance3] vpn-target 100:2 export-extcommunity
[PE1-vpn-vpn-instance3] quit
```

Set up EBGP adjacency between PE1 and CE1, import intra-CE1 VPN routes learned into MBGP VPN-instance address family, with one routing loop permitted.

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpn-instance2
[PE1-bgp-af-vpn-instance] import-route static
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] group 17216 external
[PE1-bgp-af-vpn-instance] peer 172.16.1.1 group 17216 as-number 65002
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] ipv4-family vpn-instance vpn-instance3
[PE1-bgp-af-vpn-instance] import-route static
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] group 17217 external
[PE1-bgp-af-vpn-instance] peer 172.17.1.1 group 17217 as-number 65002
```

```
[PE1-bgp-af-vpn-instance] peer 172.17.1.1 allow-as-loop 1
[PE1-bgp-af-vpn] quit
[PE1-bgp] quit
```

Bind the VLAN interface connecting PE1 and CE1 to different VPN-instances. Bind the interface of the VLAN to which the Ethernet port GigabitEthernet 2/1/1 belongs to VPN-instance2, bind the interface of the VLAN to which the Ethernet port GigabitEthernet 2/1/2 belongs to VPN-instance3.

```
[PE1] vlan 201
[PE1-vlan201] port gigabitEthernet 2/1/1
[PE1-vlan201] quit
[PE1] interface Vlan-interface 201
[PE1-Vlan-interface201] ip binding vpn-instance vpn-instance2
[PE1-Vlan-interface201] ip address 172.16.0.1 255.255.0.0
[PE1-Vlan-interface201] quit
[PE1] vlan 202
[PE1-vlan202] port gigabitEthernet 2/1/2
[PE1-vlan202] quit
[PE1] interface Vlan-interface 202
[PE1-Vlan-interface202] ip binding vpn-instance vpn-instance3
[PE1-Vlan-interface202] ip address 172.17.0.1 255.255.0.0
[PE1-Vlan-interface202] quit
```

Configure Loopback interface

```
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 11.1.1.1 255.255.255.255
[PE1-LoopBack0] quit
```

Set up MP-IBGP adjacency between PEs to exchange inter-PE VPN routing information and activate MP-IBGP peer in VPNv4 sub-address family view.

```
[PE1] bgp 100
[PE1-bgp] group 22
[PE1-bgp] peer 22.1.1.1 group 22 as-number 100
[PE1-bgp] peer 22.1.1.1 connect-interface loopback 0
[PE1-bgp] group 33
[PE1-bgp] peer 33.1.1.1 group 33 as-number 100
[PE1-bgp] peer 33.1.1.1 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 22 enable
[PE1-bgp-af-vpn] peer 22.1.1.1 group 22
[PE1-bgp-af-vpn] peer 33 enable
[PE1-bgp-af-vpn] peer 33.1.1.1 group 33
[PE1-bgp-af-vpn] quit
```

2 Configure PE2

Create a VPN-instance on PE2, import VPN routing information of VPN-target 100:2 and advertise VPN routing information of VPN-target 100:1.

```
[PE2] ip vpn-instance vpn-instance1
[PE2-vpn-vpn-instance1] route-distinguisher 100:1
[PE2-vpn-vpn-instance1] vpn-target 100:11 export-extcommunity
[PE2-vpn-vpn-instance1] vpn-target 100:2 import-extcommunity
[PE2-vpn-vpn-instance1] quit
```

Set up EBGP adjacency between PE2 and CE2, import intra-CE2 VPN routes learned into MBGP VPN-instance address family.

```
[PE2] bgp 100
[PE2-bgp] ipv4-family vpn-instance vpn-instance1
[PE2-bgp-af-vpn-instance] import-route static
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] group 172 external
[PE2-bgp-af-vpn-instance] peer 172.15.1.1 group 172 as-number 65003
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] quit
```

Bind the interface of the VLAN to which the port connecting PE2 and CE2 belongs to VPN-instance.

```
[PE2] vlan 201
[PE2-vlan201] port gigabitethernet 2/1/1
[PE2-vlan201] quit
[PE2] interface Vlan-interface 201
[PE2-Vlan-interface201] ip binding vpn-instance vpn-instance1
[PE2-Vlan-interface201] ip address 172.15.0.1 255.255.0.0
[PE2-Vlan-interface201] quit
```

Configure Loopback interface

```
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 22.1.1.1 255.255.255.255
[PE2-LoopBack0] quit
```

Set up MP-IBGP adjacency between PE2 and PE1 to exchange inter-PE VPN routing information and activate MP-IBGP peer in VPNv4 sub-address family view.

```
[PE2] bgp 100
[PE2] group 11
[PE2-bgp] peer 11.1.1.1 group 11 as-number 100
[PE2-bgp] peer 11.1.1.1 connect-interface loopback 0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer 11 enable
[PE2-bgp-af-vpn] peer 11.1.1.1 allow-as-loop 1
[PE2-bgp-af-vpn] quit
[PE2-bgp] quit
```

3 Configure PE3

Create a VPN-instance on PE3, import VPN routing information of VPN-target 100:2 and advertise VPN routing information of VPN-target 100:12.

```
[PE3] ip vpn-instance vpn-instance2
[PE3-vpn-vpn-instance2] route-distinguisher 100:4
[PE3-vpn-vpn-instance2] vpn-target 100:12 export-extcommunity
[PE3-vpn-vpn-instance2] vpn-target 100:2 import-extcommunity
[PE3-vpn-vpn-instance2] quit
```

Set up EBGP adjacency between PE3 and CE3 import intra-CE3 VPN routes learned into MBGP VPN-instance address family.

```
[PE3] bgp 100
[PE3-bgp] ipv4-family vpn-instance vpn-instance2
```

```
[PE3-bgp-af-vpn-instance] import-route static
[PE3-bgp-af-vpn-instance] import-route direct
[PE3-bgp-af-vpn-instance] group 172 external
[PE3-bgp-af-vpn-instance] peer 172.18.1.1 group 172 as-number 65001
[PE3-bgp-af-vpn-instance] quit
[PE3-bgp] quit
```

Bind the interface of the VLAN to which the port connecting PE3 and CE3 belongs to VPN-instance.

```
[PE3] vlan 201
[PE3-vlan201] port gigabitethernet 2/1/1
[PE3-vlan201] quit
[PE3] interface Vlan-interface 201
[PE3-Vlan-interface201] ip binding vpn-instance vpn-instance2
[PE3-Vlan-interface201] ip address 172.18.0.1 255.255.0.0
[PE3-Vlan-interface201] quit
```

Configure Loopback interface

```
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 33.1.1.1 255.255.255.255
[PE3-LoopBack0] quit
```

Set up MP-IBGP adjacency between PE3 and PE1 to exchange inter-PE VPN routing information and activate MP-IBGP peer in VPNv4 sub-address family view.

```
[PE3] bgp 100
[PE3-bgp] group 11
[PE3-bgp] peer 11.1.1.1 group 11
[PE3-bgp] peer 11.1.1.1 connect-interface loopback 0
[PE3-bgp] ipv4-family vpnv4
[PE3-bgp-af-vpn] peer 11 enable
[PE2-bgp-af-vpn] peer 11.1.1.1 group 11
[PE2-bgp-af-vpn] peer 11.1.1.1 allow-as-loop 1
[PE3-bgp-af-vpn] quit
[PE3-bgp] quit
```

CE Dual-home Configuration Example

Network requirements

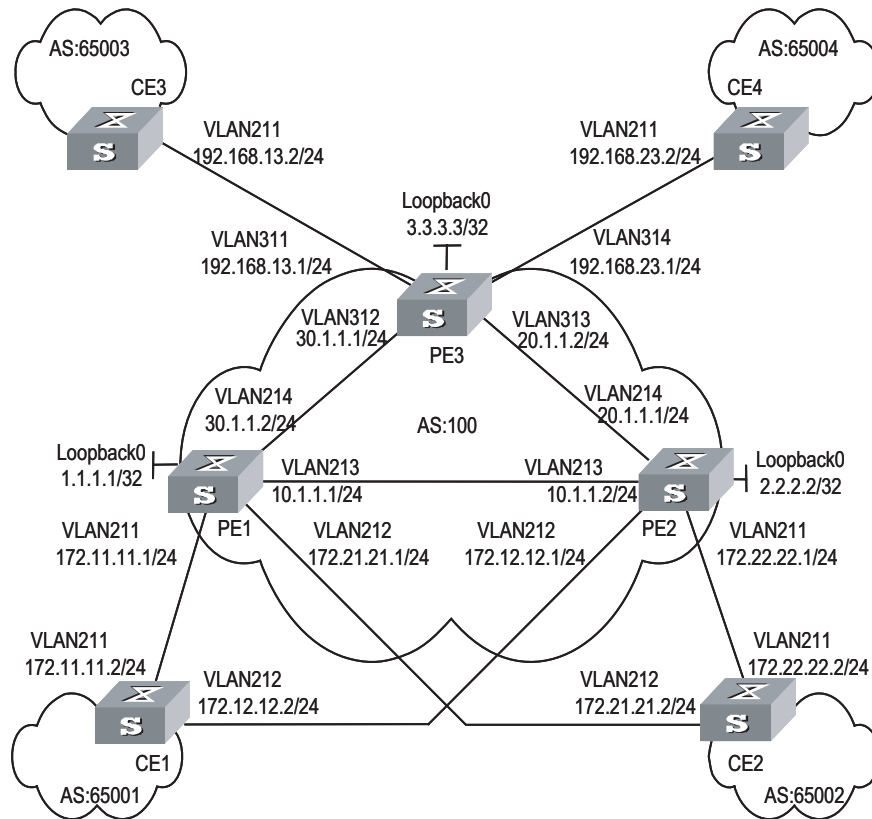
For the applications which require high robustness of network, you may use CE dual-home networking mode.

CE1 and CE2 are dual-homed; they are connected to both PE1 and PE2. Three PEs are connected to each other so the links between them are backed up. CE3 and CE4 are single-homed; each of them is only connected to one PE.

CE1 and CE3 are in one VPN, and CE2 and CE4 are in another VPN. The two VPNs cannot intercommunicate with each other.

Network diagram

Figure 137 Network diagram for CE dual-home



Configuration procedure



The configuration of CE router is omitted in this case and you can refer to Section “Integrated BGP/MPLS VPN Configuration Example” “Integrated BGP/MPLS VPN Configuration Example”.

1 Configure PE1

Configure two VPN-instances 1.1 and 1.2 respectively for CE1 and CE2 on PE1, set different VPN-targets for them.

```
[PE1] ip vpn-instance vpn-instance1.1
[PE1-vpn-vpn-instance1.1] route-distinguisher 1.1.1.1:1
[PE1-vpn-vpn-instance1.1] vpn-target 1.1.1.1:1
[PE1-vpn-vpn-instance1.1] quit
[PE1] ip vpn-instance vpn-instance1.2
[PE1-vpn-vpn-instance1.2] route-distinguisher 2.2.2.2:2
[PE1-vpn-vpn-instance1.2] vpn-target 2.2.2.2:2
[PE1-vpn-vpn-instance1.2] quit
```

Set up EBGP adjacency between PE1 and CE1 in VPN-instance 1, import intra-CE1 VPN routes learned into VPN-instance 1.1.

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpn-instance1.1
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] import-route static
```

```
[PE1-bgp-af-vpn-instance] group 17211 external
[PE1-bgp-af-vpn-instance] peer 172.11.11.2 group 17211 as-number 65001
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] quit
```

Set up EBGP adjacency between PE1 and CE2 in VPN-instance 1.2, import intra-CE2 VPN routes learned into VPN-instance 1.2.

```
[PE1-bgp] ipv4-family vpn-instance vpn-instance1.2
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] import-route static
[PE1-bgp-af-vpn-instance] group 17221 external
[PE1-bgp-af-vpn-instance] peer 172.21.21.2 group 17221 as-number 65002
[PE1-bgp-af-vpn] quit
[PE1-bgp] quit
```

Bind the interface connecting PE1 and CE1 to VPN-instance 1.1 and interface connecting PE1 and CE2 to VPN-instance 1.2.

```
[PE1] vlan 211
[PE1-vlan211] port gigabitethernet 2/1/1
[PE1-vlan211] quit
[PE1] interface Vlan-interface 211
[PE1-Vlan-interface211] ip binding vpn-instance vpn-instance1.1
[PE1-Vlan-interface211] ip address 172.11.11.1 255.255.255.0
[PE1-Vlan-interface211] quit
[PE1] vlan 212
[PE1-vlan212] port gigabitethernet 2/1/2
[PE1-vlan212] quit
[PE1] interface Vlan-interface 212
[PE1-Vlan-interface212] ip binding vpn-instance vpn-instance1.2
[PE1-Vlan-interface212] ip address 172.21.21.1 255.255.255.0
[PE1-Vlan-interface212] quit
```

Configure Loopback interface

```
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.1 255.255.255.255
[PE1-LoopBack0] quit
```

Configure MPLS basic capacity, enable LDP on the interface connecting PE1 and PE2 and the interface connecting PE1 and PE3.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1] vlan 213
[PE1-vlan213] port gigabitethernet 2/1/3
[PE1-vlan213] quit
[PE1] interface Vlan-interface213
[PE1-Vlan-interface213] mpls
[PE1-Vlan-interface213] mpls ldp enable
[PE1-Vlan-interface213] mpls ldp transport-ip interface
[PE1-Vlan-interface213] ip address 10.1.1.1 255.255.255.0
[PE1-Vlan-interface213] quit
[PE1] vlan 214
[PE1-vlan214] port gigabitethernet 2/1/4
```

```
[PE1-vlan214] quit
[PE1] interface Vlan-interface 214
[PE1-Vlan-interface214] mpls
[PE1-Vlan-interface214] mpls ldp enable
[PE1-Vlan-interface214] mpls ldp transport-ip interface
[PE1-Vlan-interface214] ip address 30.1.1.2 255.255.255.0
[PE1-Vlan-interface214] quit
```

Enable OSPF on the interface connecting PE1 and PE2 and the interface connecting PE1 and PE3 and the Loopback interface, to achieve inter-PE communication.

```
[PE1] Router-id 1.1.1.1
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 30.1.1.2 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

Set up MP-IBGP adjacency between PEs to exchange inter-PE VPN routing information and activate MP-IBGP peer in VPNv4 sub-address family view.

```
[PE1] bgp 100
[PE1-bgp] group 2
[PE1-bgp] peer 2.2.2.2 group 2
[PE1-bgp] peer 2.2.2.2 connect-interface loopback 0
[PE1-bgp] group 3
[PE1-bgp] peer 3.3.3.3 group 3
[PE1-bgp] peer 3.3.3.3 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 2 enable
[PE1-bgp-af-vpn] peer 2.2.2.2 group 2
[PE1-bgp-af-vpn] peer 3 enable
[PE1-bgp-af-vpn] peer 3.3.3.3 group 3
[PE1-bgp-af-vpn] quit
```

2 Configure PE2



The configuration of PE2 is similar to that of PE1, so only VPN-instance configuration is detailed here.

Create two VPN-instances 2.1 and 2.2 respectively for CE1 and CE2 on PE2, configure different VPN-targets for them.

```
[PE2] ip vpn-instance vpn-instance2.1
[PE2-vpn-vpn-instance2.1] route-distinguisher 1.1.1.1:1
[PE2-vpn-vpn-instance2.1] vpn-target 1.1.1.1:1
[PE2-vpn-vpn-instance2.1] quit
[PE2] ip vpn-instance vpn-instance2.2
[PE2-vpn-vpn-instance2.2] route-distinguisher 2.2.2.2:2
[PE2-vpn-vpn-instance2.2] vpn-target 2.2.2.2:2
[PE2-vpn-vpn-instance2.2] quit
```

Set up EBGP adjacency between PE2 and CE1 in VPN-instance 2.1, import intra-CE1 VPN routes learned into VPN-instance2.1.


```
[PE2] bgp 100
[PE2-bgp] ipv4-family vpn-instance vpn-instance2.1
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] import-route static
[PE2-bgp-af-vpn-instance] group 17212 external
[PE2-bgp-af-vpn-instance] peer 172.12.12.2 group 17212 as-number 65001
[PE2-bgp-af-vpn] quit
```

Set up EBGP adjacency between PE2 and CE2 in VPN-instance2.2, import intra-CE2 VPN routes learned into VPN-instance2.2.

```
[PE2-bgp] ipv4-family vpn-instance vpn-instance2.2
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] import-route static
[PE2-bgp-af-vpn-instance] group 17222 external
[PE2-bgp-af-vpn-instance] peer 172.22.22.2 group 17222 as-number 65002
[PE2-bgp-af-vpn] quit
[PE2-bgp] quit
```

Bind the interface connecting PE2 and CE1 to VPN-instance 2.1 and the interface connecting PE2 and CE2 to VPN-instance 2.2.

```
[PE2] vlan 212
[PE2-vlan212] port gigabitethernet 2/1/2
[PE2-vlan212] quit
[PE2] interface Vlan-interface 212
[PE2-Vlan-interface212] ip binding vpn-instance vpn-instance2.1
[PE2-Vlan-interface212] ip address 172.12.12.1 255.255.255.0
[PE2-Vlan-interface212] quit
[PE2] vlan 211
[PE2-vlan211] port gigabitethernet 2/1/1
[PE2-vlan211] quit
[PE2] interface Vlan-interface 211
[PE2-Vlan-interface211] ip binding vpn-instance vpn-instance2.2
[PE2-Vlan-interface211] ip address 172.22.22.1 255.255.255.0
[PE2-Vlan-interface211] quit
```

3 Configure PE3



Only the VPN-instance configuration of PE3 is detailed here, other configurations are similar to that of the PE1 and PE2, and are omitted here.

Create two VPN-instances 3.1 and 3.2 respectively for CE3 and CE4 on PE3, configure different VPN-targets for them.

```
[PE3] ip vpn-instance vpn-instance3.1
[PE3-vpn-vpn-instance3.1] route-distinguisher 1.1.1.1:1
[PE3-vpn-vpn-instance3.1] vpn-target 1.1.1.1:1
[PE3-vpn-vpn-instance3.1] quit
[PE3] ip vpn-instance vpn-instance3.2
[PE3-vpn-instance] route-distinguisher 2.2.2.2:2
[PE3-vpn-instance] vpn-target 2.2.2.2:2
[PE3-vpn-instance] quit
```

Set up EBGP adjacency between PE3 and CE3 in VPN-instance3.1, import intra-CE3 VPN routes learned into VPN-instance3.1.

```
[PE3] bgp 100
[PE3-bgp] ipv4-family vpn-instance vpn-instance3.1
```

```
[PE3-bgp-af-vpn-instance] import-route direct
[PE3-bgp-af-vpn-instance] import-route static
[PE3-bgp-af-vpn-instance] group 192 external
[PE3-bgp-af-vpn-instance] peer 192.168.13.2 group 192 as-number 65003
[PE3-bgp-af-vpn-instance] quit
[PE3-bgp] quit
```

Set up EBGP adjacency between PE3 and CE4 in VPN-instance3.2, import intra-CE4 VPN routes learned into VPN-instance3.2.

```
[PE3-bgp] ipv4-family vpn-instance vpn-instance3.2
[PE3-bgp-af-vpn-instance] import-route direct
[PE3-bgp-af-vpn-instance] import-route static
[PE3-bgp-af-vpn-instance] group 232 external
[PE3-bgp-af-vpn-instance] peer 192.168.23.2 group 232 as-number 65004
[PE3-bgp-af-vpn-instance] quit
[PE3-bgp] quit
```

Bind the interface connecting PE3 and CE3 to VPN-instance3.1 and the interface connecting PE3 and CE4 to VPN-instance 3.2.

```
[PE3] vlan 311
[PE3-vlan311] port gigabitethernet 3/1/1
[PE3-vlan311] quit
[PE3] interface Vlan-interface 311
[PE3-Vlan-interface311] ip binding vpn-instance vpn-instance3.1
[PE3-Vlan-interface311] ip address 192.168.13.1 255.255.255.0
[PE3-Vlan-interface311] quit
[PE3] vlan 314
[PE3-vlan314] port gigabitethernet 3/1/4
[PE3-vlan314] quit
[PE3] interface Vlan-interface 314
[PE3-Vlan-interface314] ip binding vpn-instance vpn-instance3.2
[PE3-Vlan-interface314] ip address 192.168.23.1 255.255.255.0
[PE3-Vlan-interface314] quit
```

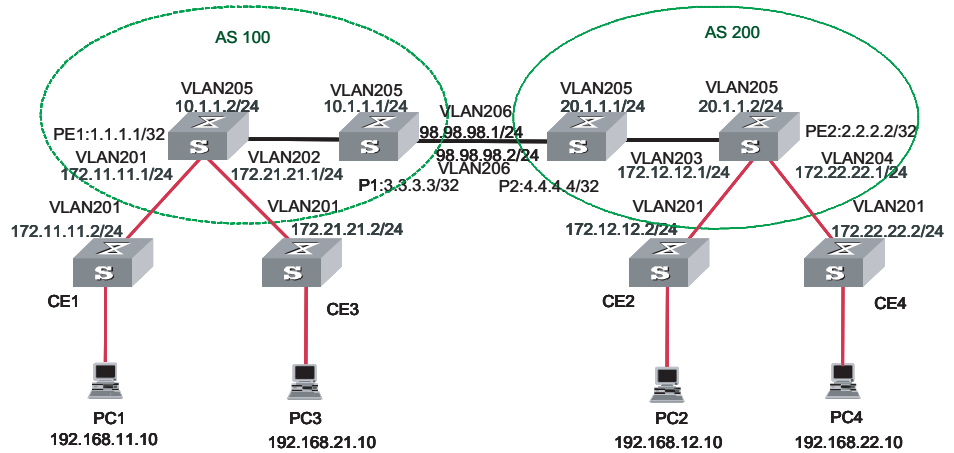
Cross-domain BGP/MPLS VPN Configuration Example

Network requirements

A VPN subscriber has sites in both city A and B. Because of the geographical reason, site in City A accesses to the MPLS/VPN network of service provider in City A, and gets AS100 as the AS number; site in City B accesses to the MPLS/VPN network of service provider in City B, and gets AS200 as the AS number. The VPN goes through two ASs. CE1 and CE2 belong to VPN-A, while CE3 and CE4 belong to VPN-B.

Network diagram

Figure 138 Network diagram for ASBR



Configuration procedure

1 Configure PE1

Enable MPLS and LDP.

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

Configure the VLAN interface connecting CE.

```
[PE1] vlan 201
[PE1-vlan201] port gigabitethernet 2/1/1
[PE1-vlan201] quit
[PE1] vlan 202
[PE1-vlan202] port gigabitethernet 2/1/2
[PE1-vlan202] quit
```

Configure Loopback interface.

```
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.1 255.255.255.255
```

Configure VPN-instance.

```
[PE1] ip vpn-instance vpna
[PE1-vpn-vpna] route-distinguisher 100:1
[PE1-vpn-vpna] vpn-target 100:1 both
[PE1] ip vpn-instance vpb
[PE1-vpn-vpb] route-distinguisher 100:2
[PE1-vpn-vpb] vpn-target 100:2 both
```

Configure VLAN interface connecting PE1 and P1.

```
[PE1] vlan 205
[PE1-vlan205] port gigabitethernet 2/2/1
[PE1-vlan205] quit
```

```
[PE1] interface Vlan-interface 205
[PE1-Vlan-interface205] mpls
[PE1-Vlan-interface205] mpls ldp enable
[PE1-Vlan-interface205] ip address 10.1.1.2 255.255.255.0
```

Bind the VLAN interface with the VPN-instance.

```
[PE1] interface Vlan-interface 201
[PE1-Vlan-interface201] ip binding vpn-instance vpna
[PE1-Vlan-interface201] ip address 172.11.11.1 255.255.255.0
[PE1-Vlan-interface201] quit
[PE1] interface Vlan-interface 202
[PE1-Vlan-interface202] ip binding vpn-instance vpnb
[PE1-Vlan-interface202] ip address 172.21.21.1 255.255.255.0
[PE1-Vlan-interface202] quit
```

Enable EBGP between PE and CE.

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] group 172-11 external
[PE1-bgp-af-vpn-instance] peer 172.11.11.2 group 172-11 as-number 65011
[PE1-bgp-af-vpn] quit
[PE1-bgp] ipv4-family vpn-instance vpnb
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] group 172-21 external
[PE1-bgp-af-vpn-instance] peer 172.21.21.2 group 172-21 as-number 65021
[PE1-bgp-af-vpn-instance] peer 172.21.21.2 next-hop-local
[PE1-bgp-af-vpn-instance] quit
```

Enable MP-IBGP between PE-ASBRs.

```
[PE1-bgp] group 3 internal
[PE1-bgp] peer 3.3.3.3 group 3
[PE1-bgp] peer 3.3.3.3 connect-interface loopback0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 3 enable
[PE1-bgp-af-vpn] peer 3.3.3.3 group 3
[PE1-bgp-af-vpn] quit
[PE1-bgp] quit
```

2 Configure PE2

Configure MPLS.

```
[PE2] mpls lsr-id 2.2.2.2
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
```

Configure the VLAN interface connecting CE.

```
[PE2] vlan 203
[PE2-vlan203] port gigabitethernet 2/1/1
[PE2-vlan203] quit
[PE2] vlan 204
[PE2-vlan204] port gigabitethernet 2/1/2
[PE2-vlan204] quit
```

Configure Loopback interface.

```
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 2.2.2.2 255.255.255.255
```

Configure VPN-instance.

```
[PE2] ip vpn-instance vpna
[PE2-vpn-vpna] route-distinguisher 200:1
[PE2-vpn-vpna] vpn-target 100:1 both
[PE2] ip vpn-instance vpb
[PE2-vpn-vpb] route-distinguisher 200:2
[PE2-vpn-vpb] vpn-target 100:2 both
```

Configure the VLAN interface connecting PE2 and P2.

```
[PE1] vlan 205
[PE1-vlan205] port gigabitethernet 2/2/1
[PE1-vlan205] quit
[PE1] interface Vlan-interface 205
[PE1-Vlan-interface205] mpls
[PE1-Vlan-interface205] mpls ldp enable
[PE1-Vlan-interface205] ip address 20.1.1.2 255.255.255.0
```

Bind the VLAN interface with the VPN-instance.

```
[PE2] interface Vlan-interface 203
[PE2-Vlan-interface203] ip binding vpn-instance vpna
[PE2-Vlan-interface203] ip address 172.12.12.1 255.255.255.0
[PE2-Vlan-interface203] quit
[PE2] interface Vlan-interface 204
[PE2-Vlan-interface204] ip binding vpn-instance vpb
[PE2-Vlan-interface204] ip address 172.22.22.1 255.255.255.0
[PE2-Vlan-interface204] quit
```

Enable EBGP between PE and CE.

```
[PE2] bgp 200
[PE2-bgp] ipv4-family vpn-instance vpna
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] group 172-12 external
[PE2-bgp-af-vpn-instance] peer 172.12.12.2 group 172-12 as-number 65012
[PE2-bgp] ipv4-family vpn-instance vpb
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] group 172-22 external
[PE2-bgp-af-vpn-instance] peer 172.22.22.2 group 172-22 as-number 65022
[PE2-bgp-af-vpn-instance] quit
[PE2] quit
```

Enable MB-IBGP between PE-ASBRs

```
[PE2-bgp] group 4
[PE2-bgp] peer 4.4.4.4 group 4
[PE2-bgp] peer 4.4.4.4 connect-interface loopback0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer 4 enable
[PE2-bgp-af-vpn] peer 4.4.4.4 group 4
```

3 Configure P1 (P2 in similar way)

Configure MPLS basic capability.

```
[P1] mpls lsr-id 3.3.3.3
[P1] mpls
[P1-mpls] quit
[P1] mpls ldp
```

Configure the interface Loopback 0.

```
[P1] interface loopback 0
[P1-LoopBack0] ip address 3.3.3.3 255.255.255.255
```

Configure VLAN interface connecting PE1.

```
[P1] vlan 205
[P1-vlan205] port gigabitethernet 2/1/1
[P1-vlan205] quit
[P1] interface Vlan-interface 205
[P1-Vlan-interface205] mpls
[P1-Vlan-interface205] mpls ldp enable
[P1-Vlan-interface205] ip address 10.1.1.1 255.255.255.0
[P1-Vlan-interface205] quit
```

Configure VLAN interface connecting PE2.

```
[P1] vlan 206
[P1-vlan206] port gigabitethernet 2/1/2
[P1-vlan206] quit
[P1] interface Vlan-interface 206
[P1-Vlan-interface206] mpls
[P1-Vlan-interface206] mpls ldp enable
[P1-Vlan-interface206] ip address 98.98.98.1 255.255.255.0
[P1-Vlan-interface206] quit
```

Configure IBGP neighbors and EBGP neighbors.

```
[P1] bgp 100
[P1-bgp] group 1 internal
[P1-bgp] peer 1.1.1.1 group 1
[P1-bgp] peer 1.1.1.1 connect-interface loopback0
[P1-bgp] group 4 external
[P1-bgp] peer 98.98.98.2 group 4 as-number 200
[P1-bgp] ipv4-family vpnv4
[P1-bgp-af-vpn] peer 1 enable
[P1-bgp-af-vpn] peer 1.1.1.1 group 1
[P1-bgp-af-vpn] peer 1 next-hop-local
[P1-bgp-af-vpn] peer 98 enable
[P1-bgp-af-vpn] peer 98.98.98.2 group 98
[P1-bgp-af-vpn] undo policy vpn-target
```

Cross-Domain BGP/MPLS VPN Configuration Example - Option C

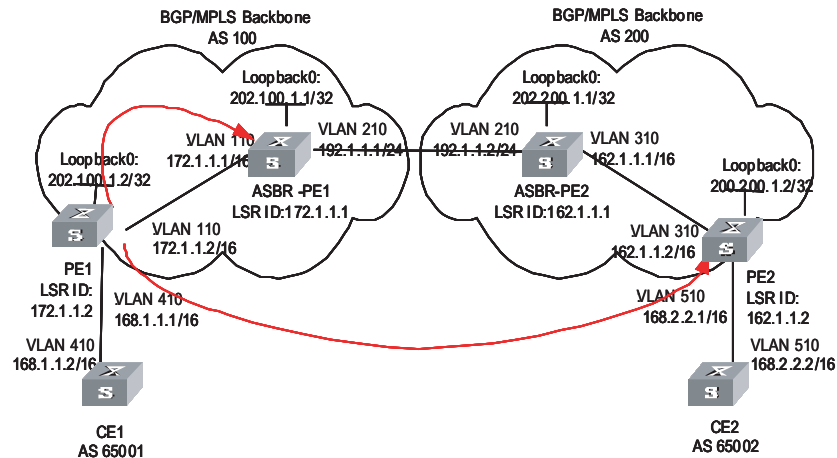
Network requirements

CE1 and CE2 belong to the same VPN. CE1 accesses the MPLS network through PE1 in AS100; and CE2 accesses the MPLS network through PE2 in AS200.

The example adopts Option C to implement a cross-domain BGP/MPLS VPN, that is, the VPN routing is managed by the Multi-hop MP-EBGP which advertise label VPN-IPv4 routes between PEs.

Network diagram

Figure 139 Network diagram for Multihop EBGP cross-domain VPN



Configuration procedure

- Configuring OSPF on the MPLS backbone network
 - Configuring basic MPLS capability on the MPLS backbone network
 - Configuring a VPN instance on PEs.
 - Configuring MP-BGP
- 1 Configure OSPF as the IGP protocol on the MPLS backbone network; making OSPFs on PEs can learn routes from each other. Create OSPF neighbor between ASBR-PE and PE in the same AS.

Configure PE1.

```
[PE1] interface loopback0
[PE1-LoopBack0] ip address 202.100.1.2 255.255.255.255
[PE1-LoopBack0] quit
[PE1] vlan 110
[PE1-vlan110] interface vlan-interface 110
[PE1-Vlan-interface110] ip address 172.1.1.2 255.255.0.0
[PE1-Vlan-interface110] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[PE1-ospf-1-area-0.0.0.0] network 202.100.1.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

Configure ASBR-PE1.

```
[ASBR-PE1] interface loopback0
[ASBR-PE1-LoopBack 0] ip address 202.100.1.1 255.255.255.255
[ASBR-PE1-LoopBack 0] quit
```

```
[ASBR-PE1] vlan 110
[ASBR-PE1-vlan110] interface vlan 110
[ASBR-PE1-Vlan-interface110] ip address 172.1.1.1 255.255.0.0
[ASBR-PE1-Vlan-interface110] quit
[ASBR-PE2] vlan 210
[ASBR-PE1-vlan210] interface vlan 210
[ASBR-PE1-Vlan-interface210] ip address 192.1.1.1 255.255.255.0
[ASBR-PE1-Vlan-interface210] quit
[ASBR-PE1] ospf
[ASBR-PE1-ospf-1] area 0
[ASBR-PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[ASBR-PE1-ospf-1-area-0.0.0.0] network 202.100.1.1 0.0.0.0
[ASBR-PE1-ospf-1-area-0.0.0.0] quit
[ASBR-PE1-ospf-1] quit
```

Configure PE2.

```
[PE2] interface loopback0
[PE2-LoopBack0] ip address 202.200.1.2 255.255.255.255
[PE2-LoopBack0] quit
[PE2]vlan 310
[PE2-vlan310] interface vlan 310
[PE2-Vlan-interface310] ip address 162.1.1.2 255.255.0.0
[PE2- Vlan-interface310] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[PE2-ospf-1-area-0.0.0.0] network 202.200.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Configure ASBR-PE2.

```
[ASBR-PE2] interface loopback0
[ASBR-PE2-LoopBack0] ip address 202.200.1.1 255.255.255.255
[ASBR-PE2-LoopBack0] quit
[ASBR-PE2] interface vlan 310
[ASBR-PE2-Vlan-interface310] ip address 162.1.1.1 255.255.0.0
[ASBR-PE2-Vlan-interface310] quit
[ASBR-PE2] vlan 210
[ASBR-PE2-vlan210] interface vlan 210
[ASBR-PE2-Vlan-interface210] ip address 192.1.1.2 255.255.255.0
[ASBR-PE2-Vlan-interface210] quit
[ASBR-PE2] ospf
[ASBR-PE2-ospf-1] area 0
[ASBR-PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[ASBR-PE2-ospf-1-area-0.0.0.0] network 202.200.1.1 0.0.0.0
[ASBR-PE2-ospf-1-area-0.0.0.0] quit
[ASBR-PE2-ospf-1] quit
```

- 2 Configure basic MPLS capability on the MPLS backbone network to enable the network to forward VPN traffic.



MPLS must be enabled between the ASBR-PEs.

Configure basic MPLS capability on PE1 and enable LDP on the interface connected to ASBR-PE1.


```
[PE1] mpls lsr-id 172.1.1.2
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface vlan 110
[PE1-Vlan-interface110] mpls
[PE1-Vlan-interface110] mpls ldp
[PE1-Vlan-interface110] quit
```

Configure basic MPLS capability on ASBR-PE1, enable LDP on the interface connected to PE1, and enable MPLS on the interface connected to ASBR-PE2.

```
[ASBR-PE1] mpls lsr-id 172.1.1.1
[ASBR-PE1-mpls] lsp-trigger all
[ASBR-PE1-mpls] quit
[ASBR-PE1] mpls ldp
[ASBR-PE1-mpls-ldp] quit
[ASBR-PE1] interface vlan 110
[ASBR-PE1-Vlan-interface110] mpls
[ASBR-PE1-Vlan-interface110] mpls ldp
[ASBR-PE1-Vlan-interface110] quit
[ASBR-PE1] interface vlan 210
[ASBR-PE1-Vlan-interface210] mpls
[ASBR-PE1-Vlan-interface210] quit
```

Configure basic MPLS capability on ASBR-PE2, enable LDP on the interface connected to PE2, and enable MPLS on the interface connected to ASBR-PE1.

```
[ASBR-PE2] mpls lsr-id 162.1.1.1
[ASBR-PE2-mpls] lsp-trigger all
[ASBR-PE2-mpls] quit
[ASBR-PE2] mpls ldp
[ASBR-PE2-mpls-ldp] quit
[ASBR-PE2] interface vlan 310
[ASBR-PE2-Vlan-interface310] mpls
[ASBR-PE2-Vlan-interface310] mpls ldp
[ASBR-PE2-Vlan-interface310] quit
[ASBR-PE2] interface vlan 210
[ASBR-PE2-Vlan-interface210] mpls
[ASBR-PE2-Vlan-interface310] quit
```

Configure basic MPLS capability on PE2 and enable LDP on the interface connected to ASBR-PE2.

```
[PE2] mpls lsr-id 162.1.1.2
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface vlan 310
[PE2-Vlan-interface310] mpls
[PE2-Vlan-interface310] mpls ldp
[PE2-Vlan-interface310] quit
```

- 3 Create a VPN instance on each PE, and bind the instance to the interface connected to the corresponding CE.

Configure CE1

```
[CE1] vlan 410
[CE1-vlan410] interface vlan 410
[CE1-Vlan-interface410] ip address 168.1.1.2 255.255.0.0
[CE1-Vlan-interface410] quit
```

Create a VPN instance on PE1 and bind it to the interface connected to CE1

```
[PE1] ip vpn-instance vpna
[PE1-vpn-vpna] route-distinguisher 100:2
[PE1-vpn-vpna] vpn-target 100:1 both
[PE1-vpn-vpna] quit
[PE1]vlan 410
[PE1] interface vlan 410
[PE1-Vlan-interface410] ip binding vpn-instance vpna
[PE1-Vlan-interface410] ip address 168.1.1.1 255.255.0.0
[PE1-Vlan-interface410] quit
```

Configure CE2

```
[CE2] vlan 510
[CE2-vlan510] interface vlan 510
[CE2-Vlan-interface510] ip address 168.2.2.2 255.255.0.0
[CE2-Vlan-interface510] quit
```

Create a VPN instance on PE2 and bind it to the interface connected to CE2

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance] route-distinguisher 200:2
[PE2-vpn-instance] vpn-target 100:1 both
[PE2-vpn-instance] quit
[PE2] vlan 510
[PE2] interface vlan 510
[PE2-Vlan-interface510] ip binding vpn-instance vpna
[PE2-Vlan-interface510] ip address 168.2.2.1 255.255.0.0
[PE2-Vlan-interface510] quit
```

- 4** Configure MP-BGP, set up IBGP peer relation between PEs, and set up EBGP peer relation between PEs and their CEs.



- Enable the exchanging of label-carried IPv4 route between the following routers: PE1 and ASBR-PE1, PE2 and ASBR-PE2, ASBR-PE1 and ASBR-PE2.
- Make each ASBR-PE change the next hop to its own when it advertises routes to the PE in the same AS.
- Configure routing policy on each ASBR-PE as follows: make the ASBR-PE assign MPLS label when it advertises a route received from the PE in this AS to the ASBR-PE in the peer AS, and let the ASBR-PE assign a new MPLS label when it advertises a label-carried IPv4 route to the PE in this AS.

Configure CE1

```
[CE1] bgp 65001
[CE1-bgp] group 20 external
```

```
[CE1-bgp] peer 168.1.1.1 group 20 as-number 100
[CE1-bgp] quit
```

Configure PE1: set up EBGP peer relation with CE1, IBGP peer relation with ASBR-PE1, and Multihop MP-EBGP peer relation with PE2.

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] group 10 external
[PE1-bgp-af-vpn-instance] peer 168.1.1.2 group 10 as-number 65001
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] group 20
[PE1-bgp] peer 20 label-route-capability
[PE1-bgp] peer 202.100.1.1 group 20
[PE1-bgp] peer 202.100.1.1 connect-interface loopback0
[PE1-bgp] group 30 external
[PE1-bgp] peer 30 ebgp-max-hop
[PE1-bgp] peer 200.200.1.2 group 30 as-number 200
[PE1-bgp] peer 200.200.1.2 connect-interface loopback0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 30 enable
[PE1-bgp-af-vpn] peer 200.200.1.2 group 30
[PE1-bgp-af-vpn] quit
[PE1-bgp] quit
```

Configure ASBR-PE1: configure the route policy.

```
[ASBR-PE1] acl number 2001
[ASBR-PE1-acl-basic-2001] rule permit source 202.100.1.2 0
[ASBR-PE1-acl-basic-2001] rule deny source any
[ASBR-PE1-acl-basic-2001] quit
[ASBR-PE1] route-policy rtp-ebgp permit node 1
[ASBR-PE1-route-policy] if-match acl 2001
[ASBR-PE1-route-policy] apply mpls-label
[ASBR-PE1-route-policy] quit
[ASBR-PE1] route-policy rtp-ibgp permit node 10
[ASBR-PE1-route-policy] if-match mpls-label
[ASBR-PE1-route-policy] apply mpls-label
[ASBR-PE1-route-policy] quit
```

Configure ASBR-PE1: set up EBGP peer relation with ASBR-PE2, and IBGP peer relation with PE1.

```
[ASBR-PE1] bgp 100
[ASBR-PE1-bgp] import-route ospf
[ASBR-PE1-bgp] group 10 external
[ASBR-PE1-bgp] peer 10 label-route-capability
[ASBR-PE1-bgp] peer 10 route-policy rtp-ebgp export
[ASBR-PE1-bgp] peer 192.1.1.2 group 10 as-number 200
[ASBR-PE1-bgp] group 20
[ASBR-PE1-bgp] peer 20 label-route-capability
[ASBR-PE1-bgp] peer 20 next-hop-local
[ASBR-PE1-bgp] peer 20 route-policy rtp-ibgp export
[ASBR-PE1-bgp] peer 202.100.1.2 group 20
[ASBR-PE1-bgp] peer 202.100.1.2 connect-interface loopback0
[ASBR-PE1-bgp] quit
```

Configure CE2.

```
[CE2] bgp 65002
[CE2-bgp] group 10 external
[CE2-bgp] peer 168.2.2.1 group 10 as-number 200
[CE2-bgp] quit
```

Configure PE2: set up EBGP peer relation with CE2, IBGP peer relation with ASBR-PE2, and Multihop MP-EBGP peer relation with PE1.

```
[PE2] bgp 200
[PE2-bgp] ipv4-family vpn-instance vpna
[PE2-bgp-af-vpn-instance] group 10 external
[PE2-bgp-af-vpn-instance] peer 168.2.2.2 group 10 as-number 65002
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] group 20
[PE2-bgp] peer 20 label-route-capability
[PE2-bgp] peer 202.200.1.1 group 20
[PE2-bgp] peer 202.200.1.1 connect-interface loopback0
[PE2-bgp] group 30 external
[PE2-bgp] peer 30 ebgp-max-hop
[PE2-bgp] peer 202.100.1.2 group 30 as-number 100
[PE2-bgp] peer 202.100.1.2 connect-interface loopback0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer 30 enable
[PE2-bgp-af-vpn] peer 202.100.1.2 group 30
[PE2-bgp-af-vpn] quit
[PE2-bgp] quit
```

Configure ASBR-PE2: configure the route policy.

```
[ASBR-PE2] acl number 2001
[ASBR-PE2-acl-basic-2001] rule permit source 200.200.1.2 0
[ASBR-PE2-acl-basic-2001] rule deny source any
[ASBR-PE2-acl-basic-2001] quit
[ASBR-PE2] route-policy rtp-ebgp permit node 1
[ASBR-PE2-route-policy] if-match acl 2001
[ASBR-PE2-route-policy] apply mpls-label
[ASBR-PE2-route-policy] quit
[ASBR-PE2] route-policy rtp-ibgp permit node 10
[ASBR-PE2-route-policy] if-match mpls-label
[ASBR-PE2-route-policy] apply mpls-label
[ASBR-PE2-route-policy] quit
```

Configure ASBR-PE2: set up EBGP peer relation with ASBR-PE1, and IBGP peer relation with PE2.

```
[ASBR-PE2] bgp 200
[ASBR-PE2-bgp] import-route ospf
[ASBR-PE2-bgp] group 10 external
[ASBR-PE2-bgp] peer 10 label-route-capability
[ASBR-PE2-bgp] peer 10 route-policy rtp-ebgp export
[ASBR-PE2-bgp] peer 192.1.1.1 group 10 as-number 100
[ASBR-PE2-bgp] group 20
[ASBR-PE2-bgp] peer 20 label-route-capability
[ASBR-PE2-bgp] peer 20 next-hop-local
```

```
[ASBR-PE2-bgp] peer 20 route-policy rtp-ibgp export
[ASBR-PE2-bgp] peer 202.200.1.2 group 20
[ASBR-PE2-bgp] peer 202.200.1.2 connect-interface loopback0
```

Hierarchical BGP/MPLS VPN Configuration Example

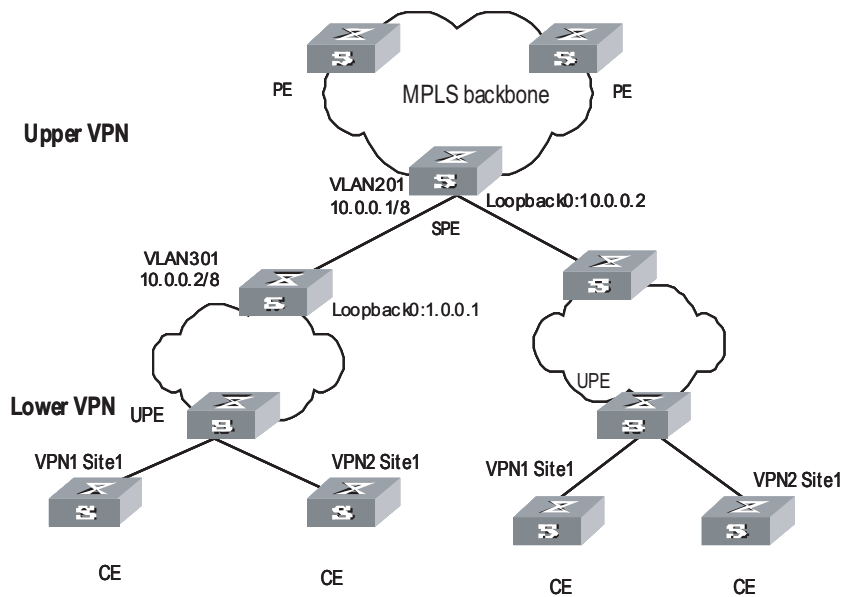
Network requirements

For those VPNs that have distinct hierarchy, an MPLS VPN covering a province and its cities, for example, incorporating the backbone network at the province level and the networks at the city level into a single MPLS VPN will impose a high requirement in performance on the equipment on the entire network, in the event that the network topology size is large. However, the requirement in equipment performance can become lower if this MPLS VPN is separated into two VPNs, the network at the province level and the network at the city level, for example.

SPE acts as a PE on the network at the province level, and is connected with a downstream MPLS VPN at the city level. UPE acts as a PE on the network at the city level and provide access service for the VPN clients which are normally low-end routers.

Network diagram

Figure 140 Network diagram for hierarchical BGP/MPLS VPN



Configuration procedure

This case only illustrates the configurations concerned with PEs in a hierarchical BGP/MPLS VPN.

1 Configure SPE

Configure the basic MPLS capability.

```
[SPE] mpls lsr-id 1.0.0.2
[SPE] mpls
[SPE-mpls] quit
[SPE] mpls ldp
```

Configure VPN-instance

```
[SPE] ip vpn-instance vpn1
[SPE-vpn-vpn1] route-distinguisher 100:1
[SPE-vpn-vpn1] vpn-target 100:1 both
```

Configure interfaces (So far as a PE router concerned, its Loopback 0 interface must be assigned with a host address of 32-bit mask.

```
[SPE] vlan 201
[SPE-vlan201] port gigabitethernet 2/1/1
[SPE-vlan201] quit
[SPE] interface Vlan-interface 201
[SPE-Vlan-interface201] ip address 10.0.0.1 255.0.0.0
[SPE-Vlan-interface201] mpls
[SPE-Vlan-interface201] mpls ldp enable
[SPE-Vlan-interface201] quit
[SPE] interface loopback0
[SPE-LoopBack 0] ip address 1.0.0.2 255.255.255.255
[SPE-LoopBack 0] quit
```

Configure BGP

```
[SPE] bgp 100
[SPE] import direct
[SPE-bgp] group 1 internal
[SPE-bgp] peer 1.0.0.1 group 1
[SPE-bgp] peer 1 connect-interface LoopBack0
[SPE-bgp] ipv4-family vpn-instance vpn1
[SPE--bgp-af-vpn-instance] import direct
[SPE--bgp-af-vpn-instance] quit
[SPE-bgp] ipv4-family vpnv4
[SPE-bgp-af-vpn] peer 1 enable
[SPE-bgp-af-vpn] peer 1.0.0.1 group 1
[SPE-bgp-af-vpn] peer 1.0.0.1 upe
[SPE-bgp-af-vpn] peer 1.0.0.1 default-route-advertise vpn-instance vpn1
[SPE-bgp-af-vpn] quit
[SPE-bgp] quit
```

Configure OSPF

```
[SPE] ospf
[SPE] import-route direct
[SPE-ospf-1] area 0
[SPE-ospf-1-area-0.0.0.0] network 1.0.0.2 0.0.0.0
[SPE-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
```

2 Configure UPE

Configure the basic MPLS capability.

```
[UPE] mpls lsr-id 1.0.0.1
[UPE] mpls
[UPE-mpls] quit
[UPE] mpls ldp
```

Configure VPN-instance

```
[UPE] ip vpn-instance vpn1
[UPE-vpn-vpn1] route-distinguisher 100:1
[UPE-vpn-vpn1] vpn-target 100:1 both
```

Configure interfaces

```
[UPE] vlan 301
[UPE-vlan301] port gigabitethernet 2/2/1
[UPE-vlan301] quit
[UPE] interface Vlan-interface 301
[UPE-Vlan-interface301] mpls
[UPE-Vlan-interface301] mpls ldp enable
[UPE-Vlan-interface301] mpls ldp transport-ip interface
[UPE-Vlan-interface301] ip address 10.0.0.2 255.0.0.0
[UPE-Vlan-interface301] quit
[UPE] interface loopback0
[UPE-LoopBack 0] ip address 1.0.0.1 255.255.255.255
```

Configure BGP

```
[UPE] bgp 100
[UPE-bgp] group 1 internal
[UPE-bgp] peer 1.0.0.2 group 1
[UPE-bgp] ipv4-family vpn-instance vpn1
[UPE--bgp-af-vpn-instance] import direct
[UPE-bgp] ipv4-family vpnv4
[UPE-bgp-af-vpn] peer 1 enable
[UPE-bgp-af-vpn] peer 1.0.0.2 group 1
```

Configure OSPF

```
[UPE] ospf
[UPE-ospf-1] import-route direct
[UPE-ospf-1] area 0
[UPE-ospf-1-area-0.0.0.0] network 1.0.0.1 0.0.0.0
[UPE-ospf-1-area-0.0.0.0] network 10.0.0.2 0.255.255.255
[UPE-ospf-1-area-0.0.0.0] quit
```

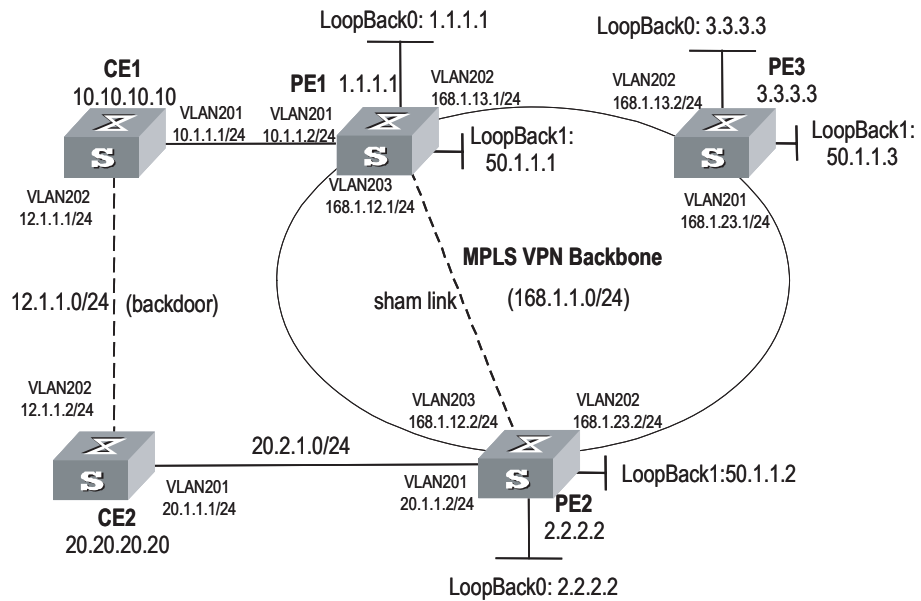
OSPF Multi-instance Sham-link Configuration Example

Network requirements

As shown in the following picture, a company connects to a WAN through OSPF multi-instance function of 3Com router. OSPF is bind to VPN1.MPLS VPN backbone runs between PEs and OSPF runs between PE and CE. Configure a Sham-link between PE1 and PE2 to ensure the traffic between CE1 and CE2 does not pass the Backdoor link that directly connects CE1 and CE2.

Network diagram

Figure 141 Network diagram for OSPF multi-instance



Configuration procedure

1 Configure PE1

Enable MPLS and LDP.

```
[PE1] mpls lsr-id 50.1.1.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
```

Configure VPN-instance.

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-vpn1] route-distinguisher 2:1
[PE1-vpn-vpn1] vpn-target 100:1 export-extcommunity
[PE1-vpn-vpn1] vpn-target 100:1 import-extcommunity
```

Configure VLAN interface.

```
[PE1] vlan 203
[PE1-vlan203] port gigabitethernet 2/1/3
[PE1-vlan203] quit
[PE1] interface Vlan-interface 203
[PE1-Vlan-interface203] ip address 168.1.12.1 255.255.255.0
[PE1-Vlan-interface203] mpls
[PE1-Vlan-interface203] mpls ldp enable
[PE1-Vlan-interface203] quit
[PE1] vlan 201
[PE1-vlan201] port gigabitethernet 2/1/1
[PE1-vlan201] quit
[PE1] interface Vlan-interface 201
[PE1-Vlan-interface201] ip binding vpn-instance vpn1
[PE1-Vlan-interface201] ip address 10.1.1.2 255.255.255.0
```



```

[PE1-Vlan-interface201] ospf cost 1
[PE1-Vlan-interface201] quit
[PE1] vlan 202
[PE1-vlan202] port gigabitethernet 2/1/2
[PE1-vlan202] quit
[PE1] interface Vlan-interface 202
[PE1-Vlan-interface202] ip address 168.1.13.1 255.255.255.0
[PE1-Vlan-interface202] ospf cost 1
[PE1-Vlan-interface202] mpls
[PE1-Vlan-interface202] mpls ldp enable
[PE1-Vlan-interface202] mpls ldp transport-ip interface
[PE1-Vlan-interface202] quit
[PE1] interface loopback0
[PE1-LoopBack0] ip binding vpn-instance vpn1
[PE1-LoopBack0] ip address 1.1.1.1 255.255.255.255
[PE1-LoopBack0] quit
[PE1] interface loopback1
[PE1-LoopBack1] ip address 50.1.1.1 255.255.255.255

```

Configure BGP Peer.

```

[PE1] bgp 100
[PE1-bgp] undo synchronization
[PE1-bgp] group fc internal
[PE1-bgp] peer 50.1.1.2 group fc
[PE1-bgp] peer 50.1.1.2 connect-interface LoopBack1
[PE1-bgp] peer 50.1.1.3 group fc

```

Configure BGP and import OSPF routing and direct-connect route.

```

[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-af-vpn-instance] import-route ospf 100
[PE1-bgp-af-vpn-instance] import-route ospf-ase 100
[PE1-bgp-af-vpn-instance] import-route ospf-nssa 100
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] undo synchronization

```

Create and activate Peer in MBGP.

```

[PE1-bgp-af-vpn] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer fc enable
[PE1-bgp-af-vpn] peer fc advertise-community
[PE1-bgp-af-vpn] peer 50.1.1.2 group fc

```

Bind OSPF process to VPN-instance.

```

[PE1] ospf 100 router-id 1.1.1.1 vpn-instance vpn1
[PE1-ospf-100] import-route bgp
[PE1-ospf-100] area 0.0.0.0
[PE1-ospf-100-area-0.0.0.0] network 10.1.1.0 0.0.0.255

```

Configuring Sham-link

```

[PE1-ospf-100-area-0.0.0.1] sham-link 1.1.1.1 2.2.2.2

```

Configure the routes distributed to PE2 and PE3.

```
[PE1] ospf 1000
[PE1-ospf-1000] area 0
[3Com-ospf-1000-area-0.0.0.0] network 168.12.1.0 0.0.0.255
[3Com-ospf-1000-area-0.0.0.0] network 50.1.1.1 0.0.0.0
```

2 Configure PE2

Enable MPLS and LDP.

```
[PE2] mpls lsr-id 50.1.1.2
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
```

Configure VPN-instance VPN1.

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-vpn1] route-distinguisher 2:1
[PE2-vpn-vpn1] vpn-target 100:1 export-extcommunity
[PE2-vpn-vpn1] vpn-target 100:1 import-extcommunity
```

Configure VLAN interface.

```
[PE2] vlan 203
[PE2-vlan203] port gigabitethernet 2/1/3
[PE2-vlan203] quit
[PE2] interface Vlan-interface 203
[PE2-Vlan-interface203] ip address 168.1.12.2 255.255.255.0
[PE2-Vlan-interface203] mpls
[PE2-Vlan-interface203] mpls ldp enable
[PE2-Vlan-interface203] quit
[PE2] vlan 201
[PE2-vlan201] port gigabitethernet 2/1/1
[PE2-vlan201] quit
[PE2] interface Vlan-interface 201
[PE2-Vlan-interface201] ip binding vpn-instance vpn1
[PE2-Vlan-interface201] ip address 20.1.1.2 255.255.255.0
[PE2-Vlan-interface201] ospf cost 1
[PE2-Vlan-interface201] quit
[PE2] vlan 202
[PE2-vlan202] port gigabitethernet 2/1/2
[PE2-vlan202] quit
[PE2] interface Vlan-interface 202
[PE2-Vlan-interface202] ip address 168.1.23.2 255.255.255.0
[PE2-Vlan-interface202] ospf cost 1
[PE2-Vlan-interface202] mpls
[PE2-Vlan-interface202] mpls ldp enable
[PE2-Vlan-interface202] quit
[PE2] interface LoopBack0
[PE2-LoopBack0] ip binding vpn-instance vpn1
[PE2-LoopBack0] ip address 2.2.2.2 255.255.255.255
[PE2-LoopBack0] quit
[PE2] interface LoopBack1
[PE2-LoopBack1] ip address 50.1.1.2 255.255.255.255
```

Configure BGP.

```
[PE2] bgp 100
[PE2-bgp] undo synchronization
[PE2-bgp] group fc internal
[PE2-bgp] peer 50.1.1.1 group fc
[PE2-bgp] peer 50.1.1.1 connect-interface LoopBack1
[PE2-bgp] peer 50.1.1.3 group fc
```

Configure VPN-instance and import OSPF and direct-connect route.

```
[PE2-bgp] ipv4-family vpn-instance vpn1
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] import-route ospf-nssa 100
[PE2-bgp-af-vpn-instance] import-route ospf-ase 100
[PE2-bgp-af-vpn-instance] import-route ospf 100
[PE2-bgp-af-vpn-instance] undo synchronization
```

Configure MBGP and enable Peer.

```
[PE2-bgp-af-vpn] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer fc enable
[PE2-bgp-af-vpn] peer fc advertise-community
[PE2-bgp-af-vpn] peer 50.1.1.1 group fc
```

Configure OSPF and import BGP and direct-connect route.

```
[PE2] ospf 100 router-id 2.2.2.2 vpn-instance vpn1
[PE2-ospf-100] import-route bgp
[PE2-ospf-100] import-route static
[PE2-ospf-100] area 0.0.0.0
[PE2-ospf-100-area-0.0.0.0] network 20.1.1.0 0.0.0.255
```

Configuring Sham-link

```
[PE2-ospf-100-area-0.0.0.0] sham-link 2.2.2.2 1.1.1.1
```

Configure static route to PE1 and PE3.

```
[PE2] ip route-static 50.1.1.1 255.255.255.255 168.1.12.1
[PE2] ip route-static 50.1.1.3 255.255.255.255 168.1.23.3
```

Configure the routes distributed to PE1 and PE3.

```
[PE1] ospf 1000
[PE1-ospf-1000] area 0
[3Com-ospf-1000-area-0.0.0.0] network 168.12.1.0 0.0.0.255
[3Com-ospf-1000-area-0.0.0.0] network 50.1.1.1 0.0.0.0
```

3 Configure CE1.

Configure interfaces

```
[CE1] vlan 202
[CE1-vlan202] port gigabitethernet 2/1/2
[CE1-vlan202] quit
[CE1] interface Vlan-interface 202
[CE1-Vlan-interface202] ip address 12.1.1.1 255.255.255.0
[CE1-Vlan-interface202] ospf cost 100
[CE1-Vlan-interface202] quit
```

```
[CE1] vlan 201
[CE1-vlan201] port gigabitethernet 2/1/1
[CE1-vlan201] quit
[CE1] interface Vlan-interface 201
[CE1-Vlan-interface201] ip address 10.1.1.1 255.255.255.0
[CE1-Vlan-interface201] ospf cost 1
```

Configure OSPF.

```
[CE1] ospf 100 router-id 10.10.10.129
[CE1-ospf-100] import-route direct
[CE1-ospf-100] area 0.0.0.0
[CE1-ospf-100-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[CE1-ospf-100-area-0.0.0.0] network 12.1.1.0 0.0.0.255
```

4 Configure CE2

Configure interface.

```
[CE2] vlan 202
[CE2-vlan202] port gigabitethernet 2/1/2
[CE2-vlan202] quit
[CE2] interface Vlan-interface 202
[CE2-Vlan-interface202] ip address 12.1.1.2 255.255.255.0
[CE2-Vlan-interface202] ospf cost 100
[CE2-Vlan-interface202] quit
[CE2] vlan 201
[CE2-vlan201] port gigabitethernet 2/1/1
[CE2-vlan201] quit
[CE2] interface Vlan-interface 201
[CE2-Vlan-interface201] ip address 20.1.1.1 255.255.255.0
[CE2-Vlan-interface201] ospf cost 1
```

Configure OSPF.

```
[CE2] ospf 100 router-id 20.20.20.20
[CE2-ospf-100] area 0.0.0.0
[CE2-ospf-100-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[CE2-ospf-100-area-0.0.0.0] network 20.1.1.0 0.0.0.255
```

Nested BGP/MPLS VPN Configuration Example

Network requirements

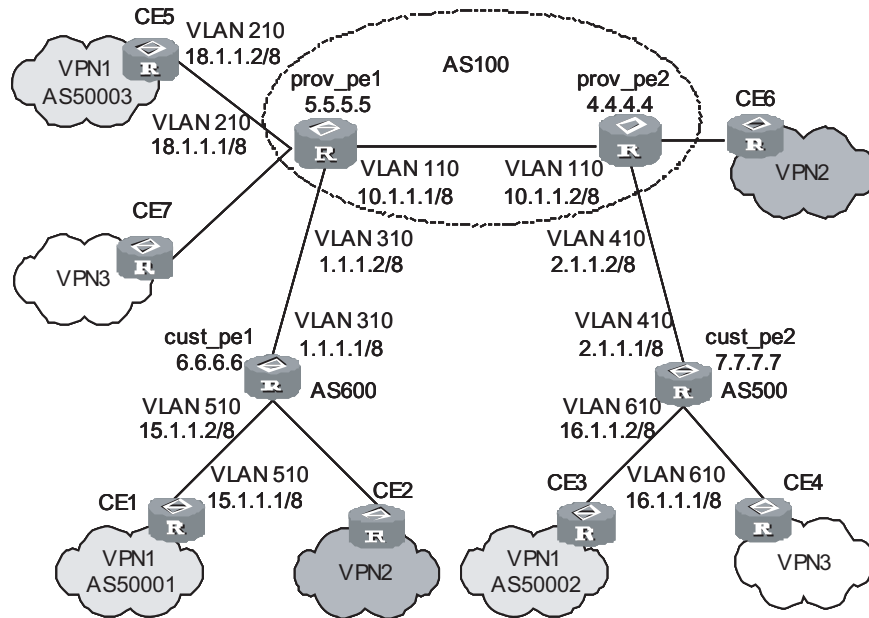
A VPN user has multiple nodes to access the service provider's BGP/MPLS backbone network. And this VPN is divided into three sub-VPNs: VPN1, VPN2 and VPN3.

Some of the nodes of these sub-VPNs directly access a PE in the network, and some access a PE through the father VPN. That is, the adopted network structure is unsymmetrical.

This example mainly describes the configuration of VPN1; the configuration of other sub-VPNs is similar.

Network diagram

Figure 142 Network diagram for nested VPN



Configuration procedure



This procedure omits part of the configuration for CE router.

- 1 Configure IGP on the service provider's backbone network.

Configure prov_pe1.

```
<SW8800> system-view
[SW8800] sysname prov_pe1
[prov_pe1] interface LoopBack0
[prov_pe1-LoopBack0] ip address 5.5.5.5 255.255.255.255
[prov_pe1-LoopBack0] quit
[prov_pe1] vlan 110
[prov_pe1-vlan110] interface vlan 110
[prov_pe1-Vlan-interface110] ip address 10.1.1.1 255.0.0.0
[prov_pe1-Vlan-interface110] quit
[prov_pe1] ospf
[prov_pe1-ospf] area 0
[prov_pe1-ospf-area-0.0.0.0] network 5.5.5.5 0.0.0.0
[prov_pe1-ospf-area-0.0.0.0] network 10.0.0.0 0.255.255.255
```

Configure prov_pe2.

```
<SW8800> system-view
[SW8800] sysname prov_pe2
[prov_pe2] interface LoopBack0
[prov_pe2-LoopBack0] ip address 4.4.4.4 255.255.255.255
[prov_pe2-LoopBack0] quit
[prov_pe1] vlan 110
[prov_pe1-vlan110] interface vlan-interface 110
```

```
[prov_pe1-Vlan-interface110] ip address 10.1.1.2 255.0.0.0
[prov_pe1-Vlan-interface110] quit
[prov_pe2] ospf
[prov_pe2-ospf] area 0
[prov_pe2-ospf-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[prov_pe2-ospf-area-0.0.0.0] network 10.0.0.0 0.255.255.255
```

Configure basic MPLS capability and MPLS LDP on the backbone network.

Configure prov_pe1.

```
[prov_pe1] mpls lsr-id 5.5.5.5
[prov_pe1] mpls ldp
[prov_pe1] interface vlan 110
[prov_pe1- Vlan-interface110] mpls
[prov_pe1- Vlan-interface110] mpls ldp
[prov_pe1- Vlan-interface110] quit
```

Configure prov_pe2.

```
[prov_pe2] mpls lsr-id 4.4.4.4
[prov_pe2] mpls ldp
[prov_pe2] interface vlan 110
[prov_pe2- Vlan-interface110] mpls
[prov_pe2- Vlan-interface110] mpls ldp
[prov_pe2- Vlan-interface110] quit
```

Configure IBGP between provider PEs.

Configure prov_pe1.

```
[prov_pe1] bgp 100
[prov_pe1-bgp] group ibgp internal
[prov_pe1-bgp] peer 4.4.4.4 group ibgp
[prov_pe1-bgp] peer 4.4.4.4 connect-interface LoopBack0
[prov_pe1-bgp] ipv4-family vpnv4
[prov_pe1-bgp-af-vpn] peer ibgp enable
[prov_pe1-bgp-af-vpn] peer ibgp next-hop-local
[prov_pe1-bgp-af-vpn] peer 4.4.4.4 group ibgp
[prov_pe1-bgp-af-vpn] quit
[prov_pe1-bgp] quit
```

Configure prov_pe2.

```
[prov_pe2] bgp 100
[prov_pe2-bgp] group ibgp internal
[prov_pe2-bgp] peer 5.5.5.5 group ibgp
[prov_pe2-bgp] peer 5.5.5.5 connect-interface LoopBack0
[prov_pe2-bgp] ipv4-family vpnv4
[prov_pe2-bgp-af-vpn] peer ibgp enable
[prov_pe2-bgp-af-vpn] peer ibgp next-hop-local
[prov_pe2-bgp-af-vpn] peer 5.5.5.5 group ibgp
[prov_pe2-bgp-af-vpn] quit
[prov_pe2-bgp] quit
```

- 2 Create a VPN instance on provider PEs to access customer PEs and directly connected user CEs.

Configure prov_pe1.

```

[prov_pe1] ip vpn-instance customer_vpn
[prov_pe1-vpn-instance] route-distinguisher 3:3
[prov_pe1-vpn-instance] vpn-target 3:3 export-community
[prov_pe1-vpn-instance] quit
[prov_pe1] ip vpn-instance vpn1
[prov_pe1-vpn-instance] route-distinguisher 1:1
[prov_pe1-vpn-instance] vpn-target 1:1
[prov_pe1-vpn-instance] vpn-target 3:3
[prov_pe1-vpn-instance] quit
[prov_pe1] vlan 310
[prov_pe1] interface vlan 310
[prov_pe1-Vlan-interface310] ip binding vpn-instance customer_vpn
[prov_pe1-Vlan-interface310] ip address 1.1.1.2 255.0.0.0
[prov_pe1- Vlan-interface310] mpls
[prov_pe1- Vlan-interface310] quit
[prov_pe1] interface vlan 210
[prov_pe1-Vlan-interface210] ip binding vpn-instance vpn1
[prov_pe1- Vlan-interface210] ip address 18.1.1.1 255.0.0.0
[prov_pe1- Vlan-interface210] quit

```

Configure prov_pe2.

```

[prov_pe2] ip vpn-instance customer_vpn
[prov_pe2-vpn-instance] route-distinguisher 3:3
[prov_pe2-vpn-instance] vpn-target 3:3
[prov_pe2-vpn-instance] quit
[prov_pe2] interface vlan 410
[prov_pe2-Vlan-interface410] ip binding vpn-instance customer_vpn
[prov_pe2- Vlan-interface410] ip address 2.1.1.2 255.0.0.0
[prov_pe2- Vlan-interface410] mpls
[prov_pe2- Vlan-interface410] quit

```

Configure cust_pe1.

```

<SW8800> system-view
[SW8800] sysname cust_pe1
[cust_pe1] interface LoopBack0
[cust_pe1-LoopBack0] ip address 6.6.6.6 255.255.255.255
[cust_pe1-LoopBack0] quit
[cust_pe1] mpls lsr-id 6.6.6.6
[cust_pe1] interface vlan 310
[cust_pe1-Vlan-interface310] ip address 1.1.1.1 255.0.0.0
[cust_pe1- Vlan-interface310] mpls
[cust_pe1- Vlan-interface310] quit

```

Configure cust_pe2.

```

<SW8800> system-view
[SW8800] sysname cust_pe2
[cust_pe2] interface LoopBack0
[cust_pe2-LoopBack0] ip address 7.7.7.7 255.255.255.255
[cust_pe2-LoopBack0] quit
[cust_pe2] mpls lsr-id 7.7.7.7
[cust_pe2] interface vlan 410
[cust_pe2-Vlan-interface410] ip address 2.1.1.1 255.0.0.0

```

```
[cust_pe2-Vlan-interface410] mpls
[cust_pe2-Vlan-interface410] quit
```

3 Configure EBGP between provider PE and customer PE.

Configure prov_pe1 to access the corresponding Customer PE.

```
[prov_pe1] route-policy comm permit node 10
[prov_pe1-route-policy-comm-10] if-match vpn-target 1:1
[prov_pe1-route-policy-comm-10] quit
[prov_pe1] bgp 100
[prov_pe1-bgp] ipv4-family vpn-instance customer_vpn
[prov_pe1-bgp-af-vpn-instance] group ebgp external
[prov_pe1-bgp-af-vpn-instance] undo peer ebgp enable
[prov_pe1-bgp-af-vpn-instance] peer 1.1.1.1 group ebgp as-number 600
[prov_pe1-bgp] ipv4-family vpnv4
[prov_pe1-bgp-af-vpn] nesting-vpn
[prov_pe1-bgp-af-vpn] peer ebgp vpn-instance customer_vpn enable
[prov_pe1-bgp-af-vpn] peer 1.1.1.1 vpn-instance customer_vpn group ebgp
[prov_pe1-bgp-af-vpn] peer 1.1.1.1 vpn-instance customer_vpn route-policy
comm import
[prov_pe1-bgp-af-vpn] quit
```

Configure prov_pe1 to access CE5

```
[prov_pe1-bgp] ipv4-family vpn-instance vpn1
[prov_pe1-bgp-af-vpn-instance] group ebgp external
[prov_pe1-bgp-af-vpn-instance] peer 18.1.1.2 group ebgp as-number 50003
```

Configure prov_pe2 to access the corresponding Customer PE.

```
[prov_pe2] route-policy com2 permit node 10
[prov_pe2-route-policy-com2-10] if-match vpn-target 1:1
[prov_pe2-route-policy-com2-10] quit
[prov_pe2] bgp 100
[prov_pe2-bgp] ipv4-family vpn-instance customer_vpn
[prov_pe2-bgp-af-vpn-instance] group ebgp external
[prov_pe2-bgp-af-vpn-instance] undo peer ebgp enable
[prov_pe2-bgp-af-vpn-instance] peer 2.1.1.1 group ebgp as-number 500
[prov_pe2-bgp] ipv4-family vpnv4
[prov_pe2-bgp-af-vpn] nesting-vpn
[prov_pe2-bgp-af-vpn] peer ebgp vpn-instance customer_vpn enable
[prov_pe2-bgp-af-vpn] peer 2.1.1.1 vpn-instance customer_vpn group ebgp
[prov_pe2-bgp-af-vpn] peer 2.1.1.1 vpn-instance customer_vpn route-policy
com2 import
```

Configure cust_pe1

```
[cust_pe1] bgp 600
[cust_pe1-bgp] group ebgp external
[cust_pe1-bgp] undo peer ebgp enable
[cust_pe1-bgp] peer 1.1.1.2 group ebgp as-number 100
[cust_pe1-bgp] ipv4-family vpnv4
[cust_pe1-bgp-af-vpn] peer ebgp enable
[cust_pe1-bgp-af-vpn] peer 1.1.1.2 group ebgp
```

Configure cust_pe2

```
[cust_pe2] bgp 500
[cust_pe2-bgp] group ebgp external
[cust_pe2-bgp] undo peer ebgp enable
[cust_pe2-bgp] peer 2.1.1.2 group ebgp as-number 100
```



```
[cust_pe2-bgp] ipv4-family vpnv4
[cust_pe2-bgp-af-vpn] peer ebgp enable
[cust_pe2-bgp-af-vpn] peer 2.1.1.2 group ebgp
```

- 4 On each Customer PE, configure the sub-VPN that accesses the network through the Customer PE.

Configure cust_pe1.

```
[cust_pe1] ip vpn-instance vpn1
[cust_pe1-vpn-instance] route-distinguisher 1:1
[cust_pe1-vpn-instance] vpn-target 1:1
[cust_pe1-vpn-instance] quit
[cust_pe1] interface vlan 510
[cust_pe1-Vlan-interface510] ip binding vpn-instance vpn1
[cust_pe1-Vlan-interface510] ip address 15.1.1.2 255.0.0.0
[cust_pe1-Vlan-interface510] quit
[cust_pe1] bgp 600
[cust_pe1-bgp] undo peer ebgp enable
[cust_pe1-bgp] ipv4-family vpn-instance vpn1
[cust_pe1-bgp-af-vpn-instance] group cegroup external
[cust_pe1-bgp-af-vpn-instance] peer 15.1.1.1 group cegroup as-number 50001
[cust_pe1-bgp-af-vpn-instance] quit
[cust_pe1-bgp] quit
```

Configure cust_pe2

```
[cust_pe2] ip vpn-instance vpn1
[cust_pe2-vpn-instance] route-distinguisher 1:1
[cust_pe2-vpn-instance] vpn-target 1:1
[cust_pe2] interface vlan 610
[cust_pe2-Vlan-interface610] ip binding vpn-instance vpn1
[cust_pe2-Vlan-interface610] ip address 16.1.1.2 255.0.0.0
[cust_pe2-Vlan-interface510] quit
[cust_pe2] bgp 500
[cust_pe2-bgp] undo peer ebgp enable
[cust_pe2-bgp] ipv4-family vpn-instance vpn1
[cust_pe2-bgp-af-vpn-instance] group cegroup external
[cust_pe2-bgp-af-vpn-instance] peer 16.1.1.1 group cegroup as-number 50002
[cust_pe2-bgp-af-vpn-instance] quit
[cust_pe2-bgp] quit
```

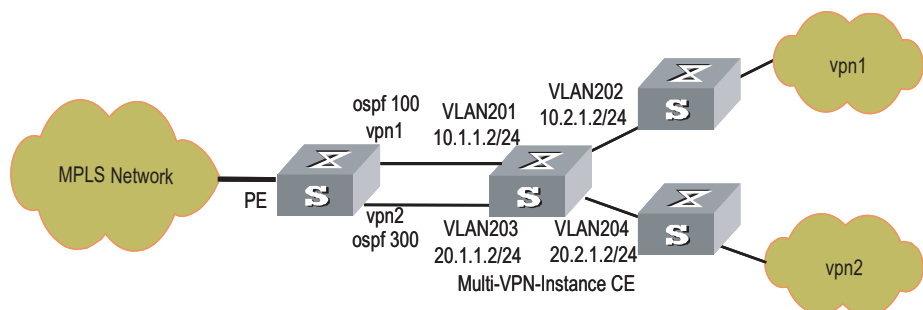
OSPF Multi-instance CE Configuration Example

Network requirements

CE router in a VPN achieves service isolation by configuring multiple VPN instances.

Network diagram

Figure 143 Network diagram for OSPF multi-instance CE configuration



Configuration procedure**1** Configuring CE router

Configure instance VPN1

```
[CE] ip vpn-instance vpn1
[CE-vpn-vpn1] route-distinguisher 100:1
[CE-vpn-vpn1] vpn-target 100:1 export-extcommunity
[CE-vpn-vpn1] vpn-target 100:1 import-extcommunity
```

Configure instance VPN2

```
[CE] ip vpn-instance vpn2
[CE-vpn-vpn2] route-distinguisher 200:1
[CE-vpn-vpn2] vpn-target 200:1 export-extcommunity
[CE-vpn-vpn2] vpn-target 200:1 import-extcommunity
```

Configure VLAN201.

```
[CE] vlan 201
[CE-vlan201] port gigabitethernet 2/1/1
[CE-vlan201] quit
[CE] interface Vlan-interface 201
[CE-Vlan-interface201] ip binding vpn-instance vpn1
[CE-Vlan-interface201] ip address 10.1.1.2 255.255.255.0
```

Configure VLAN202.

```
[CE] vlan 202
[CE-vlan202] port gigabitethernet 2/1/2
[CE-vlan202] quit
[CE] interface Vlan-interface 202
[CE-Vlan-interface202] ip binding vpn-instance vpn1
[CE-Vlan-interface202] ip address 10.2.1.2 255.255.255.0
[CE-Vlan-interface202] ospf cost 100
```

Configure VLAN203.

```
[CE] vlan 203
[CE-vlan203] port gigabitethernet 2/1/3
[CE-vlan203] quit
[CE] interface Vlan-interface 203
[CE-Vlan-interface203] ip binding vpn-instance vpn2
[CE-Vlan-interface203] ip address 20.1.1.2 255.255.255.0
```

Configure VLAN204.

```
[CE] vlan 204
[CE-vlan204] port gigabitethernet 2/1/4
[CE-vlan204] quit
[CE] interface Vlan-interface 204
[CE-Vlan-interface204] ip binding vpn-instance vpn2
[CE-Vlan-interface204] ip address 20.2.1.2 255.255.255.0
```

Configure ospf 100.

```
[CE] ospf 100 vpn-instance vpn1
[CE-ospf-100] vpn-instance-capability simple
[CE-ospf-100] area 0.0.0.0
[CE-ospf-100-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[CE-ospf-100-area-0.0.0.0] network 10.2.1.0 0.0.0.255

# Configure OSPF 300.

[CE] ospf 300 vpn-instance vpn2
[CE-ospf-300] vpn-instance-capability simple
[CE-ospf-300] area 0.0.0.1
[CE-ospf-300-area-0.0.0.1] network 20.1.1.0 0.0.0.255
[CE-ospf-300-area-0.0.0.1] network 20.2.1.0 0.0.0.255
```

Multi-Role Host Configuration Example

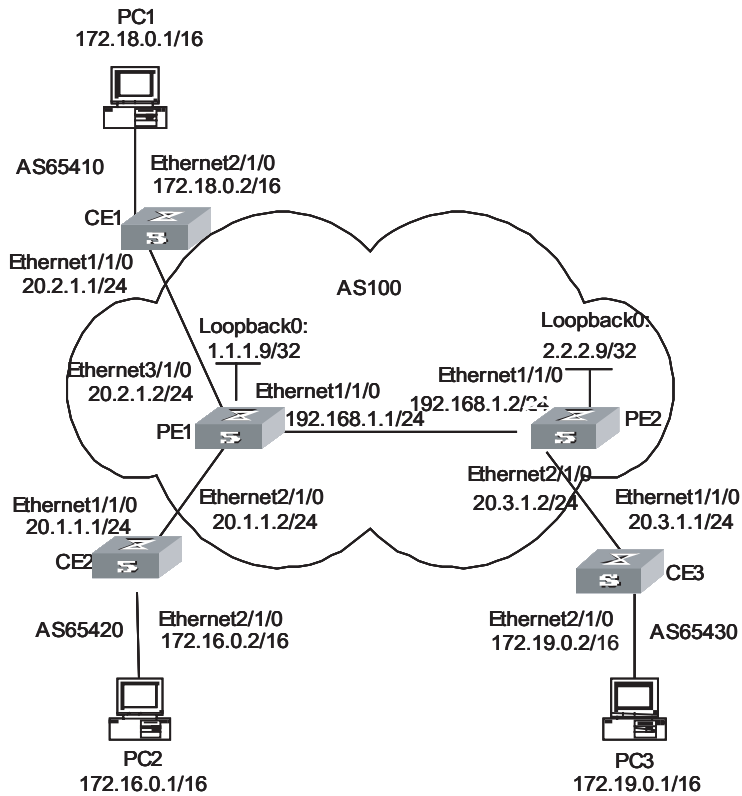
Network requirements

CE1 and CE3 belong to VPN1, and CE2 belong to VPN2.

The host PC2 with the IP address of 172.16.0.1 accesses the network through CE2. As a multi-role host, it can access both VPN1 and VPN2.

Network diagram

Figure 144 Network diagram for multi-role host application



Configuration procedure

- 1 Configure OSPF as the IGP protocol on the MPLS backbone network.

Configure OSPF on PE1:

```

[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] vlan 110
[PE1-vlan110] interface vlan-interface 110
[PE1-Vlan-interface110] ip address 192.168.1.1 24
[PE1-Vlan-interface110] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit

```

Configure OSPF on PE2:

```

[PE2] interface loopback 0
[PE2-LoopBack0] ip address 2.2.2.9 32
[PE2-LoopBack0] quit
[PE2] vlan 110
[PE2-vlan110] interface vlan-interface 110
[PE1-Vlan-interface110] ip address 192.168.1.2 24
[PE2-Vlan-interface110] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit

```

2 Configure basic MPLS capability and create VPN instances.

Configure basic MPLS capability on PE1:

```

[PE1] mpls lsr-id 1.1.1.9
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] vlan 110
[PE1-vlan110] interface vlan-interface 110
[PE1-Vlan-interface110] mpls
[PE1-Vlan-interface110] mpls ldp
[PE1-Vlan-interface110] quit

```

Create VPN instances for VPN1 and VPN2 on PE1, bind the address of the interface of VLAN310 to VPN1 and VPN2.

```

[PE1] ip vpn-instance vpn1
[PE1-vpn-vpn1] route-distinguisher 100:1
[PE1-vpn-vpn1] vpn-target 100:1 both
[PE1-vpn-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-vpn2] route-distinguisher 100:2
[PE1-vpn-vpn2] vpn-target 100:2 both
[PE1-vpn-vpn2] quit
[PE1] vlan 310
[PE1-vlan310] interface vlan-interface 310

```

```
[PE1-Vlan-interface310] ip binding vpn-instance vpn1
[PE1-Vlan-interface310] ip address 20.2.1.2 24
[PE1-Vlan-interface310] quit
[PE1] vlan 210
[PE1-vlan210] interface vlan-interface 210
[PE1-Vlan-interface210] ip binding vpn-instance vpn2
[PE1-Vlan-interface210] ip address 20.1.1.2 24
[PE1-Vlan-interface210] quit
```

Configure basic MPLS capability on PE2.

```
[PE2] mpls lsr-id 2.2.2.9
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] vlan 110
[PE2-vlan110] interface vlan-interface 110
[PE2-Vlan-interface110] mpls
[PE2-Vlan-interface110] mpls ldp
[PE2-Vlan-interface110] quit
```

Create a VPN instance for VPN1 on PE2, and bind the address of the interface of VLAN210 to VPN1.

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-vpn1] route-distinguisher 300:1
[PE2-vpn-vpn1] vpn-target 100:1 both
[PE2-vpn-vpn1] quit
[PE2] vlan 210
[PE2-vlan210] interface vlan-interface 210
[PE2-Vlan-interface210] ip binding vpn-instance vpn1
[PE2-Vlan-interface210] ip address 20.3.1.2 24
[PE2-Vlan-interface210] quit
```

Configure BGP.

Configure CE1:

```
[CE1] vlan 310
[CE1-vlan310] interface vlan-interface 310
[CE1-Vlan-interface310] ip address 20.2.1.1 24
[CE1-Vlan-interface310] quit
[CE1] bgp 65410
[CE1-bgp] import-route direct
[CE1-bgp] group 10 external
[CE1-bgp] peer 20.2.1.2 group 10 as-number 100
[CE1-bgp] quit
```

Configure CE2:

```
[CE2] vlan 210
[CE2-vlan210] interface vlan-interface 210
[CE2-Vlan-interface210] ip address 20.1.1.1 24
[CE2-Vlan-interface210] quit
```

Configure CE3:

```
[CE3] vlan 210
[CE3-vlan210] interface vlan-interface 210
[CE3-Vlan-interface210] ip address 20.3.1.1 24
[CE3-Vlan-interface210] quit
[CE3] bgp 65430
[CE3-bgp] import-route direct
[CE3-bgp] group 10 external
[CE3-bgp] peer 20.3.1.2 group 10 as-number 100
[CE3-bgp] quit
```

Configure PE1: Configure PE1 to be the IBGP peer of PE2 in BGP-VPNv4 sub-address family view. Configure PE1 to be the EBGP peer of CE1 in the BGP VPN1 instance view. Configure a static route between CE2 and PE1 to enable them to communicate with each other. Import a static route in BGP VPN2 instance view to advertise it to the remote PE.

```
[PE1] bgp 100
[PE1-bgp] group 10
[PE1-bgp] peer 2.2.2.9 group 10
[PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 10 enable
[PE1-bgp-af-vpn] peer 2.2.2.9 group 10
[PE1-bgp-af-vpn] quit
[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] group 20 external
[PE1-bgp-af-vpn-instance] peer 20.2.1.1 group 20 as-number 65410
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] ipv4-family vpn-instance vpn2
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] import-route static
```

Configure PE2: set up IBGP peer relation with PE1 in BGP-VPNv4 sub-address family view; set up EBGP peer relation with CE3 in BGP-VPN instance view.

```
[PE2] bgp 100
[PE2-bgp] group 10
[PE2-bgp] peer 1.1.1.9 group 10
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer 10 enable
[PE2-bgp-af-vpn] peer 1.1.1.9 group 10
[PE2-bgp-af-vpn] quit
[PE2-bgp] ipv4-family vpn-instance vpn1
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] group 20 external
[PE2-bgp-af-vpn-instance] peer 20.3.1.1 group 20 as-number 65430
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] quit
```

Configure multi-role host feature: If a routing protocol is employed between CE2 and PE1, configure PE1 not to advertise any route information to CE2 to avoid route loops. Following depicts a way to achieve this. You can also avoid route loops in other ways. Directly configure a static route to PC2 on PE1 if no routing protocol is employed between PE1 and CE2.

Configure a default route pointing to PE1 on CE2.

```
[CE2] ip route-static 0.0.0.0 0.0.0.0 20.1.1.2
```

Configure a multiple-role host route on PE1.

```
[PE1] ip route-static vpn-instance vpn1 172.16.0.0 16 vpn2 20.1.1.1
```

Import the route of VPN1 to VPN2 using the RT attribute.

```
[PE1] ip vpn-instance vpn2
[PE1-vpn-vpn2] vpn-target 100:1 import-extcommunity
```

Troubleshooting BGP/MPLS VPN Configuration

Symptom 1

In central server topology networking mode, the local end switch (spoke PE) cannot learn the routing information of the peer end switch (spoke PE).

Solution:

- Check whether the BGP adjacent of spoke PE and hub PE is created correctly.
- Check whether the routing attributes import/export relation of each VPN-instance is correct.
- Check from the hub PE that whether the routing information between two VPN instances can be learnt by each other. if not, perform the following operation: check if the EBGP protocol runs between hub PE and hub CE, check whether the **peer peer-address allow-as-loop** command is configured between PE and CE.

Symptom 2

PE at the local end can learn private network route of the PE at peer end, but two PEs cannot intercommunicate with each other.

Solution:

- Check whether the loopback interface configured on the PE has the address with 32-bit mask.
- Check whether the tag of private network route is correct.
- Check whether the LDP session is established using the **display mpls ldp session** command.
- Check whether the LSP tunnel is established using the **display mpls lsp** command.

Symptom 3

In Hub&Spoke networking mode, spoke PE cannot learn the private networking route of Hub PE.

Solution:

- Check whether the LSP tunnel is established using the **display mpls lsp** command.

- Check whether the BGP adjacent is established correctly.
- Check whether the routing import/export relation of the VPN-instance is correct.
- Check whether allow-as-loop is configured between spoke PE and hub PE.

Symptom 4

Fall to specify the Loopback interface at the peer end as the BGP neighbor.

Solution:

- Check whether the local routing table has learnt the Loopback interface routing information of the peer end using the **display ip routing-table** command.
- Check whether the address of the Loopback interface at the peer end can be pinged using the **ping** command.
- Check whether the configuration information is correct using the **display current-configuration bgp** command; confirm that you have specified the local loopback interface as the interface to create adjacent interface with the peer end by using the **peer peer-address connect-interface** command; confirm that you have activate the neighbor in VPNv4 sub-address family view.
- Check whether the BGP information is correct on the PE at the peer end; check whether specified the local Loopback interface as the interface to create adjacent with the peer end; and check whether you have configured VPN capacity.

Symptom 5

During ASBR configuration, VPN route interior label does not switch on the ASBR.

Solution:

- Check whether the VPN neighbor is created correctly using the **display bgp vpnv4 all peer** command.
- Check whether ASBR is configured with the **undo policy vpn-target** command. If not, configure this command.

Overview

Introduction to Card Intermixing

The intermixing feature is used to enable deployment of MPLS VPN services on cards that do not support MPLS. Switch 8800 Family routing switches support various modes of MPLS VPN function and provide abundant and differentiated MPLS VPN service to meet the differentiated needs of different users in the performance, reliability, port utilization of MPLS VPN functions.



- Unless otherwise specified, MPLS VPN services are processed by the MPLS-supporting interface cards. In this manual, an interface card that supports MPLS function is called MPLS card for short, and an interface card that does not support MPLS function is called non-MPLS card for short.
- The purpose of card intermixing is to enable the non-MPLS cards to support MPLS function through the MPLS cards. Refer to the "VPN" section in this manual for the information on the processing of MPLS VPN through VPLS Application Modules.
- Card intermixing does not support using XP4B and other interface cards on which ACL redirection is configured under the port group as non-MPLS card for intermixing.

Card Intermixing Mechanism

The implementation mechanism for card intermixing is as follows:

- The MPLS card and the non-MPLS card co-exist in the same switch;
- Use the port of the non-MPLS card for the access to the service private network side of the MPLS VPN ;
- Redirect the port of the non-MPLS card through QACL, to redirect the received packets to the specified MPLS card for processing;
- The port of MPLS card is set as Loopback port automatically and the port type is Trunk;
- The access port of the non-MPLS card and the Loopback port of the MPLS card belong to the same VLAN.

The port on the MPLS card can also be used for the access to the service private network side of the MPLS VPN. In this case, you do not need to configure card intermixing, and you must use the port of the MPLS card for the connection with the MPLS public network side.



Because the destination port in intermixing configuration is to be looped back and therefore is locked automatically, you cannot enter the port view. Therefore, you cannot perform other configurations on the destination port.

Restrictions in Intermixing Networking

Rules of Intermixing Configuration

- A non-MPLS card can be used for access to the private network side, and an MPLS card must be used for access to the public network side;
- You cannot perform other configurations on the destination port in intermixed networking, that is to say, the port view is unavailable. In addition, the destination port in intermixing networking cannot be deleted from the VLAN in the normal way, and the destination port is an inloop port;
- The configured connection status of the source port in intermixing networking is protected. For example, the port type cannot be changed from Trunk to Access or from Access to Trunk, and the source port cannot be deleted from VLAN in the normal way;
- The configuration of the service ports in intermixing networking cannot be changed, and the service ports can be reconfigured only after the intermixing configuration is removed;
- In a VLAN, multiple ports of the non-MPLS card can be redirected to one port of the MPLS card. The destination port of the MPLS card is Looped back automatically (becomes a Loopback port) after it is configured for redirection, and you cannot perform other configurations on the port. Therefore, make sure that the destination port is not in manual Shutdown state before configuring redirection. Only one Loopback port is allowed in the redirected VLAN that the destination port belongs to, but other MPLS card ports are allowed to join in;
- On the Trunk port of a non-MPLS card, you can redirect the MPLS VPNs of multiple VLANs to one destination port to meet the need when the access CE is a Layer 2 switch;
- In non-intermixing networking, VLL application requires that VLANs with only one port be used at the private network side; In intermixing networking, VLL supports only VLANs with two ports: one is the source port (port of the non-MPLS card) and the other is the destination port (port of the MPLS card);
- When the source port (Trunk port) in intermixing networking belongs to multiple VLANs, VPN binding must be implemented on the VLAN interfaces after the redirection configuration;
- If VRRP is configured on the VLAN interface to which the redirected source port of the MPLS VPN belongs, the plugging/unplugging of the MPLS card will cause VRRP group state switching on the VLAN interface.

Restrictions in Card Intermixing

- Source port aggregation and destination port aggregation are not supported;
- Nested VPN is not supported;
- Super VLAN is not supported;
- It is not allowed to change the attributes of the redirected source port;

- It is not allowed to make the redirected source port or destination port to leave redirected VLAN in the normal way;
- It is not allowed to configure protocol VLANs on the redirected source port or destination port;
- It is not allowed to delete the redirected VLAN or VLAN interface;
- It is not allowed to configure/add Loopback ports in the redirected VLAN;
- It is not allowed to use STP edge port as the redirected destination port;
- It is not allowed to change the VLANs and the default VLAN ID which the redirected destination port is permitted to pass;
- If normal ports are used, 4,094 VLL VPNs are supported; if the Trunk port of the card of a fast Ethernet card is used, a maximum of 1024 VLL VPNs are supported;

A Trunk-type 100M Ethernet port can use only 1024 VLANs for VPN access or MPLS forwarding, but you can specify the start VLAN ID of the 100M Ethernet Trunk port. Assume the start VLAN ID is VLAN ID, the range of VLAN IDs of the VLANs that pass a certain 100M Ethernet port is from VLAN ID to VLAN ID + 1023.

Intermixing Configuration Task

Introduction to intermixing configuration task

Table 559 Introduction to intermixing configuration task

Operation	Description	Related section
Configure public network routing protocols	Required	Section "Configuring Routing Protocols" "Configuring Routing Protocols"
Configure the basic capability of MPLS	Required	"MPLS Basic Capability Configuration"
Configure MPLS VPN	Required	"BGP/MPLS VPN Configuration"
Configure flow template and ACL rules	Required	Section "Configuring flow template and ACL rules" "Configuring flow template and ACL rules"
Apply flow template on the port and configure redirection	Required	Section "Applying Flow Template and Redirection in Port Mode" "Applying Flow Template and Redirection in Port Mode"

Configuring Routing Protocols

The Switch should be configured with some basic routing configurations so that it can exchange public network routing information with other P devices and PE devices. The routing protocols available currently include: static routing, RIP, OSPF, BGP and so on. Refer to the "Routing Protocols" part of the *3Com Switch 8800 Family Routing Switches Operation Manual Volume I* for detailed configuration information.

Configuring Basic Capability of MPLS

Configure MPLS basic capability to enable MPLS and LDP globally and on the public network interface, to establish an LSP tunnel for the public network. Refer to "MPLS Basic Capability Configuration" for detailed configuration information.

Configuring MPLS VPN Configure BGP/MPLS VPN (L3VPN) or L2VPN. Refer to “BGP/MPLS VPN Configuration” and the “VPN Operation” section in *3Com Switch 8800 Family Series Routing Switches Operation Manual*. for detailed configuration information.

Configuring flow template and ACL rules The packets to be redirected are identified through the flow template and ACL configurations.

For L2VPN

Table 560 Configure the flow template and ACL of L2VPN

Operation	Command	Description
Enter system view	system-view	-
Enter corresponding ACL view	acl { number <i>acl-number</i> name <i>acl-name</i> link } [match-order { config auto }]	Required. Required. L2VPN can use either the default flow template or a custom flow template. It is recommended to redirect the packets in the specified VLAN through matching them with a Layer 2 rule so that the specified VLAN packets can pass.
Configure rules of ACL	rule [<i>rule-id</i>] permit ingress <i>vlan-id</i>	

For L3VPN

Table 561 Configure flow template and ACL rules of L3VPN

Operation	Command	Description
Enter system view	system-view	- Require.
Set self-defined flow template	flow-template user-defined slot <i>slotid</i> dmac <i>wildcard</i> sip <i>wildcard</i> vlanid	When a custom flow template is specified, at least two items IP and DMAC are required. You can use the IP + VLAN + DMAC method to define the flow template so that different kinds of packets are processed in different ways.
Enter corresponding ACL view	acl { number <i>acl-number</i> name <i>acl-name</i> [advanced basic] } [match-order { config auto }]	Required. Required.
Configure IP ACL	rule [<i>rule-id</i>] permit source { <i>source-addr wildcard</i> any }	You can use the parameter permit any or specify an IP address. Required.
Configure Layer 2 ACL	rule [<i>rule-id</i>] permit ingress <i>vlan-id</i> egress <i>dest-mac-addr dest-mac-wildcard</i>	Use a Layer 2 rule to configure VLAN+DMAC. DMAC refers to the virtual MAC of the switch. You can get it through the display interface vlan <i>vlanid</i> command.

You can define the flow template by means of the IP + VLAN + DMAC method to make sure that different kinds of packets are processed in different ways:

- If ARP packets do not match IP rules in redirection, they will be processed on the non-MPLS card;
- If Layer 2 traffic does not match DMAC in redirection, it will be L2-forwarded on the non-MPLS card;
- If Layer 3 packets (including unicast protocol packets) match the rule, they will be redirected to the MPLS card.

Refer to section "QACL" and the following networking example in the manual for detailed information on configuring flow template and ACL rules.

Applying Flow Template and Redirection in Port Mode

Table 562 Applying Flow Template and Redirect in Port Mode

Operation	Command	Description
Enter system view	system-view	-
Enter port view	interface <i>interface-type</i> <i>interface-number</i>	-
Apply flow template in port mode	flow-template user-defined	Required
Configure the traffic-redirect command	traffic-redirect inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] link-group [rule <i>rule</i>] interface <i>interface-type</i> <i>interface-number</i> <i>destination-vlan</i> { I2-vpn I3-vpn } slot <i>slotid</i> <i>vlanid</i> [Join-vlan] }	Required I3-vpn I2-vpn means the command is applicable to L2VPN or L3VPN of MPLS. slot <i>slotid</i> <i>vlanid</i> : the slot id of the service card which the VPLS packets are redirected to and the ID of the VLAN to join in.

The **traffic-redirect** command is used to enable ACL flow classification and redirect the packets (only applicable to the rules whose action is **permit** in the ACL). There are two kinds of redirection commands:

- Redirect packets to a port: You can redirect packets received by the source port of the non-MPLS card to the specified destination port of the MPLS card.
- Redirect packets to an application module: You can redirect packets received by the source port of the non-MPLS card or MPLS card to the VPLS card.

There are two kinds of redirection services:

- VPLS-related redirection services: The key word **join-vlan** must be specified, and the system will add the current port into *destination-vlan* after the redirection enabled; when redirection is disabled, the system will log the current port out of the VLAN if what is deleted is a **join-vlan** enabled redirection in the VLAN.
- MPLS-independent redirection services: Such redirection services include URPT, reflexive ACL, BT traffic control and so on. **join-vlan** cannot be enabled in such a service. The port will not be added into VLAN when redirection is configured, and the port will not be removed from the VLAN when redirection is deleted.



- The source port joins in the corresponding VLAN automatically after the configuration of intermixing redirection, and the source port leaves the corresponding VLAN automatically after the intermixing redirection is deleted.
- When using the VPLS intermixing redirection command, you have to enable **join-vlan** explicitly.
- When using the VLL VPN intermixing redirection command, you must not enable the QinQ function on the source port and destination port.

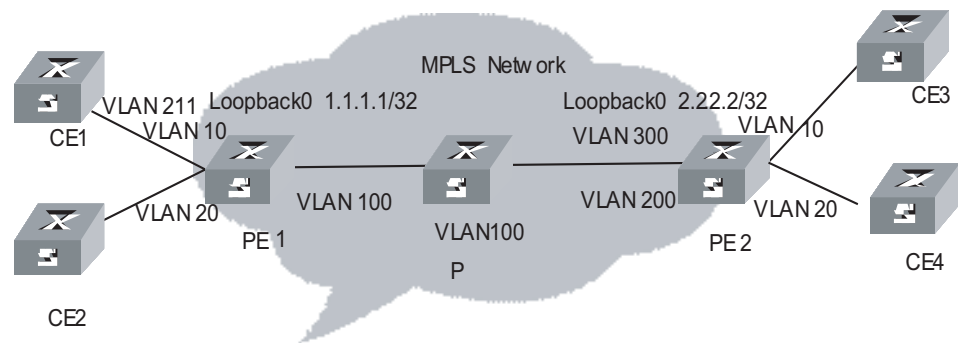
Typical Networking Example

Network requirements

- CE1 and CE3 constitute VPN A, and CE2 and CE4 constitute VPN B. In PE1, a port of an interface card is shared, and in PE2, a Layer 2 switch is shared to connect with the host directly.
- The PE devices (PE1 and PE2) are Switch 8800 Family series switches, and the PE devices need to support the MPLS function. CE1 and CE2 are common mid-range and low-end routers. CE3 and CE4 are Layer 2 switches connected with users directly.
- The configurations of the interface cards of the two PE devices are the same. On slot3 is a non-MPLS card with 100M Ethernet ports, and on Slot 2 is an MPLS card with Gigabit Ethernet ports.

Networking diagram

Figure 145 Network diagram for BGP/MPLS VPN intermixing



Configuration procedure

1 Configure CE1

Configure CE1 and CE2 as EBGp neighbors and import direct routes and static routes So that the VPN user routes of CE1 are imported into BGP routes and then advertised to PE1.

```
<CE1>system-view
[CE1] vlan 211
[CE1] interface vlan-interface 211
[CE1-vlan-interface211] ip address 10.10.10.10 255.255.255.0
[CE1-vlan-interface211] quit
[CE1] bgp 65410
[CE1-bgp] group vpna external
[CE1-bgp] peer 10.10.10.1 group vpna as-number 100
```

```
[CE1-bgp] import-route direct
[CE1-bgp] import-route static
```



The configuration on CE2 is similar to that on CE1, so the configuration procedure is omitted.

2 Configure PE1

Configure global MPLS.

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

Configure public network interface and enable MPLS on the interface.

```
[PE1] interface loopback0
[PE1-LoopBack0] ip address 1.1.1.1 32
[PE1-LoopBack0] quit
[PE1] vlan 100
[PE1-vlan100] port GigabitEthernet 2/2/1
[PE1-vlan100] interface vlan-interface 100
[PE1-vlan-interface100] ip address 196.168.1.1 255.255.255.0
[PE1-vlan-interface100] mpls
[PE1-vlan-interface100] mpls ldp enable
[PE1-vlan-interface100] quit
```

Enable OSPF on the interface connecting PE1 and P router and the Loopback interface.

```
[PE1] ospf 1 route-id 1.1.1.1
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 196.168.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
```

Configure VPN-instance. The configuration of VPN B is similar to that of VPN A, so followed is only the configuration of VPN A.

```
<PE1> system-view
[PE1] ip vpn-instance vpna
[PE1-vpn-vpna] route-distinguisher 100:1
[PE1-vpn-vpna] vpn-target 100:1 both
[PE1-vpn-vpna] quit
```

Configure ACL and redirection, and configure a basic IP ACL to permit all the IP packets in CE devices to be redirected.

```
[PE1] flow-template user-defined slot 3 dmac 0000-0000-0000 sip 0.0.0.0
vlan-id
[PE1] acl number 2000
[PE1-acl-basic-2000] rule 0 permit source any
[PE1-acl-basic-2000] quit
[PE1] acl number 4000
[PE1-acl-link-4000] rule 0 permit ingress 10 egress 00e0-fc99-6738
0000-0000-0000
[PE1-acl-link-4000] quit
```



CAUTION: *If the VRRP protocol is enabled on the VLAN port to which the source port of MPLS VPN redirection belongs, you must configure another ACL rule to redirect the packets whose destination address is the virtual MAC address of VRRP, so that ICMP packets whose destination address is the virtual MAC address of VRRP can be processed normally.*

Configure VLAN interface.

```
[PE1] vlan 10
[PE1-vlan10] interface vlan-interface 10
[PE1-vlan-interface10] quit
```

Configure redirection on ports.

```
[PE1] interface Ethernet 3/1/1
[PE1-Ethernet3/1/1] flow-template user-defined
[PE1-Ethernet3/1/1] traffic-redirect inbound ip-group 2000 rule 0 link-group
4000 rule 0 interface GigabitEthernet 2/1/1 10 l3-vpn
[PE1-Ethernet3/1/1] quit
```

Bind VPN A to the VLAN port connecting PE1 and CE1.

```
[PE1] interface vlan-interface 10
[PE1-vlan-interface10] ip binding vpn-instance vpna
[PE1-vlan-interface10] ip address 10.10.10.1 255.255.255.0
[PE1-vlan-interface10] quit
```

Establish EBGP neighbor relationship between PE1 and CE1 and import the interface routes of VPN-instance.

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] group vpna external
[PE1-bgp-af-vpn-instance] peer 10.10.10.10 group vpna as-number 65410
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] quit
```

Establish MBGP neighbor relationship between PE and PE to exchange the VPN routing information between the PEs and activate IBGP peers in VPNv4 address family view.

```
[PE1] bgp 100
[PE1-bgp] group 100
[PE1-bgp] peer 2.2.2.2 group 100
[PE1-bgp] peer 2.2.2.2 connect-interface loopback0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 100 enable
[PE1-bgp-af-vpn] peer 2.2.2.2 group 100
```

3 Configure P

Configure global MPLS.

```
[P] mpls lsr-id 3.3.3.3
[P] mpls
[P] mpls ldp
```


Configure an interface and enable MPLS on the interface.

```
[P] interface loopback0
[P-LoopBack0] ip address 3.3.3.3 32
[P-LoopBack0] quit
[P] vlan 100
[P-vlan100] port GigabitEthernet 2/1/1
[P-vlan100] interface vlan-interface 100
[P-vlan-interface100] ip address 196.168.1.2 255.255.255.0
[P-vlan-interface100] mpls
[P-vlan-interface100] mpls ldp enable
[P-vlan-interface100] quit
[P] vlan 200
[P-vlan200] port GigabitEthernet 2/1/2
[P-vlan200] interface vlan-interface 200
[P-vlan-interface200] ip address 196.168.2.2 255.255.255.0
[P-vlan-interface200] mpls
[P-vlan-interface200] mpls ldp enable
[P-vlan-interface200] quit
```

Configure OSPF.

```
[P] ospf 1 route-id 3.3.3.3
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 196.168.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 196.168.2.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
```

4 Configure PE2

Configure global MPLS.

```
[PE2] mpls lsr-id 2.2.2.2
[PE2] mpls
[PE2] mpls ldp
```

Configure a public network interface and enable MPLS on the interface.

```
[PE2] interface loopback0
[PE2-LoopBack0] ip address 2.2.2.2 32
[PE2-LoopBack0] quit
[PE2] vlan 200
[PE2-vlan200] port GigabitEthernet 2/2/1
[PE2-vlan200] interface vlan-interface 200
[PE2-vlan-interface200] ip address 196.168.2.1 255.255.255.0
[PE2-vlan-interface200] mpls
[PE2-vlan-interface200] mpls ldp enable
[PE2-vlan-interface200] quit
```

Enable OSPF on the interface connecting PE2 with P router and the Loopback interface.

```
[PE2] ospf 1 route-id 2.2.2.2
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 196.168.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
```

Configure VPN-instance. The configuration of VPN B is similar to that of VPN A, so followed is only the configuration of VPN A.

```
[PE2] ip vpn-instance vpna
[PE2-vpn-vpna] route-distinguisher 100:1
[PE2-vpn-vpna] vpn-target 100:1 both
[PE2-vpn-vpna] quit
```

Configure ACL, redirection and Layer 2 ACL (Custom flow template should be configured before this step).

```
[PE2] acl number 2000
[PE2-acl-basic-2000] rule 0 permit source any
[PE2-acl-basic-2000] quit
[PE2] flow-template user-defined slot 3 dmac 0000-0000-0000 sip
0.0.0.0 vlan-id
[PE2] acl number 4000
[PE2-acl-link-4000] rule 0 permit ingress 10 egress 00e0-fc99-6738
0000-0000-0000
[PE2-acl-link-4000] quit
```

Configure VLAN interface.

```
[PE2] vlan 10
[PE2-vlan10] interface vlan-interface 10
[PE2-vlan-interface10] quit
```

Configure redirection on the port.

```
[PE2] interface Ethernet 3/1/1
[PE2-Ethernet3/1/1] port link-type trunk
[PE2-Ethernet3/1/1] flow-template user-defined
[PE2-Ethernet3/1/1] traffic-redirect inbound ip-group 2000 rule 0
link-group 4000 rule 0 interface GigabitEthernet 2/1/1 10 13-vpn
```

Bind VPN A on the VLAN interface between PE2 and CE3.

```
[PE2] interface vlan-interface 10
[PE2-vlan-interface10] ip binding vpn-instance vpna
[PE2-vlan-interface10] ip address 20.2.1.2 255.255.255.0
[PE2-vlan-interface10] quit
```

Import the interface routes of private network between PE2 and CE 3 for VPNA.

```
[PE2] bgp 200
[PE2-bgp] ipv4-family vpn-instance vpna
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] quit
```

Establish MBGP neighbor relationship between PE and PE to exchange VPN routing information between PEs and activate IBGP peers in VPNv4 address family view.

```
[PE2] bgp 100
[PE2-bgp] group 100
[PE2-bgp] peer 1.1.1.1 group 100
```

```
[PE2-bgp] peer 1.1.1.1 connect-interface loopback0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer 100 enable
[PE2-bgp-af-vpn] peer 1.1.1.1 group 100
```



The configuration of L2 VPN VLL intermixing is similar to that of L3VPN intermixing, so the description of configuration process is omitted. The configuration of L2 VPN VLL intermixing is also implemented through the **traffic-redirect** command. You do not need to customize the flow template needed for VLL redirection and you can use the default flow template. In addition, the flow template only needs to match Layer 2 ACL of 4000 series and only the VLAN ID needs to be specified in ACL rules.

Restrictions in Networking of Various MPLS Cards

Exclusively non-MPLS Cards

Introduction to networking

Non-MPLS cards do not support related MPLS functions.

Configuration restrictions

If related MPLS service is configured, the service cannot work normally.

Exclusively MPLS Cards

Introduction to networking

MPLS cards support MPLS VPN (VLL and BGP/MPLS VPN), and VLL and BGP/MPLS VPN can be configured on MPLS cards at the same time.

Configuration restrictions

- Not supporting VPLS;
- VLL and BGP/MPLS VPN cannot be configured on a VLAN interface at the same time.

Exclusively VPLS Service Cards

Introduction to networking

This networking mode does not exist. Other service cards are needed to forward data.

Configuration restrictions

None.

Combination of One MPLS Card and Multiple non-MPLS Cards

Introduction to networking

The deployment of MPLS VPN (VLL and BGP/MPLS VPN) services can be implemented on non-MPLS cards through card intermixing configuration.

Configuration restrictions

- VLL and BGP/MPLS VPN are mutually exclusive, so it is not allowed to configure the two types of services on the same VLAN interface;

- In card intermixing networking, non-MPLS cards can only be used for access at the private network side, and MPLS card must be used for access at the public network side.
- MPLS card has influence on the forwarding performance of a switch.

Combination of Multiple MPLS cards and Multiple non-MPLS Cards

Introduction to networking

The combination of multiple MPLS cards and multiple non-MPLS cards is similar to "Combination of one MPLS card and multiple non-MPLS cards" in Section 5.4.4; however, MPLS VPN services can be processed on the MPLS cards directly, without the need of card intermixing configuration.

Configuration restrictions

It is not allowed to bind VLL and BGP/MPLS VPN to the same VLAN.

Combination of One VPLS Card and Multiple non-MPLS Cards

Introduction to networking

A VPLS card supports VPLS. However, a VPLS card does not have egress interfaces, so another interface card must be used data forwarding.

Combination of One VPLS card and Multiple MPLS Cards

Introduction to networking

VPLS cards can work with any type of interface cards to support VPLS.

Combination of One VPLS card, One MPLS Card and Multiple non-MPLS Cards

Introduction to networking

Assume only non-MPLS cards were used at the beginning, and then one MPLS card was added to support MPLS VPN services (VLL and BGP/MPLS VPN) through card intermixing configuration. Then one VPLS card was added to process VPLS services.

Configuration restrictions

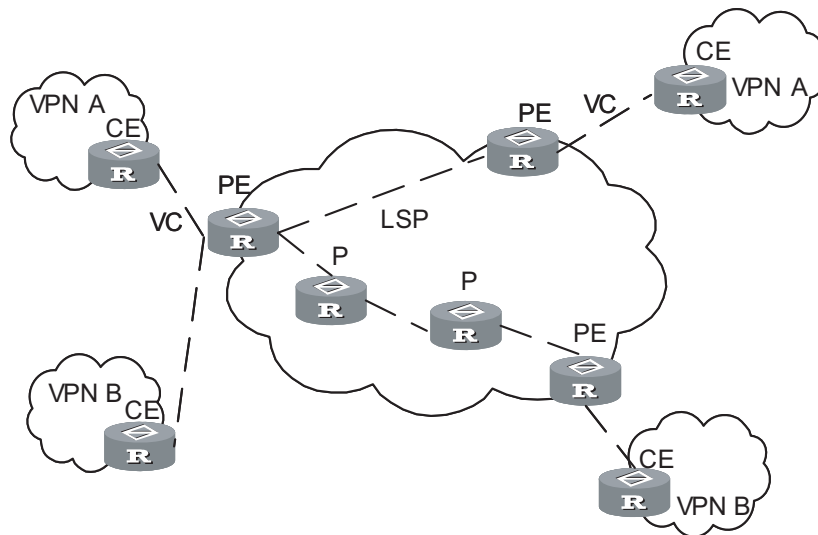
The MPLS card is used to process MPLS VPN services. It is recommended to use non-MPLS cards for the access of MPLS services at the private network side.

MPLS L2VPN Overview

Introduction to MPLS L2VPN

MPLS L2VPN provides MPLS network-based Layer 2 VPN services. For users, an MPLS L2VPN is a Layer 2 switched network, through which Layer 2 connections can be established between network nodes.

Figure 146 MPLS L2VPN

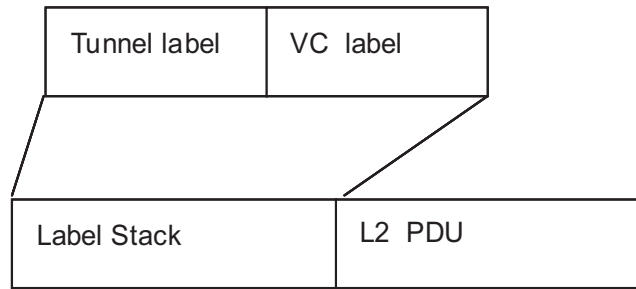


MPLS L2VPN has the following advantages:

- Multiple network layer protocols supported, such as IP, IPv6, IPX, and SNA.
- Powerful extensibility. MPLS L2VPN only establishes Layer 2 connections, rather than imports and manages the routing information. This eases work load of PE (provider edge) devices and the entire SP (service provider) network remarkably and thus enables SPs to provide more VPNs and accommodate more users.
- Reliability and privacy of user routes. As no user routing information is imported, there is no need for MPLS L2VPN to obtain and process the information, ensuring the privacy of user routes.

Figure 147 illustrates the structure of an MPLS L2VPN packet.

Figure 147 Structure of an MPLS L2VPN packet



The fields in an MPLS L2VPN packet are described as follows:

Tunnel label (the outer label) is an MPLS label or a GRE label. It is used to transmit a packet from one PE to another.

VC label (the inner label) is a lower layer label used to identify the links between PEs and CEs. Packets of MPLS L2VPNs implemented through circuit cross connect (CCC) do not contain this label.

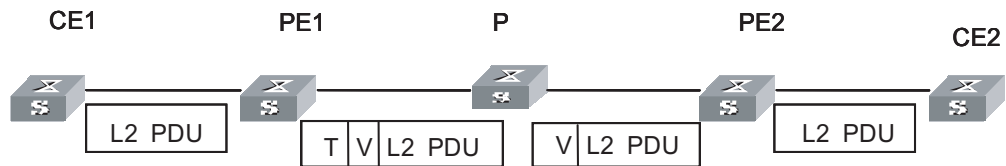
Data in MPLS L2VPN can be encapsulated as Ethernet or VLAN packets at the data link layer. At present, data of different nodes in a VPN must be encapsulated as the same type of packets.

Packet Forwarding

In an MPLS L2VPN, CE, PE, and P operate in the same way as those in a BGP/MPLS VPN. That is, they also forward packets in an MPLS network transparently by using label stacks. To forward packets in an MPLS L2VPN, tunnels must be established first between PEs (this can be achieved by either manual configuration or signaling protocols). When the interfaces connecting PEs and CEs are up, PEs insert VC labels for packets sent by CE, and then mark them with tunnel labels. On receiving these packets, the remote PEs strip off the tunnel labels and send the packets to the corresponding CEs according to their VC labels.

Table 565 illustrates changes of the label stack of a packet during the forwarding.

Figure 148 Label stack processing of MPLS L2VPN



L2 PDU: Data link layer packet

T: Tunnel label

V: VC label

Implementation

At present, the official standard for MPLS L2VPN has not been established yet. However, the PPVPN (Provider-provisioned Virtual Private Network) group of IETF (Internet Engineering Task Force) defines multiple framework drafts, two of which are commonly used. They are known as Martini draft and Kompella draft. Till May, 2005, they are depicted in the following documents respectively:

draft-martini-l2circuit-trans-mpls-09.txt

draft-kompella-ppvnp-l2vpn-02.txt

Martini draft defines the way to implement MPLS L2VPN by establishing point-to-point links. Here, LDP (Label Distribution Protocol) is used as the signaling protocol to exchange VC labels. This kind of MPLS L2VPNs is known as Martini MPLS L2VPNs.

Kompella draft defines how to establish MPLS L2VPNs in MPLS networks through end-to-end (CE-to-CE) connections. At present, BGP (border gateway protocol) is used as the signaling protocol to propagate the information about Layer 2 reachability and VC labels. This kind of MPLS L2VPNs is known as Kompella MPLS L2VPN.

Also, you can establish MPLS L2VPNs without signaling protocols. In this case, MPLS L2VPN services are provided through statically configured VC labels. An example of this is CCC, which implement MPLS L2VPNs through static configuration.

Table 563 describes the features and implementation ways of the above three types of MPLS L2VPNs.

Table 563 Features and implementation ways of the three types of MPLS L2VPNs

VPN type	Implementation	Feature
CCC	<p>Configures static LSPs to implement MPLS L2VPN.</p> <p>You must manually configure two LSPs (for sending and receiving packets respectively) for each CCC connection node by node (including PEs and Ps). The configured LSPs can only be used to transmit packets of the corresponding CCC connections.</p>	<p>Data is transmitted through packets with single-layer labels. LSPs are used exclusively.</p> <p>No signaling is needed to transmit the Layer 2 VPN information. Only MPLS forwarding is required. In this way, CEs of different SPs can be interconnected easily.</p>
Martini	<p>Uses extended LDP as the signaling to transmit the VC information.</p> <p>Uses VC-TYPE and VC-ID to identify VCs. VC-TYPE indicates the encapsulation type of data link layer, and VC-ID uniquely identifies a VC.</p> <p>PEs connecting CEs exchange VC labels through LDPs. They bind the corresponding CEs through VC-IDs.</p>	<p>Local switching like CCC is not available.</p> <p>An LSP can be shared by multiple VCs.</p>

Table 563 Features and implementation ways of the three types of MPLS L2VPNs

VPN type	Implementation	Feature
Kompella	Similar to Layer 3 BGP/MPLS VPN defined in RFC2547.	Users can assign extra labels to VPNs for future use. This eases the configuration work loads of VPN deployment and capacity expansion.
	PEs discover Layer 2 VPN nodes automatically through IBGP sessions established between them. They also propagate the VPN information.	VPN-target is used to identify VPNs. This brings great flexibility for VPN networking.
	Labels are distributed in the form of label blocks, which enables multiple connections being assigned tags simultaneously. The size of a tag block is determined by CE Range (user-configurable). VPN-target is used to differentiate VPNs.	Connections between CEs are not concerned. This type of MPLS L2VPN is implemented by dividing the entire SP network into different VPNs and numbering these CEs in the VPNs. To establish a connection between two CEs, you need to set the local CE ID and the remote CE ID on the PE, and specify the Circuit ID assigned for the connection by the local CE.



You also can configure LSPs without P devices.

CCC MPLS L2VPN Configuration

Configuring CCC MPLS L2VPN

Table 564 Configure CCC MPLS L2VPN

Operation	Command	Description
Enter system view	system-view	-
Configure LSR ID	mpls lsr-id X.X.X.X	Required
Enable MPLS	mpls	Required
Create the egress for the static LSP	static-lsp egress <i>lsp-name</i> l2vpn incoming-interface vlan-interface <i>vlan-id</i> in-label <i>in-label</i>	Required. Before configuring a CCC connection, you need to configure two static LSPs between the two PEs and all P routers in between for bidirectional packets. Refer to corresponding sections in the command manual for more information about these commands and corresponding undo commands.
Create the ingress for the static LSP	static-lsp ingress <i>lsp-name</i> l2vpn nexthop <i>next-hop-addr</i> out-label <i>out-label</i>	
Create the transit for the static LSP	static-lsp transit <i>lsp-name</i> l2vpn incoming-interface vlan-interface <i>vlan-id</i> in-label <i>in-label</i> { nexthop <i>next-hop-addr</i> } out-interface vlan-interface <i>vlan-id</i> } out-label <i>out-label</i>	
Quit MPLS view and enter system view	quit	-
Enable MPLS L2VPN	mpls l2vpn	Required

Table 564 Configure CCC MPLS L2VPN

Operation	Command	Description
Establish local CCC connection	ccc <i>ccc-connection-name</i> interface <i>vlan-interface</i> <i>vlan-id</i> out-interface	Required. Two types of CCC connections exist: local CCC connection and remote CCC connection. A local CCC connection is established between two local CEs. It can be switched directly by the PE without being configured a static LSP. A remote CCC connection is established between the local CE and a remote CE. The two CEs are attached to different PEs. In this case, you need to configure two static LSPs for bidirectional packets transmitted between the two PEs.
Establish remote CCC connection	ccc <i>ccc-connection-name</i> interface <i>vlan-interface</i> <i>vlan-id</i> transmit-lsp <i>transmit-lsp-name</i> receive-lsp <i>receive-lsp-name</i>	

**CAUTION:**

- In L2VPN, you can configure only one virtual circuit for each VLAN interface.
- L2VPN supports VLAN interfaces only. When you configure an L2VPN on a VLAN interface, data is encapsulated as Ethernet packets by default.
- You can configure only one VLAN on the access side of each VPN private network. Each VLAN can have only one interface, and all the VLANs connecting to the interface must have IGMP disabled.
- You must configure two static LSPs for each remote CCC connection. Two CCC connections cannot share one static LSP.
- A static LSP used by a remote CCC connection cannot be used for other purposes (such as carrying IP packets and BGP/MPLS VPN packets). When you configure a static LSP for a CCC connection, the next hop must be the IP address from which the ARP packets are learnt.

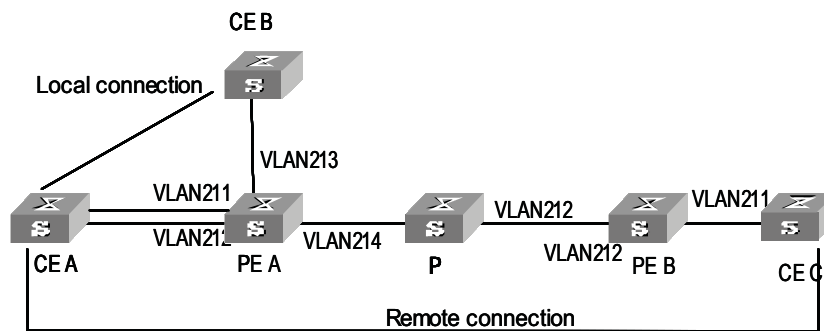
CCC MPLS L2VPN Configuration Example

Network requirements

CEs and the corresponding PEs shown in Figure 149 are interconnected through their GigabitEthernet ports. Data is encapsulated as Ethernet packets at the data link layer. A local connection is required between CE-A and CE-B, and a remote connection between CE-A and CE-C.

Network diagram

Figure 149 Network diagram for CCC MPLS L2VPN



Configuration procedure

- 1 Configure PE-A.

Enable MPLS globally.

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

Enable MPLS L2VPN globally.

```
[PE_A] mpls l2vpn
```

Configure VLAN 211.

```
[PE_A] vlan 211
[PE_A-vlan211] port gigabitethernet 2/1/1
[PE_A-Vlan211] interface vlan-interface 211
[PE_A-Vlan-interface211] quit
```

Configure VLAN 212.

```
[PE_A] vlan 212
[PE_A-vlan212] port gigabitethernet 2/1/2
[PE_A-vlan212] interface vlan-interface 212
[PE_A-Vlan-interface212] quit
```

Configure VLAN 213.

```
[PE_A] vlan 213
[PE_A-vlan213] port gigabitethernet 2/1/3
[PE_A-vlan213] interface vlan-interface 213
[PE_A-Vlan-interface213] quit
```

Enable MPLS on the interface of VLAN 214.

```
[PE_A] vlan 214
[PE_A-vlan214] port gigabitethernet 2/1/4
[PE_A-vlan214] quit
[PE_A] interface vlan-interface 214
[PE_A-Vlan-interface214] ip address 5.5.5.1 24
[PE_A-Vlan-interface214] mpls
[PE_A-Vlan-interface214] quit
```

Configure the local connection.

```
[PE_A] ccc local-conn interface vlan-interface 211 out-interface
vlan-interface 213
```

Configure a static LSP, with the out-label of 100 and the egress interface being the interface of VLAN 214.

```
[PE_A] mpls
[3Com-mpls] static-lsp ingress PEA-PEB l2vpn nexthop 5.5.5.2 out-
label 100
```

Configure a static LSP, with the in-label of 211 and the ingress interface being the interface of VLAN 214.

```
[PE_A-mpls] static-lsp egress PEB-PEA l2vpn incoming-interface vlan-
interface 214 in-label 211
```

Configure the remote connection.

```
[PE_A] ccc remote-connection interface vlan-interface 212 transmit-
lsp PEA-PEB receive-lsp PEB-PEA
```

2 Configure PE-B.

Enable MPLS globally.

```
[PE_B] mpls lsr-id 10.0.0.1
[PE_B] mpls
```

Enable MPLS L2VPN globally.

```
[PE_B] mpls l2vpn
```

Configure VLAN 211.

```
[PE_B] vlan 211
[PE_B-vlan211] port gigabitethernet 2/1/1
[PE_B] interface vlan-interface 211
[PE_B-Vlan-interface211] quit
```

Enable MPLS on the interface of VLAN 212.

```
[PE_B] vlan 212
[PE_B-vlan212] port gigabitethernet 2/1/2
[PE_B-vlan212] quit
[PE_B] interface Vlan-interface 212
[PE_B-Vlan-interface212] ip address 6.6.6.1 24
[PE_B-Vlan-interface212] mpls
```

Configure a static LSP, with the out-label of 200 and the egress interface being the interface of VLAN 212.

```
[PE_B-mpls] static-lsp ingress PEB-PEA l2vpn nexthop 6.6.6.2 out-
label 200
```

Configure a static LSP, with the in-label of 101 and the ingress interface being the interface of VLAN 212.

```
[3Com-mpls] static-lsp egress PEA-PEB l2vpn incoming-interface vlan-
interface 212 in-label 101
```

Configure the remote connection.

```
[SW8800] ccc remote-connection interface vlan-interface 211 transmit
-lsp PEB-PEA receive-lsp PEA-PEB
```

3 Configure P.

```
[PE_P] mpls lsr-id 10.0.0.2
[PE_P] mpls
[PE_P] vlan 214
[PE_P-vlan214] port gigabitethernet 2/1/1
[PE_P-vlan214] quit
[PE_P] interface Vlan-interface 214
[PE_P-Vlan-interface214] ip address 5.5.5.2 24
[PE_P-Vlan-interface214] mpls
[PE_P] vlan 212
[PE_P-vlan212] port gigabitethernet 2/1/2
[3Com-vlan212] quit
[PE_P] interface Vlan-interface 212
[PE_P-Vlan-interface212] ip address 6.6.6.2 24
[PE_P-Vlan-interface212] mpls
```

Configure a static LSP, with the in-label of 100, the ingress interface being the interface of VLAN 214, the out-label of 101, and the egress interface being the interface of VLAN 212.

```
[PE_P-mpls] static-lsp transit PEA-PEB l2vpn incoming-interface vlan-
interface 214 in-label 100 nexthop 6.6.6.1 out-label 101
```

Configure a static LSP, with the in-label of 200, the ingress interface being the interface of VLAN 212, the out-label of 211, and the egress interface being the interface of VLAN 211.

```
[PE_P-mpls] static-lsp transit PEB-PEA l2vpn incoming-interface vlan-
interface 212 in-label 200 nexthop 5.5.5.1 out-label 211
```



CAUTION: Following must be met to make a local CCC connection to go up:

- The interfaces of the two CE are physically up.
- The encapsulation types of the interfaces of the two CEs are the same and are supported by the MPLS L2VPN.

For Layer 2 connections with the MPLS L2VPN being VLAN encapsulation, the VLAN IDs of the interfaces of the two CEs can either be the same or different. However, if a trunk is configured between the CEs and the PEs on both sides, the VLAN IDs of the interfaces of the two CEs must be the same.

Martini MPLS L2VPN Configuration

Configuring Martini MPLS L2VPN

Table 565 Configure Martini MPLS L2VPN

Operation	Command	Description
Enter system view	system-view	-
Configure the LSR ID	mpls lsr-id <i>lsr-id</i>	Required
Enable MPLS	mpls	Required
Quit to system view	quit	-
Configure the LDP remote peer	mpls ldp remote-peer <i>index</i>	Required. Before configuring the connection, you need to enable LDP on each router and each port of the public network along the connection and configure the LDP remote peer on the peer PE. Refer to LDP Configuration in MPLS module for the configuration related to LDP .
Quit to system view	quit	-
Enable MPLS L2VPN	mpls l2vpn	Required
Enter VLAN interface view	interface vlan-interface <i>vlan id</i>	-
Create a Martini MPLS L2VPN virtual connection in VLAN interface view	mpls l2vc <i>ip-address vc-id</i>	Required. To configure a Martini MPLS L2VPN on a PE, you need to provide the IP address (Lsr-id) of the peer PE and specify the VC ID. The combination of the VC ID and the encapsulation type must be unique on the PE.
Quit to system view	quit	-



CAUTION:

- You can configure only one VLAN on the access side of each VPN private network. Each VLAN can have only one interface. And IGMP must be disabled on the VLAN.
- L2VPN supports VLAN interfaces only. Configure L2VPN on a VLAN interface.

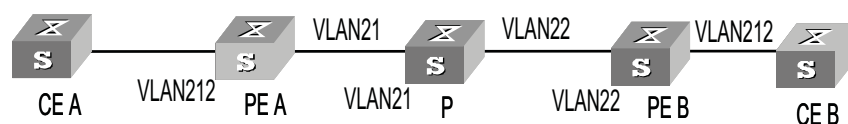
Martini MPLS L2VPN Configuration Example

Network requirements

CEs shown in Figure 150 are in the same VLAN as the corresponding PEs resides in. A remote connection is required between CE-A and CE-B.

Network diagram

Figure 150 Network diagram for Martini MPLS L2VPN



Configuration procedure**1** Configure PE-A.

Configure the LSR ID. Enable MPLS, LDP, and MPLS L2VPN.

```
[PE-A] mpls lsr-id 192.1.1.1
[PE-A] mpls
[PE-A-mpls] quit
[PE-A] mpls ldp
[PE-A] mpls l2vpn
```

Configure VLAN 212.

```
[PE-A] vlan 212
[PE-A-vlan212] port gigabitethernet 2/1/2
[PE-A-vlan212] interface vlan-interface 212
[PE-A-Vlan-interface212] quit
```

Configure VLAN 21.

```
[PE-A] vlan 21
[PE-A-vlan21] port gigabitethernet 2/1/1
[PE-A-vlan21] quit
[PE-A] interface Vlan-interface 21
[PE-A-Vlan-interface21] ip address 168.1.1.1 255.255.0.0
[PE-A-Vlan-interface21] mpls
[PE-A-Vlan-interface21] mpls ldp enable
```

Configure an IP address for the Loopback interface, which is used as the Router ID.

```
[PE-A] interface loopback 0
[PE-A-LoopBack0] ip address 192.1.1.1 255.255.255.255
```

Enable OSPF.

```
[PE-A] ospf 1
[PE-A-ospf-1] area 0.0.0.0
[PE-A-ospf-1-area-0.0.0.0] network 192.1.1.1 0.0.0.0
[PE-A-ospf-1-area-0.0.0.0] network 168.1.1.1 0.0.255.255
```

Create an LSP tunnel.

```
[PE-A] mpls
[PE-A-mpls] quit
[PE-A] mpls ldp
```

Configure the LDP Remote Peer.

```
[PE-A] mpls ldp remote-peer 1
[PE-A-remote-peer-1] remote-ip 192.1.1.2
```

Configure a Martini MPLS L2VPN connection.

```
[PE-A] interface vlan-interface 212
[PE-A-Vlan-interface212] mpls l2vc 192.1.1.2 20
```

2 Configure PE-B.

Configure the LSR ID. Enable MPLS, LDP, and MPLS L2VPN.

```
[PE-B] mpls lsr-id 192.1.1.2
[PE-B] mpls
[PE-B-mpls] quit
[PE-B] mpls ldp
[PE-B] mpls l2vpn
```

Configure VLAN 22.

```
[PE-B] vlan 22
[PE-B-vlan22] port gigabitethernet 2/1/1
[PE-B-vlan22] interface Vlan-interface 22
[PE-B-Vlan-interface22] ip address 169.1.1.1 255.255.0.0
[PE-B-Vlan-interface22] mpls
[PE-B-Vlan-interface22] mpls ldp enable
```

Configure VLAN 212.

```
[PE-B] vlan 212
[PE-B-vlan212] port gigabitethernet 2/1/2
[PE-B-vlan212] interface vlan-interface 212
[PE-B-Vlan-interface212] quit
```

Configure an IP address for the Loopback interface, which is used as the LSR ID.

```
[PE-B] interface loopback 0
[PE-B-LoopBack0] ip address 192.1.1.2 255.255.255.255
```

Enable OSPF.

```
[PE-B] ospf 1
[PE-B-ospf-1] area 0.0.0.0
[PE-B-ospf-1-area-0.0.0.0] network 192.1.1.2 0.0.0.0
[PE-B-ospf-1-area-0.0.0.0] network 169.1.0.0 0.0.255.255
```

Create an LSP tunnel.

```
[PE-B] mpls
[PE-B-mpls] quit
[PE-B] mpls ldp
```

Configure the LDP Remote Peer.

```
[PE-B] mpls ldp remote-peer 1
[PE-B-mpls-remote1] remote-ip 192.1.1.1
```

Configure a Martini MPLS L2VPN connection.

```
[PE-B] interface vlan-interface 212
[PE-B-Vlan-interface212] mpls l2vc 192.1.1.1 20
```

3 Configure P.

Configure the LSR ID. Enable MPLS, LDP, and MPLS L2VPN.

```
[PE-P] mpls lsr-id 192.1.1.3
[PE-P] mpls
[PE-P-mpls] quit
[PE-P] mpls ldp
[PE-P] mpls l2vpn
```

Configure an IP address for the Loopback interface, which is used as the LSR ID.

```
[PE-P] interface loopback 0
[PE-P-LoopBack0] ip address 192.1.1.3 255.255.255.255
[PE-P-LoopBack0] quit
```

Configure the VLAN interface.

```
[PE-P] vlan 21
[PE-P-vlan21] port gigabitethernet 2/1/1
[PE-P-vlan21] quit
[PE-P] interface Vlan-interface 21
[PE-P-Vlan-interface21] mpls
[PE-P-Vlan-interface21] mpls ldp enable
[PE-P-Vlan-interface21] ip address 168.1.1.2 255.255.0.0
[PE-P-Vlan-interface21] quit
[PE-P] vlan 22
[PE-P-vlan22] port gigabitethernet 2/1/2
[PE-P-vlan22] quit
[PE-P] interface Vlan-interface 22
[PE-P-Vlan-interface22] mpls
[PE-P-Vlan-interface22] mpls ldp enable
[PE-P-Vlan-interface22] ip address 169.1.1.2 255.255.0.0
```

Enable OSPF.

```
[PE-P] ospf 1
[PE-P-ospf-1] area 0.0.0.0
[PE-P-ospf-1-area-0.0.0.0] network 168.1.0.0 0.0.255.255
[PE-P-ospf-1-area-0.0.0.0] network 169.1.0.0 0.0.255.255
[PE-P-ospf-1-area-0.0.0.0] network 192.1.1.3 0.0.0.0
```



CAUTION: *Following must be met to make an LDP Layer 2 VPN to go up:*

- The interfaces of the two CE are physically up.
- Two LSP tunnels, which are opposite in direction, exist between two PEs.
- The encapsulation types of interfaces of the two CEs are the same and are supported by the MPLS L2VPN.
- It is recommended that the VLANs on PEA and PEB which are connected to the CEs be consistent.
- LDP remote sessions exist between PEs and are in Operational state.

To establish a tunnel, routes to the peer PE are necessary. So you need to configure IGP (interior gateway protocol) on each router along the path, such as OSPF.

Kompella MPLS L2VPN Configuration

Configuring Kompella MPLS L2VPN

Table 566 Configure Kompella MPLS L2VPN

Operation	Command	Description
Enter system view	system-view	-
Configure the LSR ID	mpls lsr-id lsr-id	Required
Enable MPLS	mpls	Required
Enable MPLS L2VPN globally	mpls l2vpn	Required
Perform BGP (border gateway protocol) related configuration. Make sure BGP operates properly and routers can discover routes to other routers.	Refer to BGP Configuration in Routing Protocol module.	Required. In a Kompella MPLS L2VPN, the extended BGP is used as the signaling protocol to distribute VC labels. So, you also need to configure BGP parameters on PEs. As for the MPLS L2VPN itself, it has no special requirements on the BGP configuration.
Enter L2VPN address family view.	l2vpn-family	Required
Activate the peer or peer group.	peer { group-name peer-address } enable	Required. By default, only the peers of BGP IPv4 unicast address families are active. The peer groups of other types are deactivated and thus cannot exchange the routing information.
Quit to system view	quit	-
Create a VPN and specify the encapsulation type.	mpls l2vpn vpn-name [encapsulation { ethernet vlan }]	Required. The default encapsulation type is Ethernet. In the Kompella mode, the encapsulation type of the access side of the private network can be Ethernet access and VLAN access. If you configure the encapsulation type as Ethernet access, the port link type in a private network VLAN is Access type; if you configure the encapsulation type as VLAN access, the port link type in a private network VLAN is Trunk type. It is not recommended to use Hybrid type as the port link type in a private network VLAN. The user access modes of the instance in all the peer PEs must be consistent.

Table 566 Configure Kompella MPLS L2VPN

Operation	Command	Description
Configure the RD (route distinguisher) of the MPLS L2VPN	route-distinguisher <i>route-distinguisher</i>	Required. For an MPLS L2VPN, you must configure the RD before performing other configurations. An RD cannot be modified once it is configured. The only way to modify a configured RD is to remove the corresponding MPLS L2VPN and create another one. As for L2VPN, it is recommended that you assign a unique RD for each VPN.
Configure the VPN-target of the MPLS L2VPN	vpn-target <i>vpn-target-ext-community [import-extcommunity export-extcommunity both]</i>	Required
Configure the Layer 2 MTU (maximum transmission unit) of the VPN	mtu <i>mtu</i>	Optional. The same MTU value must be configured for all PEs in the same VPN.
Create a CE or modify the CE Range of an existing CE	ce name id id [range range] [default-offset offset]	Required. Each CE created on a PE needs to uniquely correspond to one actual CE device connected to the PE. You need to specify a unique ID for these CEs. You can also specify the CE Range. It is desired that the CE ID begins with 1 and increases in step of 1.
Enter an existing CE	ce name	
Create connections between CEs	connection [ce-offset offset] { interface vlan-interface vlan-id }	Required. When planning a VPN, you can specify CE IDs for CEs beginning with 1 and increasing in step of 1, and then establish connections by CE IDs. You can establish connections with CE Offset not provided for simplifying the configuration. In this case, the default CE Offset is used.

**CAUTION:**

- You can only change the CE range to a number larger than the existing one. For example, you can change a CE range from 10 to 20, rather than from 10 to 5. The only way to change a CE range to a smaller number is to remove the CE and create a new one.
- You can configure only one VLAN on the access side of each VPN private network. Each VLAN can have only one interface. And all the VLANs connecting to the interface must have IGMP disabled.
- In Kompella MPLS L2VPN, the encapsulation type on the access side of each private network can be Ethernet access and VLAN access. Ethernet access is the default type. If you configure the encapsulation type as Ethernet access, the port link type in a private network VLAN is Access type; if you configure the encapsulation type as VLAN access, the port link type in a private network

VLAN is Trunk type. It is not recommended to use Hybrid type as the port link type in a private network VLAN. The user access modes of the instance in all peer PEs must be consistent.

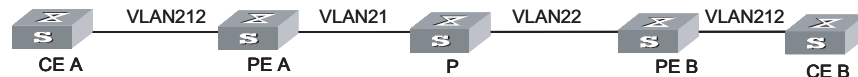
Kompella MPLS L2VPN Configuration Example

Network requirements

CEs shown in Figure 151 are in the same VLAN as the corresponding PEs resides in. A remote connection is required between CE-A and CE-B.

Network diagram

Figure 151 Network diagram for Kompella MPLS L2VPN



Configuration procedure

1 Configure PE-A.

Enable MPLS globally.

```
[PE-A] mpls lsr-id 1.1.1.1
[PE-A] mpls
[PE-A-mpls] quit
[PE-A] mpls ldp
```

Configure an IP address for the Loopback interface.

```
[PE-A] interface loopback 0
[PE-A-LoopBack0] ip address 1.1.1.1 32
```

Enable MPLS L2VPN globally.

```
[PE-A] mpls l2vpn
```

Configure VLAN 212.

```
[PE-A] vlan 212
[PE-A-vlan212] port gigabitethernet 2/1/2
[PE-A-vlan212] interface vlan-interface 212
[PE-A-Vlan-interface212] quit
```

Enable MPLS on the interface of VLAN 21.

```
[PE-A] vlan 21
[PE-A-vlan21] port gigabitethernet 2/1/4
[PE-A-vlan21] quit
[PE-A] interface vlan-interface 21
[PE-A-Vlan-interface21] ip address 5.5.5.1 24
[PE-A-Vlan-interface21] mpls
[PE-A-Vlan-interface21] mpls ldp enable
[PE-A-Vlan-interface21] mpls ldp transport-ip interface
[PE-A-Vlan-interface21] quit
```

Configure BGP.

```
[PE-A] bgp 100
[PE-A-bgp] group 100 internal
[PE-A-bgp] peer 100 connect-interface loopback0
[PE-A-bgp] peer 3.3.3.3 group 100
[PE-A-bgp] l2vpn-family
[PE-A-bgp-af-l2vpn] peer 100 enable
```

Create and configure the VPN.

```
[PE-A] mpls l2vpn vpn1 encapsulation ethernet
[PE-A-mpls-l2vpn-vpn1] route-distinguisher 100:1
[PE-A-mpls-l2vpn-vpn1] vpn-target 100:1
```

Create CE1 and configure the corresponding connection.

```
[PE-A-mpls-l2vpn-vpn1] ce ce1 id 1 range 200
[PE-A-mpls-l2vpn-vpn1-ce1] connection ce-offset 2 interface vlan-
interface 212
[PE-A-mpls-l2vpn-vpn1-ce1] quit
```

Enable OSPF.

```
[PE-A] ospf 1 router-id 1.1.1.1
[PE-A-ospf-1] area 0.0.0.0
[PE-A-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE-A-ospf-1-area-0.0.0.0] network 5.5.5.0 0.0.0.255
```

2 Configure PE-B.

Enable MPLS globally.

```
[PE-B] mpls lsr-id 3.3.3.3
[PE-B] mpls
[PE-B-mpls] quit
[PE-B] mpls ldp
```

Configure an IP address for the Loopback interface.

```
[PE-B] interface loopback 0
[PE-B-LoopBack0] ip address 3.3.3.3 32
```

Enable MPLS L2VPN globally.

```
[PE-B] mpls l2vpn
```

Configure VLAN 212.

```
[PE-B] vlan 212
[PE-B-vlan212] port gigabitethernet 2/1/2
[PE-B-vlan212] interface vlan-interface 212
[PE-B-Vlan-interface 212] quit
```

Enable MPLS on the interface of VLAN 22.

```
[PE-B] vlan 22
[PE-B-vlan22] port gigabitethernet 2/1/4
[PE-B-vlan22] quit
[PE-B] interface vlan-interface 22
```

```
[PE-B-Vlan-interface22] ip address 6.6.6.1 24
[PE-B-Vlan-interface22] mpls
[PE-B-Vlan-interface22] mpls ldp enable
[PE-B-Vlan-interface22] mpls ldp transport-ip interface
[PE-B-Vlan-interface22] quit
```

Configure BGP.

```
[SW8800] bgp 100
[PE-B-bgp] group 100 internal
[PE-B-bgp] peer 100 connect-interface loopback0
[PE-B-bgp] peer 1.1.1.1 group 100
[PE-B-bgp] l2vpn-family
[PE-B-bgp-af-l2vpn] peer 100 enable
```

Create and configure VPN1.

```
[PE-B] mpls l2vpn vpn1 encapsulation ethernet
[PE-B-mpls-l2vpn-vpn1] route-distinguisher 100 :1
[PE-B-mpls-l2vpn-vpn1] vpn-target 100 :1
```

Create CE2 and configure the corresponding connection.

```
[PE-B-mpls-l2vpn-vpn1] ce ce2 id 2 range 200
[PE-B-mpls-l2vpn-vpn1-ce2] connection ce-offset 1 interface vlan-
interface 212
[PE-B-mpls-l2vpn-vpn1-ce2] quit
```

Enable OSPF.

```
[PE-B] ospf 1 router-id 3.3.3.3
[PE-B -ospf-1] area 0.0.0.0
[PE-B -ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE-B -ospf-1-area-0.0.0.0] network 6.6.6.0 0.0.0.255
```

3 Configure the P device.

The configuration of P device is the same as that of standard MPLS configuration. Refer to the P router Configuration of BGP/MPLS VPN in Basic MPLS Operation Manual.

Note that the VLANs on PEA and PEB which are connected to the CEs must be consistent.

Displaying and Debugging MPLS L2VPN

After the above configuration, you can verify your configuration concerning MPLS L2VPN by executing the **display** command in any view and checking the output information.

You can execute the **debugging** command in user view to debug MPLS L2VPN.

Table 567 Display and debug L2VPN

Operation	Command	Description
Display information about a CCC MPLS L2VPN connection	display ccc [<i>ccc-name</i> type [local remote]]	
Display information about a Martini MPLS L2VPN connection	display mpls l2vc [interface vlan-interface <i>vlan-id</i> verbose]	
Display information about a Kompella MPLS L2VPN connection	display mpls l2vpn [<i>vsi-name</i> [local-ce remote-ce] connection [<i>vsi-name</i> [down remote-ce up verbose] brief interface Vlan-interface <i>vlan-id</i>] forwarding-info { <i>vc-label</i> interface <i>interface-type</i> }]	You can execute the display command in any view.
Display information about the system or about Kompella MPLS L2VPNs	display bgp l2vpn all	
Enable debugging for MPLS L2VPN	debugging mpls l2vpn { all loadshare advertisement error event connections [interface vlan-interface <i>vlan-id</i>] }	Execute this command in user view.

Troubleshooting MPLS L2VPN

Symptom 1: Fail to configure Layer 2 VPN on the VLAN interface.

Solution:

- Check to see if MPLS/BGP VPN, multicast, or VLL is enabled on the VLAN interface. Because you cannot perform Layer 2 VPN configuration on a VLAN interface if MPLS/BGP VPN, multicasting, or VLL is enabled on it.
- Check to see if the VLAN is a Super-Vlan or a Sub-Vlan. You can perform the Layer 2 VPN configuration only on common VLAN interfaces.

Symptom 2: Fail to ping the peer from one end of a Martini MPLS L2VPN connection. The VC is down and the Remote value is invalid.

Solution:

- VC state being down indicates the encapsulation types or VC IDs of the two ends are not the same. Make sure the interface types (Access or Trunk) of the two PE interfaces and the VC IDs of the two ends are consistent.
- As for the invalid Remote value, make sure you have configured the Remote parameters and the peer addresses correctly.

Symptom 3: Fail to ping the peer of a Kompella MPLS L2VPN connection. The Connection is down and the VPN value is null.

Solution:

- VPN value being null indicates the VPN is configured incorrectly. Make sure the VPN configurations (such as RD) of the both ends are consistent, and the connection configurations of the two CEs on both ends are correct.

- Connection being down indicates configurations concerning encapsulation of the two ends are not the same. Make sure the encapsulation types and MTUs configured for the local and remote PE devices are consistent. A connection fails if the encapsulation types configured on the two ends are not the same.

Symptom 4: Fail to ping the peer end of a CCC MPLS L2VPN connection. The sending and receiving channels are up, so does the link connection.

Solution:

- Make sure the in-label and out-label configured on the both ends correspond to each other. If a P device exists, make sure its forwarding connection configuration is correct, and the next hop configured statically is configured.



The service processor card mentioned in this chapter refers to the 3C17548 VPLS Application Module.

VPLS Overview

Introduction to VPLS

Today, IP networks have spread throughout the world. And the operators are focusing on using their existing IP networks to provide enterprises with low-cost private networks. Now, an easily implemented technique called MPLS VPN (multiprotocol label switching VPN) emerges as the times require, which enables the operators to provide arbitrary-rate MPLS-based virtual private network (VPN) services over IP networks.

MPLS VPN services fall into two types: L3 MPLS VPN and L2 MPLS VPN. The latter includes VPLS (virtual private LAN service) and VLL (virtual leased line). VLL only applies to point-to-point networking, while VPLS can apply to multipoint-to-multipoint VPN networking. VPLS provides the operators using point-to-point L2VPN with a better solution. In addition, unlike L3VPN, VPLS does not participate in user's internal routing. Now, operators need only manage and operate a single network to provide multiple kinds of services such as best-effort, L3VPN, L2VPN, traffic-engineering, and distinguished services. This greatly reduces their costs on network construction, operation and maintenance.

With VPLS, users in different areas can be connected with each other through MAN/WAN just like they are in one LAN. Switch 8800 Family series provide a VPLS solution. This solution uses MPLS-based virtual links as the links of Ethernet bridges and provides transparent transmission LAN services (TLS) over MPLS networks.

The following table lists the acronyms referred in this document:

Table 568 Acronyms

Acronym	Full name
AC	Attachment Circuit
CE	Customer Edge
FEC	Forwarding Equivalence Class
FR	Frame Relay
NPE	Network Facing PE
PE	Provider Edge Router
PW	Pseudowire
PHP	Penultimate Hop Popping

Table 568 Acronyms

Acronym	Full name
UPE	User Facing PE
VLL	Virtual Leased Line
VPLS	Virtual Private LAN Service
VSI	Virtual Switching Instance
LSP	Label Switched Path

Basic VPLS Network Architectures

There are two kinds of VPLS network architectures: PW logical multipoint-to-multipoint connection architecture and hierarchical architecture. Figure 152 depicts a VPLS network architecture with PW logical multipoint-to-multipoint connection.

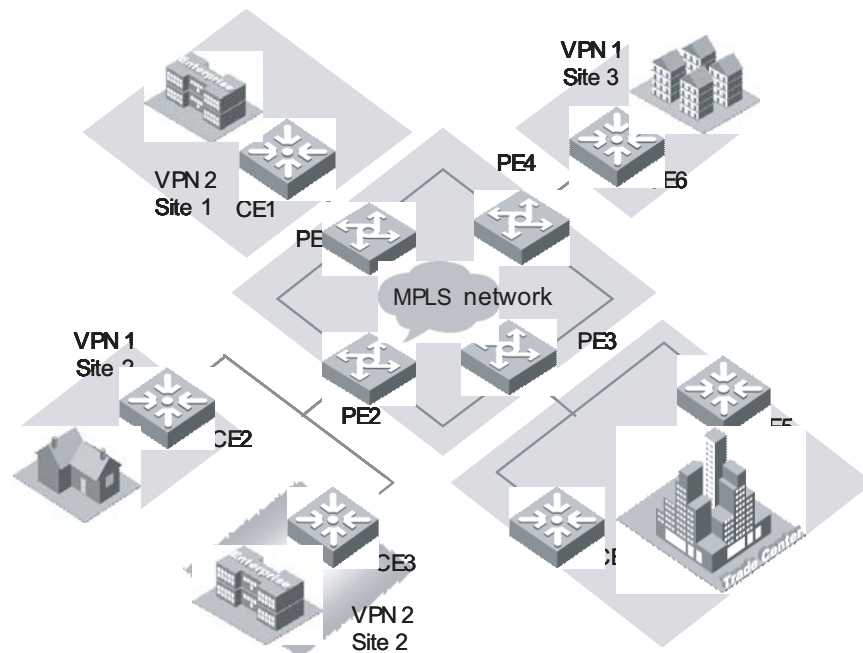
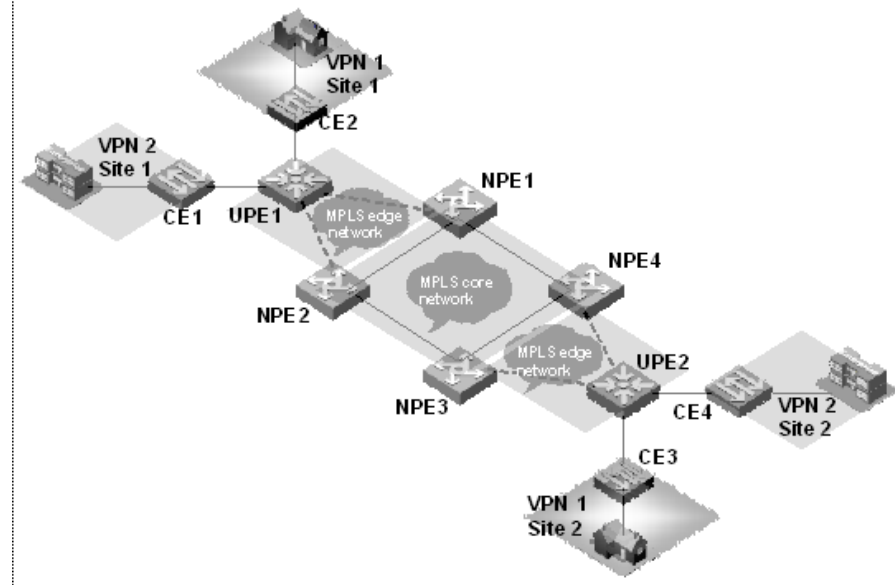


Figure 152 VPLS network with PW logical multipoint-to-multipoint connection

As shown in Figure 152, VPLS can provide point-to-multipoint connection service like a L3VPN. It can learn MAC addresses and exchange packets between multiple sites. In addition, it keeps the forwarding tables of the individual VPNs independent with each other and allows MAC address overlap between VPNs.

Figure 153 depicts a hierarchical VPLS network architecture.

Figure 153 Hierarchical VPLS network architecture

As shown in Figure 153, the network topology of the VPLS network is hierarchical, and the access range of the network is expandable. The core devices (NPEs) in the core network require high performance because VPN traffic concentrates there, while the edge devices (UPEs) require lower performance because they are mainly used for VPN service access. In addition, you can back up the links between NPEs and UPEs to make the network more robust. The access networks between UPEs and NPEs can be either a MPLS edge network connected by LSP, or a simple Ethernet network for VLAN-VPN user access.

VPLS Operational Principle

VPLS Basic Transmission Components

As shown in the following figure, the whole VPLS network is just like a huge switch. For each VPN, it sets up PWs between the sites of the VPN on MPLS tunnels and transparently transmits user's layer 2 packets from one site to another through these PWs. In this network, PEs forward packets, learn source MAC addresses, create MAC forwarding entries, and map the MAC addresses to corresponding ACs and PWs. While, the P devices (provider routers, that is, core switches in the backbone network), only implement MPLS forwarding according to MPLS labels without considering layer 2 user data encapsulated in MPLS packets.

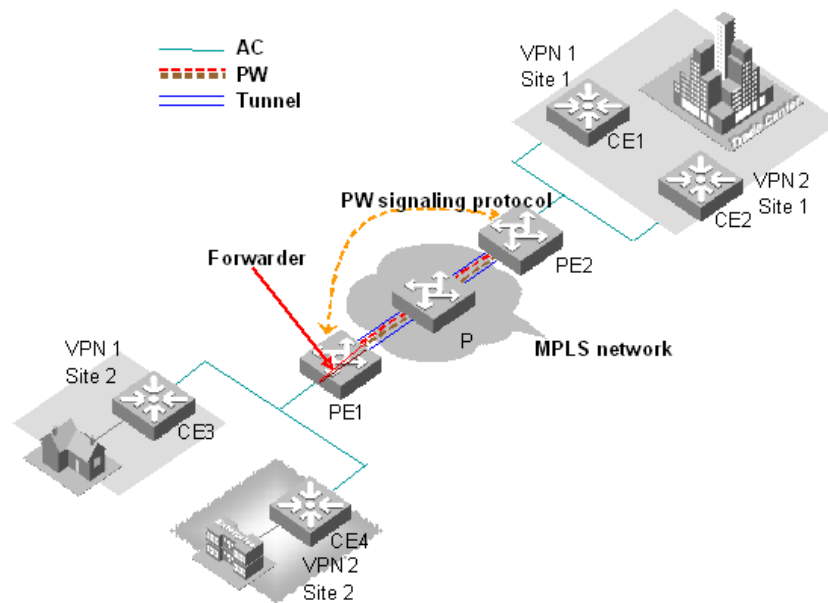


Figure 154 L2VPN universal transmission components

The transmission components and their functions in a VPLS network are as follows:

Attachment circuit

An attachment circuit (AC) is a virtual connection link between CE and PE. User's layer 2 and layer 3 data are transmitted to the peer site through AC without any modification.

Pseudowire

A pseudowire (PW) is a bidirectional virtual connection between two VSIs in a VPN. One PW contains a pair of unidirectional MPLS VCs (virtual circuits). It is established by PW signaling protocol and carried on LSP. For a VPLS system, a PW is just like a directly connected path between local and peer ACs, through which user's layer 2 data are transmitted transparently.

Forwarder

A forwarder is in fact a VPLS forwarding table, it chooses PWs to forward the frames that PEs received from ACs.

Tunnel

A tunnel is a directly connected path between local PE and peer PEs, on which data is transmitted transparently from one PE to another. A tunnel can carry multiple PWs. In general, a tunnel is an MPLS tunnel.

Encapsulation

Standard PW encapsulation formats and technique are adopted when packets are transmitted over PWs. VPLS packets carried on PWs have two encapsulation modes: VLAN and Ethernet.

PW signaling

PW signaling (pseudowire signaling) protocol on which VPLS bases is used to establish and maintain PW. It can also be used to automatically discover peer PEs of VSIs. Currently, PW signaling protocol includes label distribution protocol (LDP) and border gateway protocol (BGP).

Service quality

Service quality maps priority information in the headers of user's layer 2 packets and QoS information carried by VSI instances to QoS priority of the public network before the forwarding of the packets. This feature generally requires the MPLS network to support traffic-engineering.

As shown in Figure 154, CE3 transmits uplink layer 2 packets to PE1 through AC. When PE1 receives the packets, the forwarder chooses PW to forward them. According to PW forwarding entries, the system generates two layers of MPLS labels (private network labels are used to mark the PWs, and public network labels are used to pass through tunnels to PE2) and the Ethernet headers of the public network. After the packets reach PE2 through public network tunnel, the system pops out private network labels (public network labels have already been popped out on P device through PHP). PE2 forwarder chooses an AC to forward layer 2 packets from CE3 to CE1.

Concepts Related to VPLS

MPLS L2VPN An MPLS L2VPN is a VPN that transparently transmits user's layer 2 packets over MPLS network. In user's perspective, an MPLS network is a layer 2 switching network, over which layer 2 connections can be set up among different sites. MPLS L2VPN includes VLL and VPLS.

VPLS

This is a kind of point-to-multipoint L2VPN service provided on public networks. VPLS can connect user sites in different areas together over MAN/WAN as if they are in a single LAN.

VLL

This is a kind of point-to-point L2VPN service provided on public networks. VLL can connect two sites with each other as if they are directly connected by cables. However, it cannot provide switching directly between multiple points at the service provider level.

CE It is a user device that is directly connected with a service provider's device.

PE It is an edge router in backbone network connected with CEs. PE is responsible for VPN service access, it implement packet mapping and forwarding from private networks to public network tunnels, and vice versa. It has two types: UPE and NPE.

UPE

It is a user-facing PE device, a kind of convergence device for users to access the VPN.

NPE

It is a core PE device, located at the edge of the VPLS core network. It provides VPLS transparent transmission service in the core network.

VSI Through virtual switching instance (VSI) you can map the actually connected links to each virtual links.

VPLS Basic Configuration

VPLS Configuration Tasks

Table 569 VPLS configuration tasks

Operation	Command	Description
Configure routing protocol for public network	Refer to the related sections in <i>Operation Manual - Routing Protocol</i>	Required
Configure basic MPLS functions	Refer to chapter 2 Configuring MPLS Basic Functions in <i>Operation Manual - MPLS</i>	Required
Configure LDP expansion session peer	mpls ldp remoter-peer <i>index</i>	Required
Enabling L2VPN	mpls l2vpn	Required
Configure a VPLS instance	vsi <i>vsi-name</i> [static]	Required. static is required for configuring a VSI.
Configure an IP address of a peer PE	peer <i>peer-ip</i> [vc-id <i>vc-id</i>] [upe dual-npe] [encapsulation { ethernet vlan }]	Required
Configure static MAC addresses	mac-address { static <i>H-H-H</i> } vsi <i>vsi-name</i> { peer <i>peer-ip</i> vlan-interface <i>vlan-interface-number</i> }	Optional
Configure VLAN for user access and binding VSI	l2 binding vsi <i>vsi-name</i> [access-mode { vlan ethernet }]	Required
Configure VPLS characteristics	bandwidth <i>bw-limit</i>	Optional
Enable VLAN VPN (Q-in-Q) on port	vlan-vpn enable	Optional
Configure user-defined flow template	flow-template user-defined <i>slot slotnum</i> <i>template-info</i>	Required
Configure ACL rules	rule <i>rule-id</i> permit mpls l2label-range ingress any egress any	Required
Configure packet redirection	traffic-redirect inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] slot <i>slotid</i> <i>vlanid</i> [join-vlan] }	Required
Enable VPSL load sharing	vpls-load-share enable	Optional

Configuring Routing Protocols

You must perform some basic routing configuration on your switch such that it can exchange routing information with other P and PE devices. Currently, you can choose the following routing protocols: static routing, routing information protocol (RIP), open shortest path first (OSPF), exterior border gateway protocol (EBGP), and so on. For specific configuration, refer to *Switch 8800 Family Series Routing Switches Operation Manual - Routing Protocol*.

Configuring Basic MPLS Functions

Configure basic MPLS functions to create LSP tunnels over public network. For specific configuration, refer to the "MPLS" section in *3Com Switch 8800 Family Series Routing Switches Operation Manual Volume I*.

Configuring LDP Expansion Session Peer

Configure LDP remote peer to set up LDP remote session.

Entering the remote-peer mode

Perform the following configuration in system view.

Table 570 Enter the remote-peer mode

Operation	Command
Enter the remote-peer mode	mpls ldp remote-peer <i>index</i>
Remove the remote peer	undo mpls ldp remote-peer <i>index</i>

By default, no remote peer exists.

Configuring an address for the remote peer

You can specify any LDP-enabled interface address of a remote peer device or the loopback address of a label switch router (LSR) that has advertised its routing information as the address of the remote peer.

Perform the following configuration in remote-peer view.

Table 571 Configure an address for the remote peer

Operation	Command
Configure an address for the remote peer	remote-ip <i>remoteip</i>

Enabling L2VPN

Enable L2VPN globally before you configure VPLS and VLL; otherwise you cannot configure VPLS and VLL.

Perform the following configuration in system view.

Table 572 Enable L2VPN

Operation	Command
Enable MPLS L2VPN	mpls l2vpn
Disable MPLS L2VPN	undo mpls l2vpn

By default, MPLS L2VPN is disabled.

Creating a VPLS Instance **Specifying a VPLS instance name**

Use the **vsi** command to create a VPLS instance or enter VSI view. When creating a VPLS instance, you must specify a locally unique VPLS instance name, and must choose automatic discovery or manual configuration as peer discovery mechanism. Currently, only manual configuration, namely, static mode, is supported.

Table 573 Specify a VPLS instance name

Operation	Command
Specify a VPLS instance name	vsi <i>vsi-name</i> [static]
Remove a VPLS instance or quit the VSI view	undo vsi <i>vsi-name</i>

Entering VSI-LDP view and configure VSI-ID

Use the **pwsignal** command to specify a PW signaling protocol used by the VSI and enter the VSI-LDP view.

Specifying LDP as the PW signaling protocol for the VSI takes you to the VSI-LDP view

Perform the following configuration in VSI view.

Table 574 Specify Martini as the VPLS connection mode

Operation	Command
Specify the PW signaling protocol to be used by the VSI	pwsignal [ldp]

Currently, PW signaling supports LDP only.

Use the **vsi-id** command to specify an ID for the current VSI. The ID must be locally unique.

Perform the following configuration in VSI-LDP view.

Table 575 Configure a VPLS instance

Operation	Command
Specify a ID for the current VSI	vsi-id <i>vsi-id</i>

Configuring an IP address of a peer PE

Use the **peer** command to create a VPLS peer PE contained in an instance. When you create a VPLS peer PE, you must specify an IP address and peer type for the peer PE. By default, the peer type is NPE. When you specify UPE as the peer type, it indicates the peer is a user convergence node UPE in hierarchical VPLS architecture. You can also specify an ID for a VC to the peer, and the ID must be consistent with that of the remote. Multipoint-to-multipoint connections are needed among specified multiple remote peer NPEs, but not needed between UPEs and NPEs.

Perform the following configuration in VSI-LDP view.

Table 576 Configure an IP address for a peer PE

Operation	Command
Create a VPLS peer PE contained in the instance	peer <i>peer-ip</i> [vc-id <i>vc-id</i>] [upe dual-npe] [encapsulation { ethernet vlan }]
Remove the specified VPLS peer PE	undo peer peer-ip

By default, VC-ID is as big as VSI-ID.

Specifying the VC encapsulation type of the VSI

Perform the following configuration in VSI view.

Table 577 Specify the VC encapsulation type of the VSI

Operation	Command
Specify the VC encapsulation type of the VSI	encapsulation { vlan ethernet }

By default, the VC encapsulation type in the VSI takes this value.

Configuring VLAN for User Access and Binding a VPLS Instance

The port configuration on a VLAN interface differs depending on user access modes. If user gets access by Ethernet, you must enable VLAN-VPN on the access port of the VLAN. If user makes H-VPLS access by VLAN, or user's convergence multi-tenant unit (MTU) makes H-VPLS access by VLAN-VPN, you need not enable VLAN-VPN on the access port; instead, you must configure the port as Trunk, in this case, the VLAN Tag (VLAN ID currently configured for the user) carried in uplink packets must be consistent with that of the VLAN bound with the Trunk. If convergence UPE makes H-VPLS access by LSP, you can bind a VPLS instance to a VLAN containing no port. Additionally, you cannot bind one instance to multiple VLANs.

Perform the following configuration in VLAN interface view.

Table 578 Configure VLAN for user access and bind a VPLS instance

Operation	Command
Bind a VPLS instance to a VLAN interface	I2 binding vsi <i>vsi-name</i> [access-mode { vlan ethernet }]
Remove the binding	undo I2 binding vsi <i>vsi-name</i>



CAUTION:

- If any of GVRP, STP and 802.1x protocols is enabled on a port, you cannot enable VLAN VPN on the port;
- If IGMP Snooping is enabled in the VLAN to which the port belongs or if IGMP is enabled on the VLAN interface to which the port belongs, it is not allowed to enable VLAN VPN on the port, and vice versa;
- If a port with enabled VLAN VPN is to join in a VLAN, IGMP Snooping cannot be enabled on the VLAN and IGMP cannot be enabled on its VLAN interfaces;
- The interface of a VLAN with a VPLS instance bound to it cannot be assigned an IP address. Similarly, if the interface of a VLAN is assigned an IP address, you cannot bind VPLS instances to it.

- A VPLS instance can be bound to multiple VLANs. You can bind a VPLS instance to up to eight VLANs.
- It is not allowed to bind VSI instances to VLAN-interface1.

Configuring Static MAC Address

Use the **mac-address** command to configure a static MAC address for the VPLS instance. The address you configured can be either a MAC address on a local CE or a MAC address on a remote CE.

Perform the following configuration in system view.

Table 579 Configure static MAC address

Operation	Command
Configure a static MAC address for VPLS instance	mac-address { static <i>H-H-H</i> } vsi <i>vsi-name</i> { peer <i>peer-ip</i> vlan-interface <i>vlan-interface-number</i> }
Remove the MAC address	undo mac-address { static <i>H-H-H</i> } vsi <i>vsi-name</i>
Batch delete the MAC addresses of VPLS instances	undo mac-address vsi [<i>vsi-name</i> [peer <i>peer-ip</i> vlan-interface <i>vlan-id</i>]] [static dynamic]

Enabling VLAN VPN on a Port



CAUTION: User access mode of VSI determines whether you should enable VLAN-VPN on a port or not. If the access mode is Ethernet, you must enable VLAN-VPN on the access port such that your private VLAN Tag can be properly transferred. If the access mode is VLAN, you must set the access port to Trunk.

Perform the following configuration in Ethernet port view.

Table 580 Enable VLAN VPN on a port

Operation	Command
Enable VLAN VPN on a port	vlan-vpn enable
Disable VLAN VPN on the port	undo vlan-vpn



CAUTION:

- If GARP VLAN registration protocol (GVRP), spanning tree protocol (STP) or 802.1x protocol is enabled on a port, VLAN VPN on this port is not allowed to enable.
- If IGMP Snooping is enabled in the VLAN to which the port belongs or if IGMP is enabled on the VLAN interface to which the port belongs, it is not allowed to enable VLAN VPN on the port, and vice versa.
- If a port with enabled VLAN VPN is to join in a VLAN, IGMP Snooping cannot be enabled on the VLAN and IGMP cannot be enabled on its VLAN interfaces.

By default, VLAN VPN is disabled on ports.

Configuring user-defined flow template

Perform the following configuration in system view.

Table 581 Configure user-defined flow template

Operation	Command
Define flow template	flow-template user-defined slot <i>slotnum</i> <i>template-info</i>
Define user flow template in port view	flow-template user-defined
Remove flow template	undo flow-template user-defined

When you define the flow template, the total size of all the elements in the template must be less than 16 bytes.

Configuring ACL rules

Use the following commands to define a Layer 2 ACL.

Perform the following configuration in corresponding views.

Table 582 Configure ACL rules

Operation	Command
Enter a Layer 2 ACL view from system view	acl { number <i>acl-number</i> name <i>acl-name</i> advanced } [match-order { config auto }]
Define a sub-rule in Layer 2 ACL view	rule [<i>rule-id</i>] { permit deny } [mpls l2label-range [<i>range-id</i>]] [cos <i>cos-value</i> c-tag-cos <i>c-cos-value</i> exp <i>exp-value</i> ingress { { <i>source-vlan-id</i> [to <i>source-vlan-id-end</i>] <i>source-mac-addr</i> <i>source-mac-wildcard</i> c-tag-vlan <i>c-tag-vlanid</i> } * any } egress { <i>dest-mac-addr</i> <i>dest-mac-wildcard</i> any } s-tag-vlan <i>s-tag-vlanid</i> time-range <i>name</i>]*
Remove a sub-rule in Layer 2 ACL view	undo rule <i>rule-id</i>
Remove Layer 2 ACL or all ACLs in system view	undo acl { number <i>acl-number</i> name <i>acl-name</i> all }



Delete related redirection configurations before deleting ACL configuration.

Configuring MPLS redirection

Only VPLS service processor cards can process VPLS services, so it is necessary to redirect the VPLS packets back from the public network side to VPLS service processor card for processing by configuring ACL rules.

Perform the following configuration in Ethernet port view.

Table 583 Configure packet redirection on Ethernet port of common interface card

Operation	Command
Configure packet redirection to a specific port of VPLS service processor cards	traffic-redirect inbound link-group <i>acl-number</i> [rule <i>rule</i> [system-index <i>index</i>]] slot <i>slotid</i> vlanid [join-vlan] }
Remove packet redirection	undo traffic-redirect inbound link-group <i>acl-number</i> [rule <i>rule</i>] }



After you configure packet redirection, the ports of the public network add to the VLAN (specified **join-vlan**). After you remove packet redirection configuration, the ports exit from the corresponding VLAN.

Configuring VPLS load sharing

When multiple modules exist within a single chassis, the load can be shared between them. For example, Configure VSIs through 7 with label ranges 0 through 7 respectively. Then associate the VPLS module in slot 0 with label ranges 0 through 3 and the VPLS module in slot 1 with label ranges 4 through 7 using the ACL command listed in Table 584.

By default, a created VSI falls within the label range that has the least VSIs and the flow of the VSI is redirected by the label range to the VPLS module for processing so that the load is shared. Meanwhile, you can also change the direction of the VSI flow manually by changing the label range corresponding to the VSI so that the load on VPLS modules is shared more evenly.

The **VPLS-LOAD-SHARE** command is enabled by default. When enabled, this command allows one VPLS module to take over for another VPLS module in the event of failure. If disabled, failure of the VPLS module in slot 0 would result in loss of traffic for VSIs 0 thru 3 and failure of the VPLS module in slot 1 would result in loss of traffic for VSIs 4 thru 7.

Table 584 Enable VPLS load sharing

Operation	Command	Description
Enter system view	system-view	-
Enable VPLS load sharing	vpls-load-share enable	Optional By default, VPLS load sharing is enabled.
Configure the label range ID corresponding to the VSI	label-range label-range-id	Optional By default, the label range ID corresponding to the VSI is the smallest label range ID that currently holds the least VSIs.
Add a rule for the Link ACL.	rule [rule-id] permit mpls l2label-range [range-id] ingress any egress any	Required By default, the label ranges from 128K to 256K-1.

Configuring VPLS Characteristics

Configuring VPN rate limitation

Use the **bandwidth** command to configure the VPN rate limitation in the range of 64 kbps to 4,194,303 kbps with the increment of 64. After the configuration, the system automatically takes the biggest number that can be exactly divided by 64 and is no more than the setting number as the rate limitation. For example, if you specify the VPN rate limitation to be 200, then the actual is 192, three times of 64. The actually supported rate limitation ranges from 64 kbps to 2,097,152 kbps (included), and if the value you set is above 2,097,152 kbps, no rate limitation is performed. In the instance, the part of traffic beyond this bandwidth restriction is discarded by the system.

Perform the following configuration in VSI view.

Table 585 Configure VPN rate limitation

Operation	Command
Configure VPN rate limitation	bandwidth bw-limit

By default, the VPN rate limitation is 102,400 kbps.

Configuring VPN broadcast suppression percentage

Use the **broadcast-restrain** command to configure the VPN broadcast suppression percentage, which is in the range of 0 to 100. You cannot set the percentage to 0. In the VSI, the part of broadcast traffic (including broadcast, multicast, and unknown unicast) beyond the suppression percentage is discarded.

Perform the following configuration in VSI view.

Table 586 Configure VPN broadcast suppression percentage

Operation	Command
Configure VPN broadcast suppression percentage	broadcast-restrain <i>percent</i>

By default, VPN broadcast suppression percentage is 5%.

Configuring packet MTU

Use the **mtu** command to specify the maximum transmission unit (MTU) value for user access packets of this VPLS instance, which is in the range of 128 to 8,192. This MTU value is also the MTU value for PW.

Perform the following configuration in VSI view.

Table 587 Configure packet MTU

Operation	Command
Configure packet MTU for the VPLS instance	mtu <i>mtu</i>
Restore the default MTU	undo mtu

By default, MTU is 1,500 Bytes.

Configuring CoS

Use the command to map user priority 802.1Q COS to PSN COS (PSN: Public Switching Network; COS: Class Of Service). When configuring the CoS mapping level, you can either use the CoS mapping table suggested by the protocol, or define user priority for PSN CoS mapping. .

Perform the following configuration in VSI view.

Table 588 Configure the CoS level

Operation	Command
Configure the CoS level for the VSI	cos { <i>cos-value</i> user-define-table <i>p p p p p p p p</i> }

The default CoS level is 0.

Configuring other VPLS characteristics

Perform the following configuration in the corresponding VSI views.

Table 589 Configure other VPLS characteristics

Operation	Command
Define/remove a description of this VPLS instance	description <i>text</i> undo description
Disable/enable the VPN service of the VPLS instance	shutdown undo shutdown
Configure the maximum number of the MAC addresses in the VPN	mac-table limit <i>mac-limit</i>

Displaying and Debugging VPLS

VPLS provides various displaying and debugging commands to monitor the LDP session status, tunnel configuration, all LSPs and their status.

Execute the following commands in any view.

Table 590 Display VPLS

Operation	Command
Display a VPLS forwarding table	display mac-address vsi [<i>vsi-name</i>] [peer <i>peer-address</i> local vlan-interface <i>vlan-interface-number</i>] [dynamic static] [count]
Display VC information of the VSI	display vpls connection [vsi <i>vsi-name</i>] [peer <i>peer-ip</i>] [up down block] [verbose statistics]
Display VPLS instance information	display vsi <i>vsi-name</i>

Execute the **debugging** command to debug various LDP messages.

Execute the following commands in user view.

Table 591 Debug VPLS

Operation	Command
Enable individual kinds of L2VPN debugging	debugging mpls l2vpn { advertisement all connections error event loadshare }
Disable individual kinds of L2VPN debugging	undo debugging mpls l2vpn { advertisement all connections error event loadshare }

By default, all debugging is disabled.

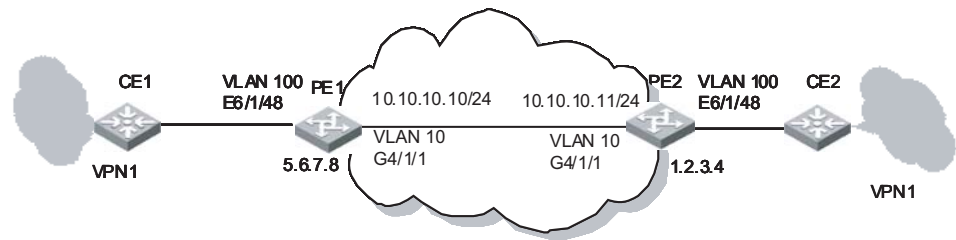
VPLS Basic Configuration Example

Network requirements

Switch 8800 Family series switch support all kinds of VPLS architectures and networking. Figure 155 shows a simple back-to-back network diagram. Where, two sites of VPN1 connect to port E6/1/48 of the two PEs (PE1 and PE2) respectively. Both PEs are configured with the private VLAN 100 and public VLAN 10 connected through G4/1/1 to implement basic VPLS service.

Network diagram

Figure 155 Network diagram for VPLS configuration of back-to-back PEs



Configuration procedure



The VPLS service processor card is on slot 5 on PE1 and PE2, and the common interface card is on slot 4.

1 Configure PE1

Configure the Router ID used to advertise OSPF routing information. Generally, the interface address of both MPLS LSR-ID and Loopback0 can be configured with the same IP address.

```
[PE1] router id 5.6.7.8
```

Configure MPLS LSI-ID. Enable MPLS and MPLS LDP globally.

```
[PE1] mpls lsr-id 5.6.7.8
[PE1] mpls
[PE1] mpls ldp
```

Configure a 32-bit Loopback address, which is used to create LSP.

```
[PE1] interface loopback0
[PE1 -LoopBack0] ip address 5.6.7.8 32
```

Configure a public VLAN, add a port to it, configure an IP address for the interface. Then, enable MPLS and MPLS LDP on the interface.

```
[PE1] vlan 10
[PE1-vlan10] port GigabitEthernet 4/1/1
[PE1-vlan10] interface vlan 10
[PE1-vlan-interface10] ip address 10.10.10.10 24
[PE1-vlan-interface10] mpls
[PE1-vlan-interface10] mpls ldp enable
```

Configure OSPF to set up routes.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 5.6.7.8 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 10.10.10.10 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] import-route direct
[PE1-ospf-1] quit
```

Configure a LDP remote peer (PE2) to set up LDP session.

```
[PE1] mpls ldp remote-peer 1
[PE1-mpls-remote1] remote-ip 1.2.3.4
```

Enable L2VPN globally.

```
[PE1] mpls l2vpn
```

Configure a VPLS instance and VSI-ID (VPN-ID). Enter VSI-LDP view to configure the IP address of PE2.

```
[PE1] vsi 3Com static
[PE1-vsi-3Com] pwsignal ldp
[PE1-vsi-3Com-ldp] vsi-id 500
[PE1-vsi-3Com-ldp] peer 1.2.3.4
[PE1-vsi-3Com-ldp] quit
```

Configure a private VLAN, add a port to it, and bind a VSI instance.

```
[PE1] vlan 100
[PE1-vlan-100] port Ethernet 6/1/48
[PE1-vlan-100] interface vlan 100
[PE1-vlan-interface100] l2 binding vsi 3Com access-mode ethernet
```

Enable VLAN-VPN on the port of the private network.

```
[PE1] interface Ethernet 6/1/48
[PE1-Ethernet6/1/48] vlan-vpn enable
```

Configure user-defined flow template, and ACL redirection rule to allow for MPLS packets with VPLS labels.

```
[PE1] flow-template user-defined slot 4 ethernet-protocol vlanid
[PE1] acl number 4000
[PE1-acl-link-4000] rule 0 permit mpls l2label-range ingress any egress any
[PE1-acl-link-4000] quit
```

Define user flow template in port view and configure redirection rule to redirect VPLS packets back from the public network to the VPLS service processor card and specify the VLAN ID of the redirection flow.

```
[PE1] interface GigabitEthernet4/1/1
[PE1-GigabitEthernet4/1/1] flow-template user-defined
[PE1-GigabitEthernet4/1/1] traffic-redirect inbound link-group 4000 rule 0
slot 5 10 join-vlan
```

Note that, if a common interface module is on slot 4 and all the eight label ranges corresponding to the rule are not assigned, you must configure the following command to prevent the flow in other label ranges not matched from being reported to the CPU:

Configure an ACL redirection rule for denying the MPLS packets with VPLS labels.

```
[PE1] acl number 4001
[PE1-acl-link-4001] rule 1 deny mpls l2label-range ingress any egress any
```


Enable the ACL in port view.

```
[PE1] interface GigabitEthernet4/1/1
[PE1-GigabitEthernet4/1/1] packet-filter inbound link-group 4001 rule 1
```

2 Configure PE2

Configure the Router ID used to advertise OSPF routing information. Generally, the interface address of both MPLS LSI-ID and Loopback0 can be configured with the same IP address.

```
[PE2] router id 1.2.3.4
```

Configure mpls lsr-id. Enable MPLS and MPLS LDP globally.

```
[PE2] mpls lsr-id 1.2.3.4
[PE2] mpls
[PE2] mpls ldp
```

Configure a 32-bit Loopback address, which is used to create LSP.

```
[PE2] interface loopback0
[PE2 -LoopBack0] ip address 1.2.3.4 32
```

Configure a public VLAN, add a port to it, configure the IP address for the interface. Then, enable MPLS and MPLS LDP on the interface.

```
[PE2] vlan 10
[PE2-vlan10] port GigabitEthernet 4/1/1
[PE2-vlan10] interface vlan 10
[PE2-vlan-interface10] ip address 10.10.10.11 24
[PE2-vlan-interface10] mpls
[PE2-vlan-interface10] mpls ldp enable
```

Configure OSPF to set up routes.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 1.2.3.4 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.10.10.11 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] import-route direct
[PE2-ospf-1] quit
```

Configure a LDP remote peer (PE1) to set up LDP session.

```
[PE2] mpls ldp remote-peer 1
[PE2-mpls-remote2] remote-ip 5.6.7.8
```

Enable L2VPN globally.

```
[PE2] mpls l2vpn
```

Configure a VPLS instance and VSI-ID (VPN-ID). Enter VSI-LDP view to configure the IP address for PE1.

```
[PE2] vsi 3Com static
[PE2-vsi-3Com] pwsignal ldp
```

```
[PE2-vsi-3Com-ldp] vsi-id 500
[PE2-vsi-3Com-ldp] peer 5.6.7.8
[PE2-vsi-3Com-ldp] quit
```

Configure a private VLAN, add a port to it, and bind a VSI instance.

```
[PE2] vlan 100
[PE2-vlan-100] port Ethernet 6/1/48
[PE2-vlan-100] interface vlan 100
[PE2-vlan-interface100] l2 binding vsi 3Com access-mode ethernet
```

Enable VLAN-VPN on the port of the private network.

```
[PE2] interface Ethernet 6/1/48
[PE2-Ethernet6/1/48] vlan-vpn enable
```

Configure user-defined flow template, and ACL redirection rule to allow for MPLS packets with VPLS labels.

```
[PE2] flow-template user-defined slot 4 ethernet-protocol vlanid
[PE2] acl number 4000
[PE2-acl-link-4000] rule 0 permit mpls l2label-range ingress any egress any
[PE2-acl-link-4000] quit
```

Define user flow template in port view and configure redirection rule to redirect VPLS packets back from the public network to the VPLS service processor card and specify the VLAN ID of the redirect flow.

```
[PE2] interface GigabitEthernet4/1/1
[PE2-GigabitEthernet4/1/1] flow-template user-defined
[PE2-GigabitEthernet4/1/1] traffic-redirect inbound link-group 4000 rule 0
slot 5 10 join vlan
```

Note that, if a common interface module on slot 4 and all the eight label ranges corresponding to the rule are not assigned, you must configure the following command to prevent the flow in other label ranges not matched from being reported to the CPU:

Configure an ACL redirection rule for denying the MPLS packets with VPLS labels.

```
[PE1] acl number 4001
[PE1-acl-link-4001] rule 1 deny mpls l2label-range ingress any egress any
```

Enable the ACL in port view.

```
[PE1] interface GigabitEthernet4/1/1
[PE1-GigabitEthernet4/1/1] packet-filter inbound link-group 4001 rule 1
```

Troubleshooting VPLS

Symptom 1: PW is not in UP state.

Solution:

- The LSP tunnel over the public network is not set up for the two ends: verify that the route is available on both ends, you can successfully ping the loopback port of the peer, and the LDP session is normal.

- Expansion session is abnormal: verify that the commands used to configure the expansion session are executed on both ends, and the configurations are all right.
- The interface of the private VLAN is not bound with the corresponding VPLS instance, or is DOWN: make sure the interface is UP, or the PW to the UPE is UP.
- The parameters for the peer or the MTU value of the VPLS instance is inconsistent: verify that the MTU value configured for the VPLS instance is consistent on both end, and the VC-ID and transmission mode for the peer is also consistent.
- The VPLS service processor card is not in Normal state: make sure that VPLS service processor card is in Normal state.

Symptom 2: Packets cannot be forwarded.

Solution:

- The service processor card is not in place: use the **display device** command to verify that the service processor card is in Normal state.
- The service processor card version is inconsistent with the SRP version: verify the service processor card version.
- The flow template and redirection are not correctly configured on the public side: verify the port for the public network is correctly configured.

Symptom 3: Packets get lost during the course of forwarding

Solution:

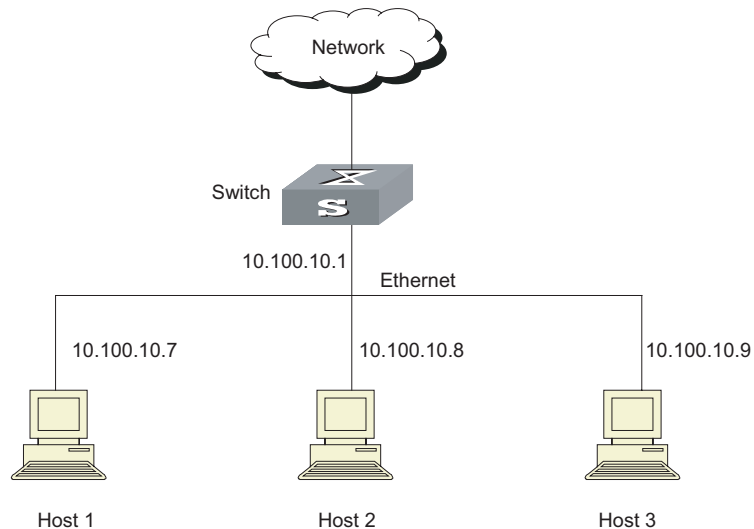
- Traffic exceeds VPN bandwidth restriction: Increase the VPN bandwidth.

Broadcast/multicast/unicast traffic exceeds the bandwidth set by broadcast suppression ratio: Modify the broadcast suppression ratio and verify by checking the broadcast suppression of the VPN and the broadcast traffic within the VPN.

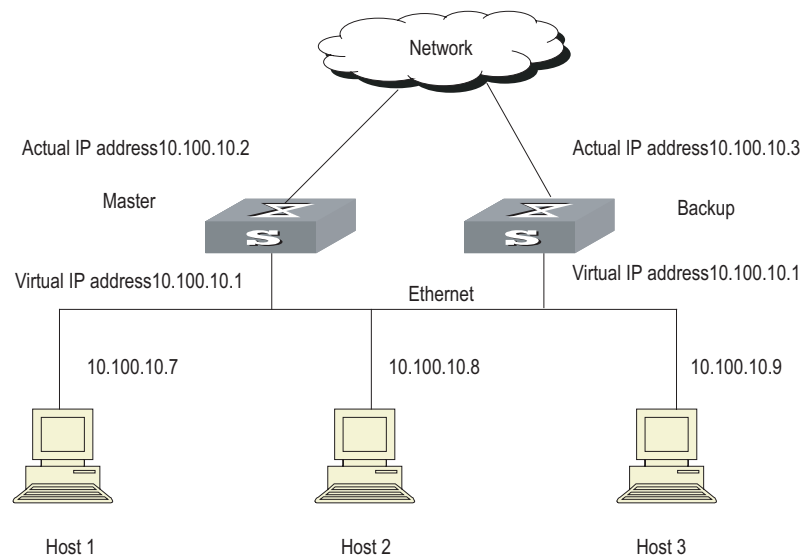
Introduction to VRRP

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant protocol. In general, a default route (for example, 10.100.10.1 as shown in the following internetworking diagram) will be configured for every host on a network, so that the packets destined to some other network segment from the host will go through the default route to the Layer 3 Switch, implementing communication between the host and the external network. If Switch is down, all the hosts on this segment taking Switch as the next-hop on the default route will be disconnected from the external network.

Figure 156 Network diagram for LAN



VRRP, designed for LANs with multicast and broadcast capabilities (such as Ethernet) settles the above problem. The diagram below is taken as an example to explain the implementation principal of VRRP. VRRP combines a group of LAN switches (including a Master and several Backups) into a virtual router.

Figure 157 Network diagram for virtual router

This virtual router has its own IP address: 10.100.10.1 (which can be the interface address of a switch within the virtual router). The switches within the virtual router have their own IP addresses (such as 10.100.10.2 for the Master switch and 10.100.10.3 for the Backup switch). The host on the LAN only knows the IP address of this virtual router 10.100.10.1 (usually called as virtual IP address of virtual router), but not the specific IP addresses 10.100.10.2 of the Master switch and 10.100.10.3 of the Backup switch. They configure their own default routes as the IP address of this virtual router: 10.100.10.1. Therefore, hosts within the network will communicate with the external network through this virtual router. If a Master switch in the virtual group breaks down, another Backup switch will function as the new Master switch to continue serving the host with routing to avoid interrupting the communication between the host and the external networks.

Configuring VRRP

The following sections describe the VRRP configuration tasks:

- "Enabling/Disabling the Function to Ping the Virtual IP Address"
- "Enabling/Disabling the Check of TTL Value of VRRP Packet"
- "Setting Correspondence between Virtual IP Address and MAC Address"
- "Adding/Deleting a Virtual IP Address"
- "Configuring the Priority of Switches in the Virtual Router"
- "Configuring Preemption and Delay for a Switch within a Virtual Router"
- "Configuring Authentication Type and Authentication Key"
- "Configuring Virtual Router Timer"
- "Configuring Switch to Track a Specified Interface"

Enabling/Disabling the Function to Ping the Virtual IP Address

This operation enables or disables the function to ping the virtual IP address of the virtual router. The standard protocol of VRRP does not support the ping function, then the user cannot judge with **ping** command whether an IP address is used by the virtual router. If the user configure the IP address for the host same as the virtual IP address of the virtual router, then all messages in this segment will be forwarded to the host.

So 3Com Switch 8800 Family Series Routing Switches (hereinafter referred to as Switch 8800 Family series) provide the ping function to ping the virtual IP address of the virtual router.

Perform the following configuration in system view.

Table 592 Enable/disable the ping function

Operation	Command
Enable to ping the virtual IP address	vrrp ping-enable
Disable to ping the virtual IP address	undo vrrp ping-enable

By default, the function to ping the virtual IP address is enabled.

You should set the ping function before configuring the virtual router. If a virtual router is already established on the switch, it is not allowed to use the **vrrp ping-enable** command and the **undo vrrp ping-enable** command to modify the configuration any more.

Enabling/Disabling the Check of TTL Value of VRRP Packet

This operation configures whether to check TTL value of VRRP packet on the Backup switch. The TTL value must be 225. If the Backup switch find TTL is not 225 when receiving VRRP packet, the packet will be discarded.

Perform the following configuration in VLAN interface view.

Table 593 Enable/disable the check of TTL value of VRRP packet

Operation	Command
Disable the check of TTL value of VRRP packet	vrrp un-check ttl
Enable the check of TTL value of VRRP packet	undo vrrp un-check ttl

By default, the switch checks TTL value of VRRP packets.

Setting Correspondence between Virtual IP Address and MAC Address

This operation sets correspondence between the virtual IP address and the MAC address. In the standard protocol of VRRP, the virtual IP address of the virtual router corresponds to the virtual MAC address, to ensure correct data forwarding in the sub-net.

Due to the chips installed, some switches support matching one IP address to multiple MAC addresses.

Switch 8800 Family series not only guarantee correct data forwarding in the sub-net, but also support such function: the user can choose to match the virtual IP address with the real MAC address or virtual MAC address of the routing interface.

The following commands can be used to set correspondence between the IP address and the MAC address.

Perform the following configuration in system view.

Table 594 Set correspondence between virtual IP address and MAC address

Operation	Command
Set correspondence between the virtual IP address and the MAC address	vrrp method { real-mac virtual-mac }
Set the correspondence to the default value	undo vrrp method

By default, the virtual IP address of the virtual router corresponds to the virtual MAC address.

You should set correspondence between the virtual IP address of the virtual router and the MAC address before configuring the virtual router. Otherwise, you cannot configure the correspondence.

If you set correspondence between the IP address of the virtual router and the real MAC address, you can configure only one virtual router on VLAN interface.

Adding/Deleting a Virtual IP Address

The following command is used for assigning a virtual IP address of the local segment to a virtual router or removing an assigned virtual IP address of a virtual router from the virtual address list.

Perform the following configuration in VLAN interface view.

Table 595 Add/delete a virtual IP address

Operation	Command
Add a virtual IP address	vrrp vrid <i>virtual-router-ID</i> virtual-ip <i>virtual-address</i>
Delete a virtual IP address	undo vrrp vrid <i>virtual-router-ID</i> [virtual-ip <i>virtual-address</i>]

The *virtual-router-ID* covers the range from 1 to 255.

The *virtual-address* can be an unused address in the network segment where the virtual router resides, or the IP address of an interface in the virtual router. If the IP address is of the switch in the virtual router, it can also be configured as *virtual-address*. In this case, the switch will be called an IP Address Owner. When adding the first IP address to a virtual router, the system will create a new virtual router accordingly. When adding a new address to this virtual router thereafter, the system will directly add it into the virtual IP address list.

After the last virtual IP address is removed from the virtual router, the whole virtual router will also be removed. That is, there is no more virtual router on the interface any more and any configuration of it is invalid accordingly.

Configuring the Priority of Switches in the Virtual Router

The status of each switch in the virtual router will be determined by its priority in VRRP. The switch with the highest priority will become the Master.

Perform the following configuration in VLAN interface view.

Table 596 Configure the priority of switches in the virtual router.

Operation	Command
Configure the priority of switches in the virtual router.	vrrp vrid <i>virtual-router-ID</i> priority <i>priority</i>
Clear the priority of switches in the virtual router.	undo vrrp vrid <i>virtual-router-ID</i> priority

The priority ranges from 0 to 255. The greater the number, the higher the priority. However the value can only be taken from 1 to 254. The priority 0 is reserved for special use and 255 is reserved for the IP address owner by the system.

By default, the priority is 100.



The priority for IP address owner is always 255, which cannot be configured otherwise.

Configuring Preemption and Delay for a Switch within a Virtual Router

Once a switch in the virtual router becomes the Master switch, so long as it still functions properly, other switches, even configured with a higher priority later, cannot become the Master switch unless they are configured to work in preemption mode. The switch in preemption mode will become the Master switch, when it finds its own priority is higher than that of the current Master switch. Accordingly, the former Master switch will become the Backup switch.

Together with preemption settings, a delay can also be set. In this way, a Backup will wait for a period of time before becoming a Master. In an unstable network if the Backup switch has not received the packets from the Master switch punctually, it will become the Master switch. However, the failure of Backup to receive the packets may be due to network congestion, instead of the malfunction of the Master switch. In this case, the Backup will receive the packet after a while. The delay settings can thereby avoid the frequent status changing.

Perform the following configuration in VLAN interface view.

Table 597 Configure preemption and delay for a switch within a virtual router

Operation	Command
Enable the preemption mode and configure a period of delay.	vrrp vrid <i>virtual-router-ID</i> preempt-mode [timer delay <i>delay-value</i>]
Disable the preemption mode.	undo vrrp vrid <i>virtual-router-ID</i> preempt-mode

The delay ranges from 0 to 255, measured in seconds. By default, the preemption mode is preemption with a delay of 0 second.



If preemption mode is cancelled, the delay time will automatically become 0 second.

Configuring Authentication Type and Authentication Key

VRRP provides following authentication types:

- **simple**: Simple character authentication
- **md5**: MD5 authentication

In a network under possible security threat, the authentication type can be set to **simple**. Then the switch will add the authentication key into the VRRP packets before transmitting it. The receiver will compare the authentication key of the packet with the locally configured one. 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 not exceeding 8 characters should be configured.

In a totally unsafe network, the authentication type can be set to **md5**. The switch will use the authentication type and MD5 algorithm provided by the Authentication Header to authenticate the VRRP packets. In this case an authentication key not exceeding 8 characters should be configured.

Those packets failing to pass the authentication will be discarded and a trap packet will be sent to the network management system.

Perform the following configuration in VLAN interface view.

Table 598 Configure authentication type and authentication key

Operation	Command
Configure authentication type and authentication key	vrrp authentication-mode <i>authentication-type authentication-key</i>
Remove authentication type and authentication key	undo vrrp authentication-mode

The authentication key is case sensitive.



The same authentication type and authentication key should be configured for all VLAN interfaces that belong to the virtual router.

Configuring Virtual Router Timer

The Master switch advertises its normal operation state to the switches within the VRRP virtual router by sending them VRRP packets regularly (at *adver-interval*). And the backup switch only receives VRRP packets. If the Backup has not received any VRRP packet from the Master after a period of time (specified by *master-down-interval*), it will consider the Master as down, and then take its place and become the Master.

You can use the following command to set a timer and adjust the interval, *adver-interval*, between Master transmits VRRP packets. The *master-down-interval* of the Backup switch is three times that of the *adver-interval*. The excessive network traffic or the differences between different switch timers will result in *master-down-interval* timing out and state changing abnormally. Such problems can be solved through prolonging the *adver-interval* and setting delay time. *adver-interval* is measured in seconds.

Perform the following configuration in VLAN interface view.

Table 599 Configure virtual router timer

Operation	Command
Configure virtual router timer	vrrp vrid <i>virtual-router-ID</i> timer advertise <i>adver-interval</i>

Table 599 Configure virtual router timer

Operation	Command
Clear virtual router timer	undo vrrp vrid <i>virtual-router-ID</i> timer advertise

By default, *adver-interval* is configured to be 1.

Configuring Switch to Track a Specified Interface

VRRP interface track function has expanded the backup function. Backup is provided not only to the interface where the virtual router resides, but also to some other malfunctioning switch interface. By implementing the following command you can track some interface.

If the interface which is tracked is Down, the priority of the switch including the interface will reduce automatically by the value specified by *value-reduced*, thus resulting in comparatively higher priorities of other switches within the virtual router, one of which will turn to Master switch so as to track this interface.

When the IP forwarding module (IFM) device is being monitored, the priority of the switch including the interface will increase automatically by the value specified by *value-increased*. When the interface or the IFM device of this interface is Down, the priority of the switch will decrease by the value specified by *value-reduced*, thus resulting in comparatively higher priorities of other switches within the virtual router, one of which will turn to Master switch so as to track this interface.

Perform the following configuration in VLAN interface view.

Table 600 Configure switch to track a specified interface

Operation	Command
Configure the switch to track a specified interface	vrrp vrid <i>virtual-router-ID</i> track { ifm [increased <i>value-increased</i>] vlan-interface <i>interface-number</i> [reduced <i>value-reduced</i>] }
Stop tracking the specified interface	undo vrrp vrid <i>virtual-router-ID</i> track [ifm vlan-interface <i>interface-number</i>]

By default, *value-reduced* is taken 10 and *value-increased* is taken 2.



When the switch is an IP address owner, its interfaces cannot be tracked.

If the interface tracked is up again, the corresponding priority of the switch, including the interface, will be restored automatically

You can only track up to eight interfaces in one virtual router.

Displaying and debugging VRRP

After the above configuration, execute **display** command in any view to display the running of the VRRP configuration, and to verify the configuration. Execute **debugging** command in user view to debug VRRP configuration.

Table 601 Display and debug VRRP

Operation	Command
Display VRRP state information	display vrrp [interface <i>vlan-interface</i> <i>interface-number</i> [<i>virtual-router-ID</i>]]

Table 601 Display and debug VRRP

Operation	Command
Display the configuration information of the VRRP-enabled IFM device	display vrrp ifm
Display VRRP statistics information	display vrrp statistics [vlan-interface <i>interface-number</i> [<i>virtual-router-ID</i>]
Display VRRP summary information	display vrrp summary
Clear the statistics information about VRRP	reset vrrp statistics [vlan-interface <i>interface-number</i> [<i>virtual-router-ID</i>]]
Enable VRRP debugging.	debugging vrrp { state packet error }
Disable VRRP debugging.	undo debugging vrrp { state packet error }

You can enable VRRP debugging to check its running. You may choose to enable VRRP packet debugging (*option* as packet), VRRP state debugging (*option* as state), and/or VRRP error debugging (*option* as error). By default, VRRP debugging is disabled.

VRRP Configuration Example

VRRP Single Virtual Router Example

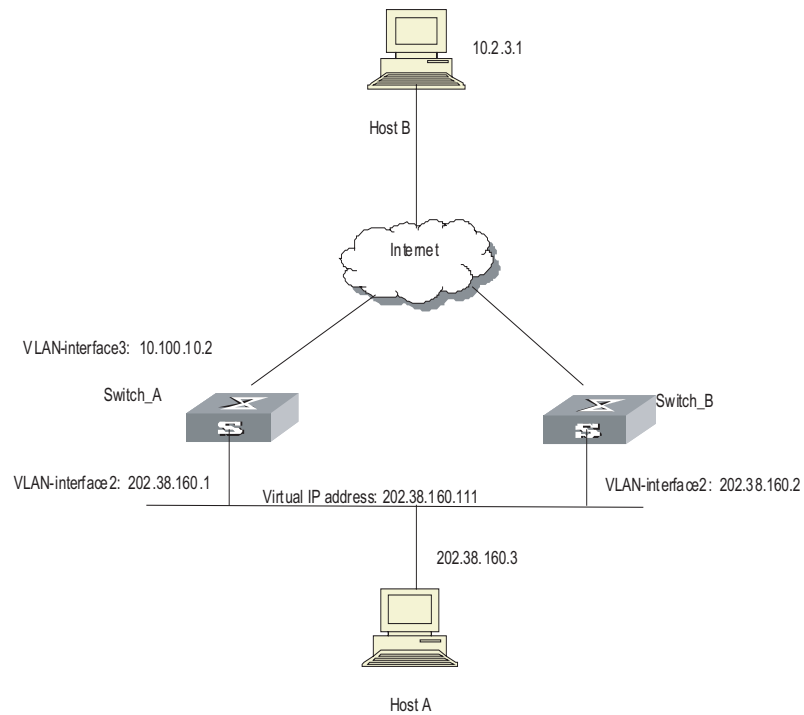
Networking requirements

Host A uses the VRRP virtual router which combines switch A and switch B as its default gateway to access host B on the Internet.

VRRP virtual router information includes: virtual router ID1, virtual IP address 202.38.160.111, switch A as the Master and switch B as the Backup allowed preemption.

Networking diagram

Figure 158 Network diagram for VRRP configuration



Configuration Procedure

Configure switch A

Configure VLAN 2.

```
[LSW-A] vlan 2
[LSW-A-vlan2] interface vlan 2
[LSW-A-vlan-interface2] ip address 202.38.160.1 255.255.255.0
[LSW-A-vlan-interface2] quit
```

Configure VRRP.

```
[LSW-A] vrrp ping-enable
[LSW-A] interface vlan 2
[LSW_A-vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
[LSW_A-vlan-interface2] vrrp vrid 1 priority 110
[LSW-A-vlan-interface2] vrrp vrid 1 preempt-mode
```

Configure switch B

Configure VLAN2.

```
[LSW-B] vlan 2
[LSW-B-vlan2] interface vlan 2
[LSW-B-vlan-interface2] ip address 202.38.160.2 255.255.255.0
[LSW-B-vlan-interface2] quit
```

Configure VRRP.

```
[LSW-B] vrrp ping-enable
[LSW-B] interface vlan 2
[LSW-B-vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
[LSW-B-vlan-interface2] vrrp vrid 1 preempt-mode
```

The virtual router can be used soon after configuration. Host A can configure the default gateway as 202.38.160.111.

Under normal conditions, switch A functions as the gateway, but when switch A is turned off or malfunctioning, switch B will function as the gateway instead.

Configure preemption mode for switch A, so that it can resume its gateway function as the Master after recovery.

VRRP Tracking Interface Example

Networking requirements

Even when switch A is still functioning, it may want switch B to function as gateway when the Internet interface connected with it does not function properly. This can be implemented by configuration of tracking interface.

In simple language, the virtual router ID is set as 1 with additional configurations of authorization key and timer.

Networking diagram

See Figure 158.

Configuration Procedure

Configure switch A

Configure VLAN2.

```
[LSW-A] vlan 2
[LSW-A-vlan2] interface vlan 2
[LSW-A-vlan-interface2] ip address 202.38.160.1 255.255.255.0
[LSW-A-vlan-interface2] quit
```

Enable the function to ping the virtual IP address of virtual router.

```
[3ComLSW-A ] vrrp ping-enable
```

Create a virtual router.

```
[LSW-A] interface vlan 2
[LSW_A-vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Set the priority for the virtual router.

```
[LSW_A-vlan-interface2] vrrp vrid 1 priority 110
```

Set the authentication key for the virtual router.

```
[LSW_A-vlan-interface2] vrrp authentication-mode md5 switch
```

Set Master to send VRRP packets every 5 seconds.

```
[LSW_A-vlan-interface2] vrrp vrid 1 timer advertise 5
```

Track an interface.

```
[LSW_A-vlan-interface2] vrrp vrid 1 track vlan-interface 3 reduced 30
```

Configure switch B

Configure VLAN2.

```
[LSW-B] vlan 2
[LSW-B-vlan2] interface vlan 2
[LSW-B-vlan-interface2] ip address 202.38.160.2 255.255.255.0
[LSW-B-vlan-interface2] quit
```

Enable the function to ping the virtual IP address of virtual router.

```
[3ComLSW-B] vrrp ping-enable
```

Create a virtual router.

```
[LSW-B] interface vlan 2
[LSW_B-vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Set the authentication key for the virtual router.

```
[LSW_B-vlan-interface2] vrrp authentication-mode md5 switch
```

Set Master to send VRRP packets every 5 seconds.

```
[LSW_B-vlan-interface2] vrrp vrid 1 timer advertise 5
```

Under normal conditions, switch A functions as the gateway, but when the interface vlan-interface 3 of switch A is down, its priority will be reduced by 30, lower than that of switch B so that switch B will preempt the Master for gateway services instead.

When vlan-interface3, the interface of switch A, recovers, this switch will resume its gateway function as the Master.

Multiple Virtual Routers Example

Networking requirements

A Switch can function as the backup switch for many virtual routers.

Such a multi-backup configuration can implement load balancing. For example, switch A as the Master switch of virtual router 1 can share the responsibility of the backup switch for virtual router 2 and vice versa for switch B. Some hosts employ virtual router 1 as the gateway, while others employ virtual router 2 as the gateway. In this way, both load balancing and mutual backup are implemented.

Networking diagram

Refer to Figure 158.

Configuration Procedure

Configure switch A

Configure VLAN2.

```
[LSW-A] vlan 2
[LSW-A-vlan2] interface vlan 2
[LSW-A-vlan-interface2] ip address 202.38.160.1 255.255.255.0
```

Create virtual router 1.

```
[LSW_A-vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Set the priority for the virtual router.

```
[LSW_A-vlan-interface2] vrrp vrid 1 priority 150
```

Create virtual router 2.

```
[LSW_A-vlan-interface2] vrrp vrid 2 virtual-ip 202.38.160.112
```

Configure switch B

Configure VLAN2.

```
[LSW-B] vlan 2
[LSW-B-vlan2] interface vlan 2
[LSW-B-vlan-interface2] ip address 202.38.160.2 255.255.255.0
```

Create virtual router 1.

```
[LSW_B-vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Create virtual router 2.

```
[LSW_B-vlan-interface2] vrrp vrid 2 virtual-ip 202.38.160.112
```

Set the priority for the virtual router.

```
[LSW_B-vlan-interface2] vrrp vrid 2 priority 110
```



Multiple virtual routers are often used in actual network applications.

Troubleshooting VRRP

As the configuration of VRRP is not very complicated, almost all the malfunctions can be found through viewing the configuration and debugging information. Here are some possible failures you might meet and the corresponding troubleshooting methods.

Fault 1: Frequent prompts of configuration errors on the console

This indicates that an incorrect VRRP packet has been received. It may be because of the inconsistent configuration of another switch within the virtual router, or the attempt of some devices to send out illegal VRRP packets. The first possible fault can be solved through modifying the configuration. And as the second possibility is caused by the malicious attempt of some devices, non-technical measures should be resorted to.

Fault 2: More than one Masters existing within the same virtual router

There are also 2 reasons. One is short time coexistence of many Master switches, which is normal and needs no manual intervention. Another is the long time coexistence of many Master switches, which may be because switches in the virtual router cannot receive VRRP packets from each other, or receive some illegal packets.

To solve such problems, an attempt should be made to ping among the many Master switches, and if such an attempt fails, check the device connectivity. If they can be pinged, check the VRRP configuration. For the configuration of the same VRRP virtual router, complete consistency for the number of virtual IP addresses, each virtual IP address, timer duration and authentication type must be guaranteed.

Fault 3: Frequent switchover of VRRP state

Such problem occurs when the virtual router timer duration is set too short. So the problem can be solved through prolonging this duration or configuring the preemption delay.

Introduction to HA

HA (high availability) is to achieve a high availability of the system and to recover the system as soon as possible in the event of fabric failures so as to shorten the MTBF (Mean Time Between Failure) of the system.

The functions of HA are mainly implemented by the application running on master and slave modules. The two modules are working in the master-slave mode: one module works in master mode, the other work in slave mode. If the master-slave system detects a fault in the master module, a hot master-slave switchover will be performed automatically. The slave module will try to connect and control the system bus while the original master module will try to disconnect from the bus. Thus, the master-slave switchover of the active system is completed, and at the same time the original master module is reset to recover as soon as possible and then function as the slave module. Even if the master module fails, the slave module can also take its role to ensure the normal operation, and the system can recover as soon as possible.

Switch 8800 Family series support hot swap of master and slave modules. The hot swap of master modules will cause master-slave switchover.

Switch 8800 Family series support manual master-slave switchover. You can change the current module state manually by executing command.

The configuration file of slave is copied from master module at the same time. This can ensure that the slave system continues to operate in the same configuration as that of the original active system after the slave system has taken place of the active system. Switch 8800 Family series support automatic synchronization. The active system stores its configuration file and backup the configuration file to the slave system simultaneously when the master's configuration file is modified, ensuring the consistency of the configurations of the active system and slave system.

Besides, the system can monitor the power supply and the working environment of the system and give timely alarms to avoid the escalation of failures and ensure safe operations of the system.



CAUTION: *The Switch 8800 Family active and standby modules must both be in position and run the same version of program. Otherwise, the switch cannot operate normally.*

Configuring HA

The following sections describe the HA configuration tasks:

- “Restarting the Slave System Manually”
- “Starting the Master-Slave Switchover Manually”

- “Enabling/Disabling Automatic Synchronization”
- “Synchronizing the Configuration File Manually”
- “Configuring the Load Mode of the Master and Slave Modules”

Restarting the Slave System Manually

In the environment in which the slave system is available, the user can restart the slave system manually.

Perform the following configuration in user view.

Table 602 Restart the slave system manually

Operation	Command
Restart the slave system manually	slave restart

Starting the Master-Slave Switchover Manually

In the environment in which the slave module is available and master in real-time backup state, the user can inform the slave module of a master-slave switchover by using a command if he expects the slave module to operate in place of the master module. After the switchover, the slave module will control the system and the original master module will be forced to reset.

Perform the following configuration in user view.

Table 603 Start the master-slave switchover manually

Operation	Command
Start the master-slave switchover manually	slave switchover

The switchover manually will be ineffective if user set the system forbid master-slave switchover manually.

Enabling/Disabling Automatic Synchronization

Switch 8800 Family series support automatic synchronization. The active system stores its configuration file and backup the configuration file to the slave system simultaneously when the master's configuration file is modified, ensuring the consistency of the configurations of the active system and slave system.

You can enable/disable automatic synchronize of Switch 8800 Family series.

Perform the following configuration in system view.

Table 604 Enable/Disable automatic synchronization

Operation	Command
Enable automatic synchronization	slave auto-update config
Disable automatic synchronization	undo slave auto-update config

By default, the automatic synchronization of system is enabled.

Synchronizing the Configuration File Manually

Although the system can perform the synchronization automatically, the synchronization can occur only when the master module saves its configuration file. If the user expects to determine the backup of the configuration file by

himself, he can do it manually to backup the configuration file saved in the master module.

Perform the following configuration in user view.

Table 605 Synchronize the configuration file manually

Operation	Command
Synchronize the configuration file manually	slave update configuration

This operation can backup the configuration file to the slave module only if a slave system is available. The configuration file will be fully copied once at every time the operation is executed.

Configuring the Load Mode of the Master and Slave Modules

Switch 8800 Family series support two kinds of load modes (balance and single) between the master and slave modules. You can use the **xbar** command to configure XBar (cross bar) load mode.

Perform the following configuration in system view.

Table 606 Configure the XBar load mode

Operation	Command
Configure the load mode of the master and slave modules	xbar [load-balance load-single]

By default, the load mode of the master and slave modules is **load-single**.



CAUTION: When a single fabric is in position, the load-balance mode is not effective and the fabric changes to the load-single mode automatically.

Displaying and Debugging HA Configuration

After the above configuration, execute **display** command in relevant view to display the running of the ACL configuration, and to verify the configuration. Execute **debugging** command in user view to enable HA module debugging function.

Perform the following configuration in relevant view.

Table 607 Display and debug HA configuration

Operation	Command
Display the status of the master and slave modules(any view)	display switchover state [slot-id]
Display the load mode of the master and slave modules(system view)	display xbar
Enable the debugging information output of the HA module(user view)	debugging ha { all event message state }
Disable the debugging information output of the HA module(user view)	undo debugging ha { all event message state }

HA Configuration Example**Network requirements**

Take the master module out and make the slave module take over the work of the master to ensure the normal operation.

Configuration procedure

Synchronize the configuration file manually.

```
<SW8800>slave update configuration
```

Display the switchover state.

```
<SW8800>display switchover state
```

Start the master-slave switchover manually after you confirm and press <Enter>.

```
<SW8800>slave switchover
```

```
Caution!!! Confirm to switch slave to master[Y/N]?y
```

Introduction to ARP

Address resolution protocol (ARP) is used to resolve an IP address into a MAC address.

Necessity of ARP

An IP address cannot be directly used for communication between network devices because network devices can identify only MAC addresses. An IP address is only an address of a host in the network layer. To send datagrams through the network layer to the destination host, the MAC address of the host is required. So the IP address must be resolved into a MAC address.

ARP implementation procedure

When two hosts on the Ethernet need to communicate with each other, they must know the MAC addresses of each other. Every host maintains the IP-MAC address translation table, which is known as the ARP mapping table. A series of mappings between IP addresses and MAC addresses of other hosts which recently communicate with the local host are stored in the ARP mapping table. When a dynamic ARP mapping entry is not in use for a specified period of time, the host removes it from the ARP mapping table so as to save the memory space and shorten the interval for the switch to search ARP mapping table.

Suppose there are two hosts on the same network segment: Host A and Host B. The IP address of Host A is IP_A and the IP address of Host B is IP_B. Host A needs to transmit messages to Host B.

ARP implementation procedure is as follows: Host A checks its own ARP mapping table first to know whether there are corresponding ARP entries of IP_B in the table. If the corresponding MAC address is found, Host A uses the MAC address in the ARP mapping table to encapsulate the IP packet in frame and sends it to Host B. If the corresponding MAC address is not found, Host A puts the IP packet into the send queue, create an ARP request packet and broadcast it throughout the Ethernet. The ARP request packet contains the IP address of Host B and IP address and MAC address of Host A. Since the ARP request packet is broadcasted, all hosts on the network segment can receive the request. However, only the requested host (namely, Host B) needs to process the request. Host B first stores the IP address and the MAC address of the request sender (Host A) in the ARP request packet in its own ARP mapping table. Then, Host B generates an ARP reply packet by adding its own MAC address into the packet, and then send it to Host A. The reply packet is directly sent to Host A in stead of being broadcasted. Receiving the reply packet, Host A extracts the IP address and the corresponding MAC address of Host B and adds them to its own ARP mapping table. Then Host A sends Host B all the packets standing in the queue.

Normally, dynamic ARP takes effect and automatically searches for the resolution from the IP address to the Ethernet MAC address without the help of an administrator.

ARP concepts

ARP entries used in Switch 8800 Family series routing switches include dynamic ARP entries and static ARP entries. Static entries are further divided into long static ARP entries and short static ARP entries.

- Dynamic ARP entries are automatically created and maintained by the ARP protocol through ARP packets. They can be discarded after the aging time expires, and updated by new ARP packets. They can also be overlaid by long static ARP entries and short static ARP entries. When the aging time expires, the port is disabled or the VLAN interface is disabled, dynamic ARP entries will be deleted.
- Static ARP entries are configured and maintained manually, including short ARP entries and long ARP entries.
- Long ARP entries contain all elements of an ARP entry. They can forward data directly. They cannot be aged, and overlaid by dynamic ARP entries.
- Short ARP entries are configured with IP addresses and MAC addresses only other than VLANs and egresses. They are generally used in users requiring IP address and MAC address binding. Its initial state is non-resolution, so it cannot forward data directly. It can resolve VLANs and egresses dynamically through ARP packets. A resolved static ARP entry can forward data and will not be aged. When the port and VLAN interface are disabled, a static ARP entry will be restored to the non-resolution state.

Configuring ARP

The ARP mapping table can be maintained dynamically or manually. Usually, the manually configured mapping from the IP addresses to the MAC addresses is known as static ARP. The user can display, add or delete the entries in the ARP mapping table through relevant manual maintenance commands.

The following sections describe static ARP configuration tasks:

- “Manually Adding/Deleting Static ARP Mapping Entries”
- “Configuring the Dynamic ARP Aging Timer”
- “Adding/Deleting Multicast ARP Ports”
- “ARP Proxy Configuration”
- “Gratuitous ARP Learning Configuration”
- “Configuring ARP Packets Not to Broadcast in VLAN”

Manually Adding/Deleting Static ARP Mapping Entries

Perform the following configuration in system view.

Table 608 Manually add/delete static ARP mapping entries

Operation	Command
Manually add a static ARP mapping entry	arp static <i>ip-address</i> [<i>mac-address</i> [<i>vlan-id</i> { <i>interface-type interface-number</i> }] [vpn-instance <i>vpn-instance-name</i>]]
Manually delete a static ARP mapping entry	undo arp <i>ip-address</i>

By default, the ARP mapping table is empty and the address mapping is obtained through dynamic ARP.

Note that:

- As long as a switch operates, its static ARP mapping entries remain valid unless you perform operations that make ARP invalid, such as change or remove VLAN virtual interfaces, remove a VLAN, or remove an interface from a VLAN. These operations cause the corresponding ARP mapping entries to be automatically removed.
- The *vlan-id* argument must be the ID of a VLAN that has been created by the user, and the Ethernet port specified behind this parameter must belong to the VLAN.
- The argument *vpn-instance-name* must be the VPN instance name of an existing MPLS VPN.
- ARP map entries with port parameters can be configured on manually aggregated ports or static aggregated ports, but cannot be configured on LACP-enabled dynamic aggregated ports.
- If the *mac-address* of an ARP entry is a multicast MAC address, the system will assume this ARP entry to be multicast ARP entry.
- Long static ARP can be configured only on manually aggregated ports, but not on static aggregated ported or dynamic aggregated ports.

Configuring the Dynamic ARP Aging Timer

For purpose of flexible configuration, the system provides the following commands to assign dynamic ARP aging period. When the system learns a dynamic ARP entry, its aging period is based on the current value configured.

Perform the following configuration in system view.

Table 609 Configure the dynamic ARP aging timer

Operation	Command
Configure the dynamic ARP aging timer	arp timer aging <i>aging-time</i>
Restore the default dynamic ARP aging time	undo arp timer aging

By default, the aging time of dynamic ARP aging timer is 20 minutes.

Adding/Deleting Multicast ARP Ports

The multicast ARP feature allows you to associate a common unicast route to a Layer 2 multicast group, that is, add multiple outgoing ports for an outgoing ARP packet so that the packet can be sent to multiple ports. As a result, a static multicast ARP entry is generated. In brief, a multicast ARP entry is a static ARP entry with a multicast MAC address, which may correspond to multiple ports.

According to the **multi-port** keyword in this command, the switch decides that the port to be added is for a multicast ARP entry. Only one port can be added every time the command is executed. If the multicast ARP entry does not exist, a new multicast ARP entry is generated. If the multicast ARP entry exists and the same egress exists, the switch will not add a multicast ARP port.

Perform the following configuration in system view.

Table 610 Add multicast ARP ports

Configuration step	Command	Description
Enter system view	system-view	-
Add multicast ARP ports	arp static <i>ip-address mac-address vlan-id</i> multi-port <i>interface-type interface-number</i> [vpn-instance <i>vpn-instance-name</i>]	-

To cancel the configuration, use the corresponding **undo** command.

After the configuration, you can use the **display arp multi-port** command in any view to check the detailed information about multicast ARP configuration.

**CAUTION:**

- You cannot configure multicast ARP for aggregation ports. Otherwise, the system will prompt error message.
- You cannot add a port in a multicast ARP entry to an aggregation group; if you want to do this, you must first delete the port from any multicast ARP entry it belongs to.
- At present, the outgoing ports in the same multicast ARP entry cannot be in different modules.
- Multicast static ARP can cover dynamic ARP, short static ARP and long static ARP, but not the other way around.

ARP Proxy Configuration

With the Super VLAN function enabled, the ARP proxy function is also needed to enable Layer 3 communications between sub-VLANs. If you enable the ARP proxy function for a network device that is connected to two networks simultaneously, the network device enables two ports in these two networks to communicate with each other on Layer 3 by forwarding ARP requests between the two networks even if the two ports are isolated from each other on Layer 2.



*You must enable **isolate-user-vlan** feature for all the devices connected to the VLAN with ARP proxy enabled.*

Table 611 Enable ARP proxy

Operation	Command	Description
Enter system view	system-view	-
Enter VLAN view	vlan <i>vlan-id</i>	<i>vlan-id</i> is the ID of a VLAN
Enable ARP proxy	arp proxy enable	By default, ARP proxy function is disabled.

Use the **undo** form of the command to cancel the configuration.

Gratuitous ARP Learning Configuration**Introduction to Gratuitous ARP Packets**

The following are the characteristics of gratuitous ARP packets:

- Both source and destination IP addresses carried in a gratuitous ARP packet are the local addresses, and the source MAC address carried in it is the local MAC addresses.

- If a device finds that the IP addresses carried in a received gratuitous packet conflict with those of its own, it returns an ARP response to the sending device to notify of the IP address conflict.

By sending gratuitous ARP packets, a network device can:

- Determine whether or not IP address conflicts exist between it and other network devices.
- Trigger other network devices to update its hardware address stored in their caches.

With the gratuitous ARP packet learning function enabled, a network device stores the ARP address carried in a received gratuitous ARP packet in its ARP address table if no ARP address in the cache of the network device matches the IP address carried by the gratuitous ARP packet. If the cache contains an ARP entry that matches the received gratuitous ARP packet, the switch updates the ARP entry using the hardware address of the sender carried in the gratuitous ARP packet. A switch operates like this whenever it receives an ARP packet.

Gratuitous ARP packet learning configuration

The following table lists the operations to configure the gratuitous ARP packet learning function.

Table 612 Configure the gratuitous ARP packet learning function

Operation	Command	Description
Enter system view	system-view	-
Enable the gratuitous ARP packet learning function	gratuitous-arp-learning enable	By default, the gratuitous ARP packet learning function is enabled.

Configuring ARP Packets Not to Broadcast in VLAN

In order to disable the mutual access function for two devices in the same network segment, you can manually control ARP packets and send them as trap packets to the CPU, so that ARP request packets will not be broadcast in the VLAN. Thus, the two devices cannot learn the addresses of each other from ARP packets and the function above is implemented.

Table 613 Configure non-flooding ARP request packets in VLAN

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	The port specified by the <i>interface-type</i> argument can be Ethernet port only
Enable ARP non-flooding in a VLAN	arp non-flooding enable	Required This function is disabled by default

Displaying and Debugging ARP

After the above configuration, execute the **display** command in any view to display the running of the ARP configuration, and to verify the effect of the configuration.

Execute the **reset** command in user view to clear ARP mapping table. Execute the **debugging** command in user view to debug ARP configuration.

Table 614 Display and debug ARP

Operation	Command
Display ARP mapping table	display arp [<i>ip-address</i>] [dynamic static] [[{ begin include exclude } <i>text</i>]]
Display the current setting of the dynamic ARP aging timer	display arp timer aging
Display multicast ARP configuration information	display arp multi-port [<i>ip-address</i>]
Display ARP proxy information	display arp proxy [vlan <i>vlan-id</i>]
Reset ARP mapping table	reset arp [dynamic static interface { <i>interface-type</i> <i>interface-number</i> } all]
Enable ARP information debugging	debugging arp { error info packet }
Disable ARP information debugging	undo debugging arp { error info packet }

Introduction to ARP Table Size Configuration

You can manually configure the maximum numbers of ARP entries (that is, the sizes of ARP tables) on an Switch 8800 Family routing switch to meet your actual needs.

The following table lists the specifications and numbers of ARP entries on various models.

Table 615 Numbers of ARP entries with different models

Model	IP address format and number of FIB entries supported	MPLS support	Maximum number of ARP entries supported by the whole switch if the card exists in the system	Maximum number of ARP entries supported by the card	Maximum number of aggregation ARP entries supported by the card
3C17511					
3C17512					
3C17513	IPv4-128K	Not supported	4K	4K	0K, 1K, 3K
3C17514					
3C17516					
3C17526					
3C17532	IPv4-128K/IPv6-7K				
3C17528	IPv4-128K/IPv6-64K				
3C17525					
3C17527	IPv4-256K	Supported	4K, 64K	4K, 5K, 6K, 7K, 8K	0K, 1K, 3K, 7K, 8K
3C17530					
3C17531					



CAUTION:

- After the configuration of a short static ARP entry, the system will include it into the number of non-aggregated ARP entries. If the short static ARP entry is resolved from a non-aggregated port, the number of non-aggregated ARP entries will remain unchanged; if the short static ARP entry is resolved from an aggregated port, it will be deducted from the number of non-aggregated ARP entries and included into the number of aggregation ARP entries.

- As a short static ARP entry is included into the number of normal ARP entries like a normal long static ARP entry, if a card is configured to support up to 8K aggregation ARP entries, the card does not support the configuration of neither kinds.

Configuring ARP Table Size Dynamically

Configuration Task Overview

The operations in configuring ARP table size dynamically include:

- Configuring the maximum number of ARP entries supported by a card
- Configuring the maximum number of aggregation ARP entries supported by a card
- Configuring the maximum number of ARP entries supported by the switch

Configuring ARP Table Size Dynamically

Table 616 Configure ARP table size dynamically

Operation	Command	Description
Enter system view	system-view	-
Configure the maximum number of ARP entries supported by a card	arp max-entry <i>slot-num</i> <i>max-num</i>	The maximum number of ARP entries supported by a card is 4K by default
Configure the maximum number of aggregation ARP entries supported by a card	arp max-aggregation-entry <i>max-aggnum</i>	The maximum number of aggregation ARP entries supported by a card is 1K by default
Configure the maximum number of ARP entries supported by the switch	arp enable size { 4 64 }	The maximum number of ARP entries supported by the whole switch is 4K by default

To cancel the configurations, use the corresponding **undo** commands.



CAUTION:

- Restart the system to make the above dynamic ARP configurations effective.
- After the ARP table size configuration, do not change cards or slots before you restart the system. Otherwise, the configuration above may fail to take effect.
- After the ARP table size configuration, do not perform active/standby switchover before you restart the system. Otherwise, the configuration will not take effect even if you restart the system.

Displaying ARP Table Size Configuration

After performing the above configurations, you can execute the **display** command in any view to display the maximum numbers of ARP entries to verify the configurations.

Table 617 Display ARP table size configuration

Operation	Command	Description
Display the current maximum numbers of ARP entries and the intending counterparts that will take effect after the switch is restarted next time	display arp max-entry	You can carry out the display command in any view.

Configuration Example

Network requirements

A host is connected to a Switch 8800 Family series routing switch and appropriate modules are installed

Network diagram

Figure 159 Diagram for ARP table size configuration

Configuration procedure

Configure the maximum number of ARP entries supported by the whole switch to 64K.

```

<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] arp enable size 64
The configuration won't be enable until the system is rebooted
  
```

Configure the maximum number of ARP entries supported by the interface card in slot 2 to 8K.

```

[SW8800] arp max-entry 2 8
The configuration won't be enable until the system is rebooted
  
```

Configure the maximum number of aggregation ARP entries supported by each interface card in the system to 8K.

```

[SW8800] arp max-aggregation-entry 8
The configuration won't be enable until the system is rebooted
  
```

Restart the system for the configurations to take effect.

Some Concepts about DHCP

DHCP Principles This is a world where networks are ever-growing in both size and complexity, and the network configuration is getting more and more complex. As is often the case, the number of hosts in a network exceeds that of the available IP addresses, and position changes of hosts (when users carry their laptops from here to there, or move to a wireless network) require reassigned new IP addresses. Dynamic host configuration protocol (DHCP) is designed to accommodate this context. DHCP adopts client/server model, where DHCP clients send requests to the DHCP server dynamically and the DHCP server in turn returns corresponding configuration information (such as IP addresses) according to the policies configured for it.

A typical DHCP implementation comprises a DHCP server and multiple DHCP clients (PCs or laptops). Figure 160 illustrates a network that employs DHCP.

Figure 160 Network diagram for DHCP

IP address assignment**1** IP address assignment policy

Different types of clients have different requirements for IP addresses. Servers usually require long-term fixed IP addresses, some hosts may require automatically assigned long-term fixed IP addresses, and some hosts may only require dynamically assigned temporary IP addresses.

A DHCP server provides three policies to meet these requirements.

- Manual IP address assignment. The administrator assigns fixed IP addresses to DHCP clients that are of special uses, such as a WWW server.

- Automatic IP address assignment. The DHCP server automatically assigns fixed IP addresses to DHCP clients when they connect to the network for the first time. After that, the IP addresses are always occupied by the DHCP clients.
 - Dynamic IP address assignment. The DHCP server leases IP addresses to DHCP clients for predetermined period of time and reclaims them at the expiration of the period. In this case, a DHCP client must reapply for an IP address regularly. This is the common case for normal users.
- 2 IP address assignment order.

The DHCP server assigns IP addresses except the forbidden ones to clients in the following orders.

- IP addresses in the address pool of the DHCP server that are statically bound to the MAC addresses of the DHCP clients.
 - IP addresses that are reclaimed by the DHCP server. That is, those in the Requested IP Addr Option fields of DHCP Discover packets sent by DHCP clients.
 - The first available IP address in the address pool the DHCP server finds.
 - The first expired or once conflicted IP address it finds. A DHCP server returns an error if it cannot find any available IP address from all these types of IP addresses when assigning an IP address.
- 3 Types of address pools of DHCP server
- Global address pool, valid for the entire switch. An address pool of this type is created using the **dhcp server ip-pool** command in system view.
 - VLAN interface address pool, valid for a specific VLAN interface. An address pool of this type is created by the system when the VLAN interface is configured with a legal unicast IP address and you specify to assign IP addresses in VLAN interface address pool using the **dhcp select interface** command in VLAN interface view. The address range of the available addresses is that of the network segment the VLAN interface resides.

Communications between DHCP clients and DHCP server

To obtain valid dynamic IP addresses, the DHCP clients exchange different information with the DHCP server in different phases. Usually, three modes are involved:

1 First round registration

A DHCP client goes through the following four steps when it accesses a network for the first time:

- Discovery. The DHCP client tries to find a DHCP server by broadcasting a DHCP_Discover packet in the network. (Only DHCP servers respond to this type of packet.)
- Provision. Each DHCP server that receives the DHCP_Discover packet selects an available IP address from an address pool and sends a DHCP_Offer packet that carries the selected IP address and other configuration information to the DHCP client.
- Selection. The DHCP client only receives the first arriving DHCP_Offer packet if there are DHCP_Offer packets from several DHCP servers. Then, it retrieves the

IP address carried in the packet, and broadcasts a DHCP_Request packet to each DHCP server. The packet contains the IP address carried by the DHCP_Offer packet.

- Acknowledgement. Upon receiving the DHCP_Request packet, the DHCP server that owns the IP address the DHCP_Request packet carries sends a DHCP_ACK packet to the DHCP client. And then the DHCP client binds TCP/IP protocol components to its network adapter.
- IP addresses offered by other DHCP servers (if any) through DHCP_Offer packets but not selected by the DHCP client are still available for other clients.

2 Second round registration

A second round registration goes through the following steps:

- After going through the first round registration successfully and logging out, when the DHCP client logs on to the network again, it directly broadcasts a DHCP_Request packet that contains the IP address assigned to it in the first round registration instead of a DHCP_Discover packet. .
- Upon receiving the DHCP_Request packet, if the IP address carried in the packet is still available, the DHCP server owning the IP address answers with a DHCP_ACK packet to enable the DHCP client to use the IP address again.
- If the IP address is not available (for example, it is occupied by other DHCP client), the DHCP server answers with a DHCP_NAK packet, which enables the DHCP client to go through steps in the first round registration.

3 Prolonging the lease time of IP address

An IP address assigned dynamically is valid for a specified lease time and will be reclaimed by the DHCP server when the time expires. So the DHCP client must update the lease to prolong the lease time if it is to use the IP address for a longer time.

By default, a DHCP client updates its IP address lease automatically by sending a DHCP_Request packet to the DHCP server when half of the lease time elapses. The DHCP server, in turn, answers with a DHCP_ACK packet to notify the DHCP client of the new lease.

BOOTP Relay Agent

Bootstrap protocol (BOOTP) relay agent is an Internet host or router that transports DHCP messages between the DHCP server and DHCP clients. BOOTP is designed for remote boot, mainly to notify the connected client about the location of the boot file.

DHCP is an extension of the BOOTP mechanism. This feature enables an existing BOOTP client to interoperate with the DHCP server without changing the installed software. RFC 1542 describes in detail the interactions among BOOTP, DHCP client and DHCP server.

DHCP and BOOTP Relay Agent

Like BOOTP, DHCP also works in the Client/Server mode. This protocol enables a DHCP client to request dynamically the DHCP server for the configuration information, including important parameters such as the allocated IP address, subnet mask, and default gateway, and the DHCP server can configure these parameters for the client conveniently.

DHCP provide a framework about how to set a host on a TCP/IP network. DHCP is derived from BOOTP, and possesses more function such as automatic allocation of reusable network addresses and additional configuration options. DHCP can act as a BOOTP relay agent, so a DHCP user and a BOOTP user can interact with each other.

The message format of DHCP is based on the message format of BOOTP, so that it can work as a relay agent and allow the coordination (interoperability) between existing BOOTP clients and the DHCP server. The use of a BOOTP relay agent makes it unnecessary to employ a DHCP server for every physical network segment.

DHCP defers from BOOTP in that:

- DHCP defines a mechanism through which a client can be allocated with a network address valid for a fixed lease period. In addition, it allows for continuous reallocation of network addresses to different clients.
- DHCP provides a mechanism through which a client is allowed to obtain all IP configuration parameter for subsequent operations.

Configuring General DHCP

General DHCP configuration refers to those that are applicable to both DHCP server and DHCP relay.

The following sections describe the general DHCP configuration tasks:

- “Enabling/Disabling DHCP Service”
- “Configuring Processing Method of DHCP Packets”
- “Enabling/Disabling Fake DHCP Server Detection”

Enabling/Disabling DHCP Service

For both DHCP server and DHCP relay, you must enable the DHCP service first before performing other DHCP configurations. The other related DHCP configurations take effect only after the DHCP service is enabled.

Perform the following configuration in system view.

Table 618 Enable/Disable DHCP service

Operation	Command
Enable DHCP service	dhcp enable
Disable DHCP service	undo dhcp enable

DHCP service is disabled by default.

Configuring Processing Method of DHCP Packets

You can perform the configurations listed in the following tables on your switch. After that, the switch processes the DHCP packets it received from DHCP clients in the methods you have configured.

Perform the following configuration in VLAN interface view to configure the processing method of DHCP packets for current VLAN interface.

Table 619 Configure the processing method for current VLN interface

Operation	Command
Specify to forward DHCP packets to local DHCP server and let the local server assign IP addresses in global address pools to DHCP clients	dhcp select global
Specify to forward DHCP packets to local DHCP server and let the local server assign IP addresses in VLAN interface address pool to DHCP clients	dhcp select interface
Specify to forward DHCP packets to remote DHCP servers. In this case, the current switch operates as a DHCP relay, and IP addresses are assigned by DHCP servers located in other networks	dhcp select relay
Revert to the default processing mode	undo dhcp select



CAUTION: The *dhcp select interface* command cannot be used together with the *ip relay address* or *dhcp relay security address-check enable* command.

Perform the following configuration in system view to configure the processing method of DHCP packets for multiple VLAN interfaces.

Table 620 Configure the processing method for multiple VLAN interfaces

Operation	Command
Specify to forward DHCP packets to local DHCP server and let the local server assign IP addresses in global address pools to DHCP clients	dhcp select global { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }
Specify to forward DHCP packets to local DHCP server and let the local server assign IP addresses in VLAN interface address pool to DHCP clients	dhcp select interface { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }
Specify to forward DHCP packets to remote DHCP servers. In this case, the current switch operates as a DHCP relay, and IP addresses are assigned by DHCP servers located in other networks	dhcp select relay { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }
Revert to the default processing mode	undo dhcp select { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }

By default, DHCP packets are processed in **global** method. That is, DHCP packets are forwarded to local DHCP server and IP addresses in global address pools are assigned.

Enabling/Disabling Fake DHCP Server Detection

If an unauthorized DHCP server exists in a network, it also answers when users in the network request IP addresses, and then interacts with the DHCP clients. This causes that the users cannot obtain correct IP addresses to access network. This kind of DHCP servers are known as fake DHCP servers.

With fake DHCP server detection enabled, the switch can record information (such as the IP addresses) about the DHCP servers. This helps administrators to detect fake DHCP servers in time and take proper measures.

Perform the following configuration in system view.

Table 621 Enable/Disable fake DHCP server detection

Operation	Command
Enable fake DHCP server detection	dhcp server detect
Disable fake DHCP server detection	undo dhcp server detect

Fake DHCP server detection is disabled by default.

Configuring DHCP Server

The following sections describe the DHCP server configuration tasks:

- “Creating a Global DHCP IP Address Pool”
- “Configuring IP Address Assignment Mode”
- “Forbidding Specified IP Addresses to Be Automatically Assigned”
- “Configuring Lease Time For DHCP Address Pool”
- “Configuring DHCP Client Domain Names”
- “Configuring DNS Server Address for DHCP Clients”
- “Configuring NetBIOS Server Address for DHCP Clients”
- “Configuring NetBIOS Node Type for DHCP Clients”
- “Configuring Custom DHCP Options”
- “Configuring Outbound Gateway Address for DHCP Clients”
- “Configuring Parameters for DHCP Server to Send Ping Packets”



Some of the above DHCP configurations can be performed for global IP address pools, IP address pool of current VLAN interface, or IP address pools of multiple specified VLAN interface respectively. They are:

- Configuring lease time for DHCP address pool
- Configuring DHCP client domain names
- Configuring DNS server address for DHCP clients
- Configuring NetBIOS server address for DHCP clients
- Configuring NetBIOS node type for DHCP clients
- Configuring DHCP custom options

Creating a Global DHCP IP Address Pool

An IP address pool contains IP addresses that can be assigned to DHCP clients. In response to DHCP request sent by a DHCP client, the DHCP server selects an appropriate IP address pool based on your configuration, choose an available IP address from the pool, and sends the IP address and other parameters (such as the lease time of the IP address) to the DHCP client. At present, you can configure up to 128 global DHCP address pools for a DHCP server.

The address pools of a DHCP server are hierarchically grouped like a tree. The root holds the IP address of the network segment, the branches hold the subnet IP addresses, and finally, the leaves hold the IP addresses of DHCP clients, which are manually bound to the corresponding network adapters. Such a structure enables configurations to be inherited. That is, configurations of the network segment can be inherited by its subnets, whose configurations in turn can be inherited by their clients. So, you can configure the parameters (such as domain name) that are

common to all levels in the address pool structure or some subnets only for the network segment or for corresponding subnets.

The **display dhcp server tree** command displays the tree-like structure of address pool, where address pools on the same level are sorted by the time they are created.

The **dhcp server ip-pool** command can be used to create a global DHCP address pool and enter the corresponding address pool view. If the address pool already exists, this command brings you to the address pool view directly.

Perform the following configuration in system view.

Table 622 Create a global DHCP address pool

Operation	Command
Create a DHCP address pool and enter the corresponding DHCP address pool view	dhcp server ip-pool <i>pool-name</i>
Remove a DHCP address pool	undo dhcp server ip-pool <i>pool-name</i>

By default, no global DHCP address pool is created.

Note that a VLAN interface address pool is created by the system after a legal unicast IP address is assigned to the VLAN interface and you specify to assign IP addresses in VLAN interface address pool by using the **dhcp select interface** command in VLAN interface view.

Configuring IP Address Assignment Mode

IP address can be assigned in two modes: static binding and dynamic assignment. You can statically bind an IP address in an address pool to the MAC address of a client or configure a address range to allow the DHCP server dynamic allocate the addresses in the range to DHCP clients. The two modes cannot coexist in a global DHCP address pool, but they can coexist in a VLAN interface address pool (but those that are dynamically assigned have the same network segment as that of the IP address of the VLAN interface).

For the dynamic assignment mode, you must specify the range of the addresses to be dynamically assigned. A global DHCP address pool whose IP addresses are statically bound to DHCP clients is actually a special kind of DHCP address pool.

Configuring static address binding for a global DHCP address pool

fixed IP address to the MAC address of a DHCP client who needs fixed IP address. After that, when the client requests for an IP address, the DHCP server finds (according to the MAC address) and assigns the fixed IP address to the client. At present, only one-to-one MAC-IP binding is supported for global DHCP address pool.

Perform the following configuration in DHCP address pool view.

Table 623 Configure static address binding for a global DHCP address pool

Operation	Command
Configure an IP address to be statically bound	static-bind ip-address <i>ip-address</i> [mask <i>netmask</i>]

Table 623 Configure static address binding for a global DHCP address pool

Operation	Command
Free a statically bound IP address	undo static-bind ip-address
Configure a MAC address to be statically bound	static-bind mac-address <i>mac-address</i>
Free a statically bound MAC address	undo static-bind mac-address

IP addresses in a global DHCP address pool are not statically bound by default.



The **static-bind ip-address** command and the **static-bind mac-address** command must be used together as a pair when you configure static binding entries. When you re-execute the command pair with the same IP address/MAC address, the newly configured IP address/MAC address overwrites the existing one.

Configuring static address binding for a VLAN interface address pool

At present, a VLAN interface DHCP address pool supports one-to-multiple MAC-IP address binding.

Perform the following configuration in VLAN interface view.

Table 624 Configure static address binding for a VLAN interface address pool

Operation	Command
Configure static address binding for the current VLAN interface address pool	dhcp server static-bind ip-address <i>ip-address</i> mac-address <i>mac-address</i>
Remove a statically bound IP address entry	undo dhcp server static-bind { ip-address <i>ip-address</i> mac-address <i>mac-address</i> }

IP addresses in the address pool of a VLAN interface are not statically bound by default.



CAUTION: A binding in a VLAN interface address pool cannot be overwritten directly. If an IP-to-MAC address binding entry is configured and you want to modify it, you must remove it and redefine a new one.

Configuring dynamic IP address assignment

If you specify to assign IP addresses dynamically, that is, IP addresses are leased permanently or temporarily, you need to configure an available address range.

Perform the following configuration in DHCP address pool view.

Table 625 Configure an address range for dynamic IP address assignment

Operation	Command
Configure an address range for dynamic IP address assignment	network <i>ip-address</i> [mask <i>netmask</i> <i>mask-length</i>]
Remove an dynamic assignment address range	undo network

By default, no IP address range is configured for dynamic IP address assignment.

Each DHCP address pool can be configured with only one address range. If you execute the **network** command multiple times, then only the last configured address range works.



CAUTION: When addresses are obtained through DHCP Relay, the subnet mask of the normal address pool, the global binding address pool and the Relay address must be the same. Otherwise, the binding will fail, or the address assigned to the client will not be in the same network segment with the Relay address.

Forbidding Specified IP Addresses to Be Automatically Assigned

You can use the command here to prevent a DHCP server from assigning IP addresses that are already occupied by such network devices as gateways and file transfer protocol (FTP) servers to other DHCP clients to avoid IP address conflicts.

Perform the following configuration in system view.

Table 626 Forbid specified IP addresses to be automatically assigned

Operation	Command
Forbid specified IP addresses to be automatically assigned	dhcp server forbidden-ip <i>low-ip-address</i> [<i>high-ip-address</i>]
Cancel the forbiddance	undo dhcp server forbidden-ip <i>low-ip-address</i> [<i>high-ip-address</i>]

All IP addresses in a DHCP address pool can be automatically assigned by default.

You can set multiple IP address ranges that are not assigned automatically by executing the **dhcp server forbidden-ip** command multiple times.

Configuring Lease Time For DHCP Address Pool

You can configure different lease times for different DHCP address pools. But you can configure only one lease time for one DHCP address pool and all the address in the same pool will have the same lease time.

Configuring a lease time for a global DHCP address pool

Perform the following configuration in DHCP address pool view.

Table 627 Configure a lease time for a global DHCP address pool

Operation	Command
Configure a lease time for a global DHCP address pool	expired { <i>day day</i> [<i>hour hour</i> [<i>minute minute</i>]] unlimited }
Restore the lease time of a global DHCP address pool to the default value	undo expired

Configuring a lease time for current VLAN interface

Perform the following configuration in VLAN interface view.

Table 628 Configure a lease time for current VLAN interface

Operation	Command
Configure a lease time for DHCP address pool of current VLAN interface	dhcp server expired { <i>day day</i> [<i>hour hour</i> [<i>minute minute</i>]] unlimited }
Restore the lease time of DHCP address pool of current VLAN interface to the default value	undo dhcp server expired

Configuring a lease time for multiple VLAN interfaces

Perform the following configuration in system view.

Table 629 Configure a lease time for multiple VLAN interfaces

Operation	Command
Configure a lease time for DHCP address pools of multiple VLAN interfaces	dhcp server expired { day <i>day</i> [hour <i>hour</i> [minute <i>minute</i>]] } unlimited } { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }
Restore the lease time of DHCP address pools of multiple VLAN interfaces to the default value	undo dhcp server expired { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }

The default lease times for global address pools and VLAN interface address pools are all one day.

Configuring DHCP Client Domain Names

You can configure a domain name used by DHCP clients for each address pool on a DHCP server.

Configuring a DHCP client domain name for a global DHCP address pool

Perform the following configuration in DHCP address pool view.

Table 630 Configure a DHCP client domain name for a global DHCP address pool

Operation	Command
Configure a DHCP client domain name for a global DHCP address pool	domain-name <i>domain-name</i>
Remove the DHCP client domain name configured for a global DHCP address pool	undo domain-name

Configuring a DHCP client domain name for current VLAN interface

Perform the following configuration in VLAN interface view.

Table 631 Configure a DHCP client domain name for current VLAN interface

Operation	Command
Configure a DHCP client domain name for the DHCP address pool of the current VLAN interface	dhcp server domain-name <i>domain-name</i>
Remove the DHCP client domain name configured for the DHCP address pool of the current VLAN interface	undo dhcp server domain-name

Configuring a DHCP client domain name for multiple VLAN interfaces

Perform the following configuration in system view.

Table 632 Configure a DHCP client domain name for multiple VLAN interfaces

Operation	Command
Configure a DHCP client domain name for DHCP address pools of multiple VLAN interfaces	dhcp server domain-name <i>domain-name</i> { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }
Remove the DHCP client domain name configured for DHCP address pools of multiple VLAN interfaces	undo dhcp server domain-name <i>domain-name</i> { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }

By default, global address pools and VLAN interface address pools are not configured with any DHCP client domain name.

If you execute the **dhcp server domain-name** command multiple times, the newly configured DHCP client domain name overwrites the existing one.

Configuring DNS Server Address for DHCP Clients

When a host uses a domain name to access the Internet, the domain name must be translated into an IP address. Domain name system (DNS) is responsible for the translation. Therefore, when a DHCP server assigns an IP address to a DHCP client, it must also send a DNS server address to the client. At present, you can configure up to eight DNS server addresses for one DHCP address pool.

Configuring DNS server address for a global DHCP address pool

Perform the following configuration in DHCP address pool view.

Table 633 Configure DNS server address for a global DHCP address pool

Operation	Command
Configure one or more DNS server addresses for a global DHCP address pool	dns-list <i>ip-address</i> [<i>ip-address</i>]
Remove one or all DNS server addresses configured for a global DHCP address pool	undo dns-list { <i>ip-address</i> all }

Configuring DNS server address for current VLAN interface

Perform the following configuration in VLAN interface view.

Table 634 Configure DNS server address for current VLAN interface

Operation	Command
Configure one or more DNS server addresses for the DHCP address pool of the current VLAN interface	dhcp server dns-list <i>ip-address</i> [<i>ip-address</i>]
Remove one or all DNS server addresses configured for the DHCP address pool of the current VLAN interface	undo dhcp server dns-list { <i>ip-address</i> all }

Configuring DNS server address for multiple VLAN interfaces

Perform the following configuration in system view.

Table 635 Configure DNS server address for multiple VLAN interfaces

Operation	Command
Configure one or more DNS server addresses for the DHCP address pools of multiple VLAN interfaces	dhcp server dns-list <i>ip-address</i> [<i>ip-address</i>] { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }
Remove one or all DNS server addresses configured for the DHCP address pools of multiple VLAN interfaces	undo dhcp server dns-list { <i>ip-address</i> all } { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }

By default, no DNS server address is configured for global and VLAN interface address pools.

If you execute the **dhcp server dns-list** command multiple times, the newly configured IP addresses overwrite the existing ones.

Configuring NetBIOS Server Address for DHCP Clients

For clients running a Windows operating system and communicating through the NetBIOS protocol, translations between host name and IP address are carried out by Windows Internet Naming Service (WINS) servers. So you need to perform configurations concerning WINS for these clients. At present, you can configure up to eight NetBIOS server addresses for a DHCP address pool.

Configuring NetBIOS server address for a global DHCP address pool

Perform the following configuration in DHCP address pool view.

Table 636 Configure NetBIOS server address for a global DHCP address pool

Operation	Command
Configure one or more NetBIOS server addresses for a global DHCP address pool	nbns-list <i>ip-address</i> [<i>ip-address</i>]
Remove one or all NetBIOS server addresses configured for a global DHCP address pool	undo nbns-list { <i>ip-address</i> all }

Configuring NetBIOS server address for current VLAN interface

Perform the following configuration in VLAN interface view.

Table 637 Configure NetBIOS server address for current VLAN interface

Operation	Command
Configure one or more NetBIOS server addresses for the DHCP address pool of current VLAN interface	dhcp server nbns-list <i>ip-address</i> [<i>ip-address</i>]
Remove one or all NetBIOS server addresses configured for the DHCP address pool of the current VLAN interface	undo dhcp server nbns-list { <i>ip-address</i> all }

Configuring NetBIOS server address for multiple VLAN interfaces

Perform the following configuration in system view.

Table 638 Configure NetBIOS server address for multiple VLAN interfaces

Operation	Command
Configure one or more NetBIOS server addresses for the DHCP address pools of multiple VLAN interfaces	dhcp server nbns-list <i>ip-address</i> [<i>ip-address</i>] { interface <i>vlan-interface</i> <i>vlan-id</i> [to <i>vlan-interface</i> <i>vlan-id</i>] all }
Remove one or all NetBIOS server addresses configured for the DHCP address pools of multiple VLAN interfaces	undo dhcp server nbns-list { <i>ip-address</i> all } { interface <i>vlan-interface</i> <i>vlan-id</i> [to <i>vlan-interface</i> <i>vlan-id</i>] all }

By default, no NetBIOS server address is configured for global and VLAN interface address pools.

If you execute the **dhcp server nbns-list** command multiple times, the newly configured IP addresses overwrite the existing ones.

Configuring NetBIOS Node Type for DHCP Clients

For DHCP clients communicating in wide area network (WAN) by NetBIOS protocol, the mapping between their host names and IP addresses must be established. According to the ways they establish their mappings, NetBIOS nodes fall into the following four types:

- b-node: Nodes of this type establish their mappings by broadcasting. (b stands for broadcast.)

- p-node: Nodes of this type establish their mappings by communicating with NetBIOS server. (p stands for peer-to-peer.)
- m-node: Nodes of this type are p nodes which take some broadcast features. (m stands for mixed.)
- h-node: Nodes of this type are b nodes which take peer-to-peer mechanism. (h stands for hybrid.)

Configuring NetBIOS node type for a global DHCP address pool

Perform the following configuration in DHCP address pool view.

Table 639 Configure a NetBIOS node type for a global DHCP address pool

Operation	Command
Configure the NetBIOS node type for a global DHCP address pool	netbios-type { b-node h-node m-node p-node }
Cancel the NetBIOS node type configuration for a global DHCP address pool	undo netbios-type

Configuring NetBIOS node type for current VLAN interface

Perform the following configuration in VLAN interface view.

Table 640 Configure a NetBIOS node type for current VLAN interface

Operation	Command
Configure the NetBIOS node type for DHCP clients of the current VLAN interface DHCP address pool	dhcp server netbios-type { b-node h-node m-node p-node }
Remove NetBIOS node type configured for DHCP clients of the current VLAN interface DHCP address pool	undo dhcp server netbios-type

Configuring NetBIOS node type for multiple VLAN interfaces

Perform the following configuration in system view.

Table 641 Configure a NetBIOS node type for multiple VLAN interfaces

Operation	Command
Configure NetBIOS node types for DHCP clients of multiple VLAN interface DHCP address pools	dhcp server netbios-type { b-node h-node m-node p-node } { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }
Remove NetBIOS node type configurations of multiple VLAN interface DHCP address pools	undo dhcp server netbios-type { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }

By default, the DHCP clients of global and VLAN interface address pools are all of h-node type.

Configuring Custom DHCP Options

With the evolvement of DHCP, new options come forth continuously. To utilize these options, you can manually add them to the property list of a DHCP server.

Configuring custom DHCP options for a global DHCP address pool

Perform the following configuration in DHCP address pool view.

Table 642 Configure a custom DHCP options for a global DHCP address pool

Operation	Command
Configure a custom DHCP option for a global DHCP address pool	option code { ascii <i>ascii-string</i> hex <i>hex-string</i> ip-address <i>ip-address</i> [<i>ip-address</i>] }
Remove a custom DHCP option configured for a global DHCP address pool	undo option code

Configuring custom DHCP options for current VLAN interface

Perform the following configuration in VLAN interface view.

Table 643 Configure custom DHCP options for current VLAN interface

Operation	Command
Configure a custom DHCP option for DHCP address pool of the current VLAN interface	dhcp server option code { ascii <i>ascii-string</i> hex <i>hex-string</i> ip-address <i>ip-address</i> [<i>ip-address</i>] }
Remove a custom DHCP option configured for the DHCP address pool of the current VLAN interface	undo dhcp server option code

Configuring custom DHCP options for multiple VLAN interfaces

Perform the following configuration in system view.

Table 644 Configure custom DHCP options for multiple VLAN interfaces

Operation	Command
Configure a custom DHCP option for DHCP address pools of multiple VLAN interfaces	dhcp server option code { ascii <i>ascii-string</i> hex <i>hex-string</i> ip-address <i>ip-address</i> [<i>ip-address</i>] } { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }
Remove a custom DHCP option configured for DHCP address pools of multiple VLAN interfaces	undo dhcp server option code { interface vlan-interface <i>vlan-id</i> [to vlan-interface <i>vlan-id</i>] all }

If you execute the **dhcp server option** command multiple times, the newly configured option overwrites the existing one.

Configuring Outbound Gateway Address for DHCP Clients

An outbound gateway enables DHCP clients to access external network devices. Packets destined for external networks are forwarded by outbound gateways. At present, you can configure up to eight IP addresses for outbound gateways.

Perform the following configuration in DHCP address pool view.

Table 645 Configure outbound gateway address for DHCP clients

Operation	Command
Configure one or more outbound gateway addresses for DHCP clients	gateway-list <i>ip-address</i> [<i>ip-address</i>]
Remove one or all outbound gateway addresses configured for DHCP clients	undo gateway-list { <i>ip-address</i> all }

By default, no outbound gateway address is configured for DHCP clients.

If you execute the **gateway-list** command multiple times, the newly configured IP addresses overwrite the existing ones.

Configuring Parameters for DHCP Server to Send Ping Packets

To avoid address conflict caused by reassigning an in-use IP address, before assigning an IP address to a DHCP client, the DHCP server detects the network using the **ping** instructions to ensure the IP address is not occupied. The DHCP server determines whether an IP address is reachable by sending specified number of ping packets. It waits for response packet for a specified period after sending each of these packets. If the DHCP server receives no response after sending all these packets, it considers the IP address is not used by other devices in this network and assigns the IP address to this DHCP client. Otherwise, it does not assign the IP address.

Perform the following configuration in system view.

Table 646 Configure parameters for DHCP server to send ping packets

Operation	Command
Set the maximum number of ping packets the DHCP is allowed to send	dhcp server ping packets <i>number</i>
Revert to the default maximum number	undo dhcp server ping packets
Set the maximum duration for the DHCP server to wait for response to a ping packet	dhcp server ping timeout <i>milliseconds</i>
Revert to the default maximum duration	undo dhcp server ping timeout

By default, the DHCP server sends up to 2 ping packets to test an IP address and waits for a response for up to 500 milliseconds before it sends another ping packet.

Note that the DHCP server detects address conflict by ping packets, whereas a DHCP client does this by ARP packets.

Displaying and Debugging the DHCP Server

After the above configuration, you can execute the **display** command in any view to display operating information about the DHCP server to verify your configuration, and execute the **debugging** command to enable debugging for the DHCP server

Execute the following command in any view.

Table 647 Display the configuration information about the DHCP server

Operation	Command
Display the statistics about DHCP address conflicts	display dhcp server conflict { all ip <i>ip-address</i> }
Display information about lease-expired addresses in DHCP address pool(s). The lease-expired IP addresses in an address pool are assigned to other DHCP clients as needed if the address pool runs out of its available IP addresses	display dhcp server expired { ip <i>ip-address</i> pool [<i>pool-name</i>] interface [vlan-interface <i>vlan-id</i>] all }
Display the ranges of available (unassigned) IP addresses in DHCP address pools	display dhcp server free-ip

Table 647 Display the configuration information about the DHCP server

Operation	Command
Display the forbidden IP addresses in the DHCP address pool	display dhcp server forbidden-ip
Display the information about IP address binding in DHCP address pool(s)	display dhcp server ip-in-use { ip <i>ip-address</i> pool [<i>pool-name</i>] interface [vlan-interface <i>vlan-id</i>] all }
Display the statistics about the DHCP server	display dhcp server statistics
Display the information about the tree-like structure of DHCP address pool(s)	display dhcp server tree { pool [<i>pool-name</i>] interface [vlan-interface <i>vlan-id</i>] all }

Perform the following configuration in user view.

Table 648 Enable/Disable debugging for the DHCP server

Operation	Command
Disable debugging for the DHCP server	undo debugging dhcp server { all error event packet }
Enable debugging for the DHCP server	debugging dhcp server { all error event packet }

Clearing the Configuration Information of the DHCP Server

You can clear the configuration information of the DHCP server by executing the **reset** command in user view.

Perform the following configuration in user view.

Table 649 Clear the configuration information of the DHCP server

Operation	Command
Clear the statistics about DHCP address conflicts	reset dhcp server conflict { ip <i>ip-address</i> all }
Clear the information about dynamically bound DHCP addresses	reset dhcp server ip-in-use { all interface [vlan-interface <i>vlan-id</i>] ip <i>ip-address</i> pool [<i>pool-name</i>] }
Clear the statistics about the DHCP server	reset dhcp server statistics

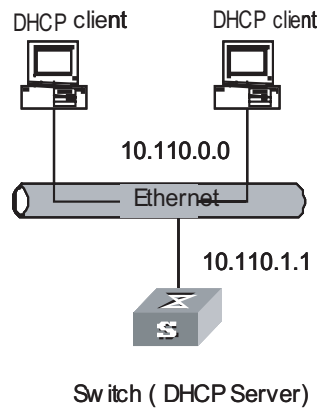
DHCP Server Configuration Example

Network requirements

As shown in Figure 161, two DHCP clients at the same network segment (10.110.0.0) are connected to the following switch through a port in VLAN2. The switch, acting as a DHCP server, is supposed to assign IP addresses to the two DHCP clients without the help of any DHCP Relay.

Network diagram

Figure 161 Network diagram for DHCP server



Configuration procedure

Enter system view.

```
<SW8800>system-view
```

Create VLAN2.

```
[SW8800]vlan 2
```

Enter VLAN interface view and create Vlan-interface 2.

```
[SW8800]interface Vlan-interface 2
```

Assign an IP address to Vlan-interface 2.

```
[3Com-Vlan-interface2]ip address 10.110.1.1 255.255.0.0
```

Specify to assign IP addresses in the interface address pool to DHCP clients.

```
[3Com-Vlan-interface2]dhcp select interface
```

Specify to assign IP addresses in global address pool to DHCP clients (it is also the default configuration).

```
[3Com-Vlan-interface2]dhcp select global
```

Or execute the following command to revert to the default.

```
[3Com-Vlan-interface2]undo dhcp select
```

Configure a global address pool.

```
[8505Tlhy]dhcp server ip-pool 1
[8505Tlhy-dhcp-1]network 10.110.0.0 mask 255.255.0.0
[8505Tlhy-dhcp-1]gateway-list 10.110.1.1
```

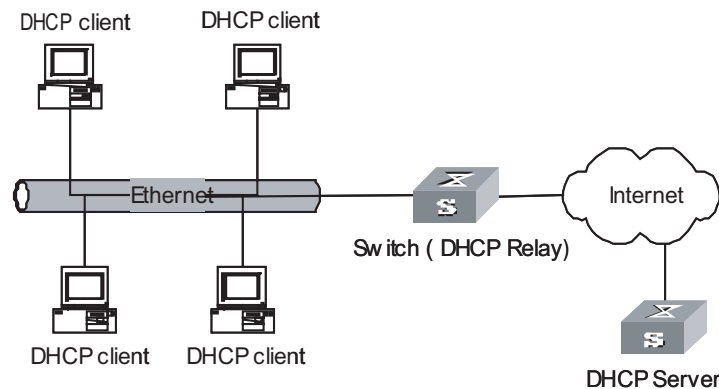
Configuring DHCP Relay

Introduction to DHCP Relay

This is a world where networks are ever-growing in both size and complexity, and the network configuration is getting more and more complex. As is often the case, the number of hosts in a network exceeds that of the available IP addresses, and position changes of hosts (when users carry their laptops from here to there, or move to a wireless network) require reassigned new IP addresses. Dynamic host configuration protocol (DHCP) is designed to accommodate this context. DHCP adopts client/server model, where DHCP clients send requests to the DHCP server dynamically and the DHCP server in turn returns corresponding configuration information according to the policies configured for it.

Early implementations of DHCP only work when DHCP clients and DHCP servers are in the same subnet. That is, they cannot work across networks. So, to implement dynamic host configuration, you must deploy at least one DHCP server in each subnet, and this is obviously uneconomical. DHCP Relay is designed to resolve this problem. Through a DHCP relay, DHCP clients in a LAN can communicate with DHCP servers in other subnets to acquire IP addresses. This enables DHCP clients of multiple networks to share a common DHCP server and thus enables you to save your cost and perform centralized administration. Figure 162 illustrates a typical DHCP Relay application.

Figure 162 Network diagram for DHCP Relay



The dynamic host configuration procedure with DHCP relay is as follows:

- A DHCP client broadcasts configuration request packet in the local network when it starts up and initializes the configuration.
- If a DHCP server exists in the network, it processes the configuration request packet directly without the help of a DHCP Relay.
- If no DHCP server exists in the network, the network device serving as a DHCP Relay in the network appropriately processes the configuration request packet and forwards it to a specified DHCP server located in another network.
- After receiving the packet, the DHCP server generates configuration information accordingly and sends it to the DHCP client through the DHCP Relay to complete the dynamic configuration of the DHCP client.

Note that the entire configuration procedure may go through multiples times of such interactions.

Configuring DHCP Relay

DHCP Relay configuration includes the following: The following text describes the DHCP Relay configuration tasks:

- “Configuring a DHCP server for a VLAN interface”
- “Configure user address entries for a DHCP Relay”
- “Enable/Disable DHCP security on a VLAN interface”

Configuring a DHCP server for a VLAN interface

You can execute the **ip relay address** command to configure the DHCP packet processing mode on VLAN interface as relay and a corresponding DHCP server for a VLAN interface.

Perform the following configuration in VLAN interface view.

Table 650 Configure a corresponding DHCP server for a VLAN interface

Operation	Command
Configure a corresponding DHCP server for current VLAN interface	ip relay address <i>ip-address</i>
Remove the DHCP server configured for current VLAN interface	undo ip relay address { <i>ip-address</i> all }

No DHCP server is configured for a VLAN interface by default.

Note that when configuring a new DHCP server for a VLAN that already has a DHCP server configured for it, the newly configured one does not overwrite the existing ones. Both the new and the old ones are valid. You can configure up to 20 DHCP server addresses for a VLAN interface.



CAUTION: *The IP address of the intended DHCP server for the DHCP relay feature cannot be IP address of the VLAN interface corresponding to the DHCP relay. Otherwise, the system gives the information such as "Can't set ip relay address as interface address on interface Vlan-interface 100!".*

Configure user address entries for a DHCP Relay

In a VLAN that has DHCP Relay configured, to enable a DHCP client using a legal fixed IP address to pass the address checking of the DHCP security feature, you must add a static address entry for the DHCP client. A static address entry indicates the relation between a fixed IP address and a MAC address.

Perform the following configuration in system view or in VLAN interface view.

Table 651 Configure user address entries for DHCP relay

Operation	Command
Add a user address entry for DHCP relay	dhcp relay security <i>ip-address mac-address static</i>
Remove a user address entry for DHCP relay	undo dhcp relay security <i>ip-address</i>



- The DHCP client applies for an IP address through the DHCP relay. When the packet from DHCP client passes the DHCP relay, the DHCP relay adds its primary IP address in the packet and forwards the packet to the DHCP server. When receiving the packet, DHCP server allocates an IP address in the same segment as the IP address added by the DHCP relay.
- If there is a local DHCP Server, when the DHCP Client applies for IP addresses, it can be assigned with only the address which is in the same network segment with the primary IP address of the interface connecting the client to the server. The client cannot be assigned with the address which is in the same network segment with the secondary IP address of the interface connecting the client to the server.
- If there is no local DHCP Server, when the DHCP client applies for IP address through Relay, the DHCP Serer can be assigned with only the address which is in the same network segment with the primary IP address of the Relay. The DHCP Server cannot be assigned with the address which is in the same network segment with the secondary IP address of the Relay.

Enable/Disable DHCP security on a VLAN interface

If you enable the DHCP security feature on a VLAN interface, the switch performs user address checking on the VLAN interface to prevent unauthorized binding request. If you disable the DHCP security feature on a VLAN interface, the switch does not perform user address checking on the VLAN interface.

Perform the following configuration in VLAN interface view.

Table 652 Enable/disable DHCP security on a VLAN interface

Operation	Command
Enable DHCP security on a VLAN interface	dhcp relay security address-check enable
Disable DHCP security on a VLAN interface	dhcp relay security address-check disable

The DHCP security feature is disabled on a VLAN interface by default.



CAUTION: After the DHCP security feature is enabled on a VLAN interface, the client that has already obtained an IP address will lose its access right and has to apply for an IP address again. Therefore, it is recommended that the administrator should conduct this configuration before any user has obtained an IP address.

Displaying and Debugging DHCP Relay

After the above configuration, you can execute the **display** command in any view to display running information about DHCP Relay to verify your configuration.

Execute the **debugging** command in user view to debug DHCP Relay.

Table 653 Display and debug DHCP Relay

Operation	Command
Display information about the DHCP relay configured for VLAN interface	display dhcp relay address { interface vlan-interface <i>vlan-id</i> all }
Display information about legal user address entries for DHCP relay	display dhcrelay-security [<i>ip-address</i>]

Table 653 Display and debug DHCP Relay

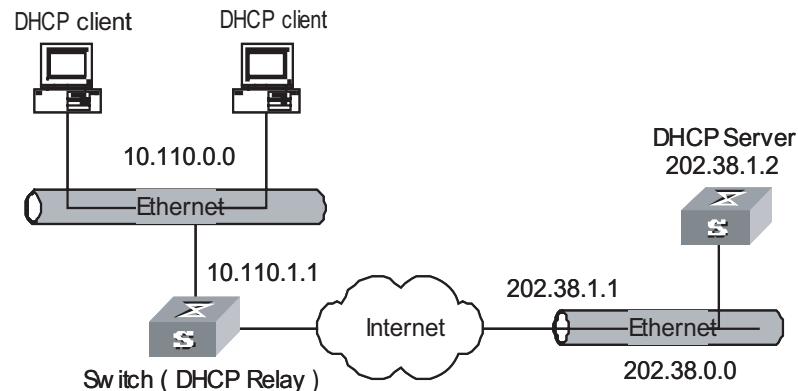
Operation	Command
Enable debugging for DHCP Relay	debugging dhcp relay { all packet error event }
Disable debugging for DHCP Relay	undo debugging dhcp relay { all packet error event }

DHCP Relay Configuration Example

Network requirements

As shown in Figure 163, two DHCP clients located at the same network segment (10.110.0.0) are connected to a switch through a port in VLAN 2. The switch, acting as a DHCP relay, is supposed to forward DHCP packets between the two DHCP clients and the DHCP server with the IP address of 202.38.1.2.

Network diagram

Figure 163 Network diagram for DHCP Relay

Configuration procedure

Enter system view.

```
<SW8800>system-view
```

Create VLAN 2.

```
[SW8800]vlan 2
```

Create Vlan-interface 2 and enter VLAN interface view.

```
[SW8800]interface Vlan-interface 2
```

Assign an IP address to Vlan-interface 2.

```
[3Com-Vlan-interface2]ip address 10.110.1.1 255.255.0.0
```

Specify to forward DHCP packets to a remote DHCP server.

```
[3Com-Vlan-interface2]dhcp select relay
```

Configure the IP address of the DHCP server to which VLAN 2 sends DHCP packets.

```
[3Com-Vlan-interface2]ip relay address 202.38.1.2
```



Besides the above configurations for DHCP Relay, you need to configure address pool on the DHCP server and make sure the DHCP server and the switch interface connecting the two DHCP clients is routing reachable with each other.



CAUTION: Do not change or delete the IP address of the interface corresponding to the DHCP Relay; otherwise users will be unable to obtain IP addresses to access the Internet.

DHCP Option 82 Configuration

Introduction to Option 82 Support on DHCP Relay

Option 82 is the relay agent information option in the DHCP packets. When a DHCP client sends a DHCP request packet and the packet must be forwarded by a DHCP relay to reach a DHCP server, if Option 82 support is enabled on the DHCP relay, the DHCP relay adds Option 82 into the request packet. Option 82 can be composed of many sub-options, but Option 82 mentioned in this chapter only supports sub-option 1, sub-option 2 and sub-option 5. Sub-option 1 defines the agent circuit ID (that is, Circuit ID), and sub-option 2 defines the agent remote ID (that is, Remote ID). sub-option 5 is the subitem of link selection, which includes the IP address that the DHCP Relay adds.

With Option 82, the information about the addresses of the DHCP clients and the DHCP relay devices can be recorded on the DHCP server. Using Option 82 together with other software can implement the DHCP allocation restrictions and the accounting function.

Concepts

■ Option

A DHCP packet has a field called options, which contains part of the lease information and the packet type. The options field is length-variable and consists of one option at least and 255 options at most.

■ Option 82

Option 82 is also called relay agent information option and is a part of the options field in a DHCP packet. Option 82 is defined in RFC 3046 before Option 255 and behind other options. You can define a minimum of one sub-option and a maximum of 255 sub-options for Option 82. At present, the commonly used sub-options in Option 82 include sub-option 1, sub-option 2 and sub-option 5.

■ sub-option 1

Sub-option 1 belongs to Option 82 and defines the Circuit ID. Usually configured on the DHCP relay devices, it indicates that the forwarded packets will carry the VLAN ID and Layer 2 port number of the port of the switch that the DHCP client is connected to. Generally, sub-option 1 and sub-option 2 are used together to identify a DHCP client.

■ Sub-option 2

Sub-option 2 also belongs to Option 82 and defines the Remote ID. Usually configured on the DHCP relay devices, it indicates that the forwarded packets will carry the MAC address of the relay device. Generally, sub-option 1 and sub-option 2 are used together to identify a DHCP client.

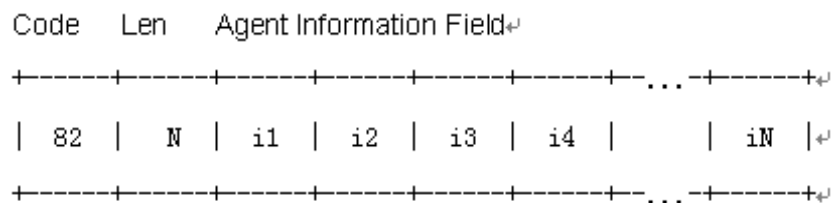
- Sub-option 5

Sub-option 5 also belongs to Option 82 and defines the link selection. It contains an IP address which is added by the DHCP relay, so that the DHCP server can assign to the DHCP client an IP address that is in the same network segment with this address.

Option 82 Structure

There is a field named options in the DHCP packets. It can be null or contains at least one feature-specific option, such as Option 82 which may comprise multiple sub-options. Figure 164 illustrates the structure of Option 82.

Figure 164 Option 82 structure

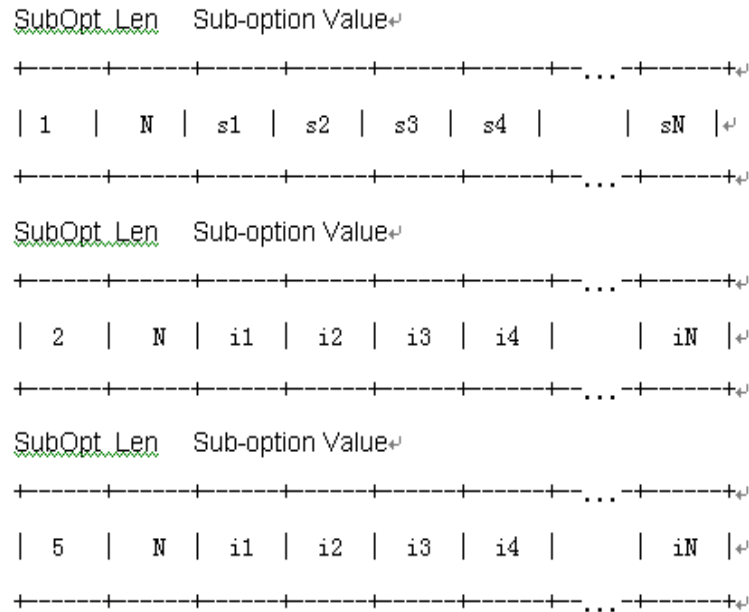


Code: Identifies the number of the relay agent information option. It is 82 in the packet, which represents Option 82. Option 82 is before Option 255 and is behind other options in RFC 3046.

Len: Indicates the length of the Agent Information Field.

Agent Information Field: Specifies the available sub-options.

Sub-option packet structure: Figure 165 shows the sub-option structure.

Figure 165 Sub-option structure

SubOpt: Indicates the number of the sub-option. Sub-options contained in this packet are sub-option 1, sub-option 2 and sub-option 5. They have the following meanings:

- Sub-option 1 defines the Circuit ID.
- Sub-option 2 defines the Remote ID.
- Sub-option 5 defines the Link Selection.

Len: Indicates the length of the Sub-option Value field.

Sub-option Value: Indicates the sub-option value. For example, the value for sub-option 1 is Circuit ID.

Normal mode and 3Com fixed network mode

DHCP supports option 82. It can add option 82 into the request packets from the client to the server to identify the user location information. Only sub-option-1 and sub-option 2 can be added while sub-option 5 cannot be added currently. In the normal mode, sub-option 1 is the layer 2 port number and VLAN ID of the received packet, and sub-option 2 is the MAC address of the device to receive packets.

In order to locate the users more exactly, we put forward the IP DSLAM user physical position location solution for DSLAM application, and define the 3Com fixed network mode of the DHCP option 82, where the sub-option 1 of Option 82 is expressed in the form of "Node identifier + frame number/slot number/subslot/port number + vlan", sub-option2 still represents the MAC address of the Relay system, and sub-option5 is not added.

The node identifier in the sub-option1 of Option82 is a string, which can adopt the MAC address of the administration port of the device by default, in the form of 00-E0-FC-0D-DC-EC. You can modify the user node identifiers through

configurations for maintenance convenience. You can select to use the bridge MAC address of the Relay, the device name (configured through sysname), or user-defined strings.

The identifier format of sub-option1 in the 3Com fixed network mode of Option 82 is:

AccessNodeIdentifier eth frame/slot/subslot/port: vlan

The following section describes the meaning of each field in the formula above:

AccessNodeIdentifier: Access node identifier, which is a string no longer than 50 characters. It is the bridge MAC address by default

frame: Frame number, which is 0 if the frame is not supported

eth: Ethernet port type

slot: Slot number

subslot: Subslot number

port: Port number

vlan: VLAN Identifier

related protocols and specifications

The protocols and specifications related to Option 82 support on DHCP relay are:

- RFC 2131 Dynamic Host Configuration Protocol
- RFC 3046 DHCP Relay Agent Information Option

Working Mechanism of Option 82 Support on DHCP Relay

The process for a DHCP client to acquire an IP address from a DHCP server through a DHCP relay is the same as that for a DHCP client to acquire an IP address directly from the DHCP server in the same network segment. Both the processes have four phases: discovery, offer, selection and acknowledgement. For the details, refer to the DHCP section in "Network Layer Protocols" in this manual. The following only introduces the working mechanism of Option 82 support on DHCP relay.

- 1 A DHCP client broadcasts a request packet during initialization.
- 2 If a DHCP server exists in the local network, the DHCP client acquires an IP address from this server directly. If not, the broadcast packet is processed by the DHCP relay device that is connected to the local network. The DHCP relay device will check whether Option 82 exists in the packet.
- 3 If Option 82 exists in the packet, the relay processes the packet according to the configured strategy. The relay may drop the packet, replace the original Option 82 with its own Option 82, or keep the original Option 82 unchanged. Then, the relay forwards the packet (if not dropped) to a DHCP server.
- 4 If Option 82 does not exist in the request packet, the DHCP relay device adds Option 82 into the packet and then forwards it to a DHCP server. In this way, the packet contains the MAC address and VLAN ID of the port of the switch that the DHCP client is connected to, and the MAC address of the DHCP relay itself.

- 5 After receiving the DHCP request packet forwarded by the DHCP relay, the DHCP server records the information carried by the option in the packet. Then, the DHCP server sends to the DHCP relay a response packet which carries the DHCP configuration information and Option 82 information.
- 6 After receiving the response packet sent by the DHCP server, the DHCP relay strips Option 82 information in the packet. Then, it forwards the packet that carries the DHCP configuration information to the DHCP client.



The request packets sent by a DHCP client fall into two types: DHCP_DISCOVER packets and DHCP_REQUEST packets. The DHCP relay device adds Option 82 into both types of request packets. This is because that the DHCP servers from different manufacturers process the request packets in different ways. Some of them process Option 82 in the DHCP_DISCOVER packets, while others process Option 82 in the DHCP_REQUEST packets.

Configuring Option 82 Supply on DHCP Relay

Configuration Prerequisites

Before enabling Option 82 support on DHCP relay, you should configure:

- The network parameters and the relay function on the DHCP relay
- The network parameters, the parameters related to the allocation strategy such as the address pools and the address allocation lease on the DHCP server.

In addition, you should make proper configuration to ensure that the DHCP relay and the DHCP server devices are reachable to each other.

For detailed configurations, refer to DHCP section in the "Network Layer Protocols" in this manual.

Enabling Option 82 Support on DHCP Relay

The configurations here can only be performed on the network devices where the DHCP relay function is enabled.

Perform the following configuration in VLAN interface view to configure the Option 82 support on DHCP relay for the current VLAN Interface.

Table 654 Enable Option 82 support on DHCP relay on the current VLAN interface

Operation	Command	Remarks
Enter system view	system-view	-
Create and enter VLAN interface view	interface vlan-interface <i>vlan-id</i>	Required The corresponding VLAN must exist
Enable Option 82 support on DHCP relay	dhcp relay information enable	Required This feature is disabled by default

Table 654 Enable Option 82 support on DHCP relay on the current VLAN interface

Operation	Command	Remarks
Configure the strategy for the DHCP relay to process the request packets that carry Option 82	<code>dhcp relay information strategy { drop keep replace }</code>	Optional By default, the DHCP relay adopts the strategy replace to process the request packets that carry Option 82. That is, the DHCP relay replaces the original Option 82 in the packets with its own Option 82.
Configure the mode of DHCP Relay option 82	<code>dhcp relay information format { normal verbose }</code>	Optional The mode of DHCP Relay option 82 is normal by default
Configure the user identifier of DHCP Relay option 82 when it is in 3Com fixed network mode	<code>dhcp relay information format verbose node-identifier { mac sysname user-defined string <1-50> }</code>	Optional The user identifier of DHCP Relay option 82 is the system bridge MAC address by default

Perform the following configuration in system view to configure Option 82 support on DHCP relay for multiple VLAN interfaces at the same time.

Table 655 Enable Option 82 support on DHCP relay on the current VLAN interfaces

Operation	Command	Description
Enter system view	<code>system-view</code>	-
Enable Option 82 support on DHCP relay	<code>dhcp relay information enable</code> <code>{ interface vlan-interface vlan-id [to vlan-interface vlan-id] all }</code>	Optional This feature is disabled by default

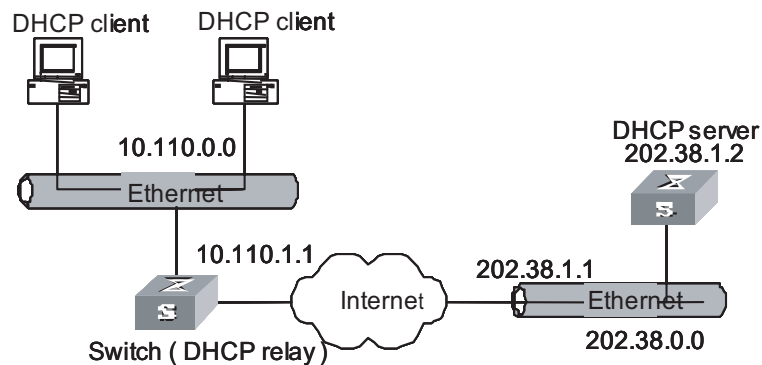
Option 82 Support on DHCP Relay Configuration Example

Network requirements

Two DHCP clients are on 10.110.0.0, and they acquire IP addresses from the DHCP server through a DHCP relay device. The DHCP relay function is enabled on a VLAN interface of the switch serving as the DHCP relay. Option 82 support is enabled on the DHCP relay.

Network diagram

Figure 166 Network diagram for Option 82 support on DHCP relay configuration



Configuration procedure

Suppose the DHCP relay and the DHCP server is reachable to each other. The following only introduces the configuration on the switch which serves as the DHCP relay.

Enable the DHCP service

```
<SW8800> system-view
[SW8800] dhcp enable
```

Enter the view of the interface on which the DHCP relay function will be enabled. Configure an IP address and a subnet mask for the interface so that it belongs to the same network segment with the DHCP client

```
[SW8800] interface vlan-interface 100
[3Com-vlan-interface 100] ip address 10.110.1.1 255.255.0.0
```

Enable the DHCP relay function on the interface, and configure an IP address for the DHCP relay function (this address specifies the location of the DHCP server for this interface). Enable Option 82 support on DHCP relay and specify the strategy to **keep**. Specify the mode as 3Com fixed network mode and the system name as the node identifier.

```
[SW8800] interface vlan-interface 100
[3Com-vlan-interface 100] dhcp select relay
[3Com-vlan-interface 100] ip relay address 202.38.1.2
[3Com-vlan-interface 100] dhcp relay information enable
[3Com-vlan-interface 100] dhcp relay information strategy keep
[3Com-vlan-interface 100] dhcp relay information format verbose
[3Com-vlan-interface 100] dhcp relay information format verbose node-
identifier sysname
```

The configuration of the DHCP server is omitted here.

Introduction to DNS

Used in the TCP/IP application, Domain Name System (DNS) is a distributed database which provides the translation between domain name and the IP address. In this way, the user can use domain names that are easy to memorize and meaningful, and never needs to keep obscure IP addresses in mind.

There are two kinds of domain name resolutions: static domain name resolution and dynamic domain name resolution, which supplement each other in real application. On resolving a domain name, use the static resolution first. If it fails, use the dynamic resolution method. You can put some common domain names into the static domain name resolution table to raise the domain name resolution efficiency greatly.

Static Domain Name Resolution

Static domain resolution is to establish maps between domain name and the IP address manually. When you perform some applications using domain names, the system can obtain the IP address of the specified domain name by searching the static domain name resolution table.

Dynamic Domain Name Resolution

Dynamic domain name resolution is implemented by inquiring the domain name server. As a DNS client, the switch sends an inquiry request to the domain name server, and the domain name server searches the related IP address of the domain name in its own database and sends it back to the switch. If the domain name server judges that the domain name does not belong to the local domain, it forwards the request to the upper level domain name resolution server till the resolution is finished.

Dynamic domain name resolution supports the buffer function. It stores each successful domain name/IP address mapping that is resolved dynamically in the dynamic domain name buffer. When the same domain name is searched next time, it can be read directly from the buffer, without requesting the domain name server. The aged mapping in the buffer is deleted after a certain period of time to ensure the updated contents can be got from the domain name server timely. The aging time is set by the domain name server and obtained by the switch from the protocol packet.

Dynamic domain name resolution supports the domain name suffix list function. You can set some domain name suffixes beforehand and input part of the domain name field during the domain name resolution, then the system adds different suffixes to the input domain name automatically for resolution. For example, if a user wants to search the domain name "3Com.com", he can configure the "com" in the suffix list and input "3Com". Then the system connects the input domain name with the suffix into "3Com.com" automatically to search. When the domain name suffix is used, if the input domain name does not include ".", like

"3Com", the system regards it as a host name and add a domain name suffix to search. After all the domain names are failed to be searched out in this way, the system finally searches with the primarily input domain name. If the input domain name does include ".", like "www.3Com", the system searches with it directly. The system adds each suffix to search one by one only after the search fails. If the input domain name contains a "." in the final position, like "3Com.com.", it indicates that the domain name suffix needs not to be added. The system removes the last "." from the input domain name and search with the remaining part. Succeeded or not, the system returns to the originally input domain name. Put it more specifically, if the last character of the input domain name is ".", the system only searches according to characters before the "." rather than matches the domain name. In this sense, the last "." is also called "search terminator".

Configuring Static Domain Name Resolution

You can use this command to map the host name to the host IP address. When you use applications like Telnet, you can use the host name directly, and the system translates it into the IP address, rather than the obscure IP address.

Perform the following configuration in system view.

Table 656 Configure host name and the corresponding IP address

Operation	Command
Configure host name and the corresponding IP address	ip host <i>hostname ip-address</i>
Cancel host name and the corresponding IP address	undo ip host <i>hostname [ip-address]</i>

Each host can have only one IP address. If you configure a host name more than once, then the IP address configured at last is effective.

Configuring Dynamic Domain Name Resolution

Dynamic domain name resolution configuration includes:

- "Enable/Disable Static Domain Name Resolution"
- "Configure the IP Address of Domain Name Server"
- "Configure Domain Name Suffix"

Enable/Disable Static Domain Name Resolution

You can use the following command to enable dynamic domain name resolution. However, since dynamic domain name resolution may take some time, you can disable this function when you do not want to perform dynamic domain name resolution sometimes.

Perform the following configuration in system view.

Table 657 Enable/disable dynamic domain name resolution

Operation	Command
Enable dynamic domain name resolution	dns resolve
Disable dynamic domain name resolution	undo dns resolve

By default, dynamic domain name resolution is disabled.

Configure the IP Address of Domain Name Server

You are required to configure the domain name sever if you need to use the function of the dynamic domain name resolution. In this way, you can send the inquiry request packets to the appropriate sever. The system supports up to six domain name severes.

Perform the following configuration in system view.

Table 658 Configure the IP address of the domain name sever

Operation	Command
Configure the IP address of the domain name sever	dns server <i>ip-address</i>
Delete the IP address of the domain name sever	undo dns server [<i>ip-address</i>]

Configure Domain Name Suffix

You can use the following command to configure domain name suffix list. By configuring this, you can just input part of the domain name and the system automatically adds the preconfigured suffix to perform the resolution. The system supports up to 10 domain name suffixes.

Perform the following configuration in system view.

Table 659 Configure domain name suffix

Operation	Command
Configure domain name suffix	dns domain <i>domain-name</i>
Delete domain name suffix	undo dns domain [<i>domain-name</i>]

Displaying and Debugging Domain Name Resolution

After the above configuration, you can execute the **display** command in any view to view the running states of the domain name resolution, and verify the configuration results through the displayed information.

Execute the **reset** command in user view to clear the dynamic domain name buffer. Execute the **debugging** command to debug the domain name resolution.

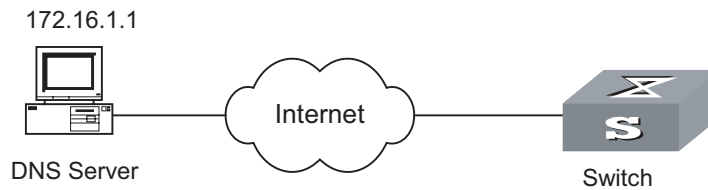
Table 660 Display and debug the domain name resolution

Operation	Command
Display the static domain name resolution table	display ip host
Display the information on domain name sever	display dns server
Display the information on domain name suffix list	display dns domain
Display the information on the dynamic domain name buffer	display dns dynamic-host
Clear dynamic domain name buffer	reset dns dynamic-host
Enable the debugging for the domain name resolution	debugging dns
Disable the debugging for the domain name resolution	undo debugging dns

DNS Configuration Example

Network requirements

As the client, the switch uses dynamic domain name resolution. The IP address of the domain name server is 172.16.1.1. The configured suffix of the domain name is "com". There is a route between the switch and the server.

Network diagram**Figure 167** Network diagram for DNS client**Configuraiton procedure**

Enable dynamic domain name resolution

```
[SW8800] dns resolve
```

Configure the IP address of the domain name server to 172.16.1.1.

```
[SW8800] dns server 172.16.1.1
```

Configure the domain name suffix as com.

```
[SW8800] dns domain com
```

Ping a host with the specified domain name.

```
[SW8800] ping ftp
Trying DNS server (172.16.1.1)
PING ftp.com (200.200.200.200): 56 data bytes, press CTRL_C to break
  Reply from 200.200.200.200: bytes=56 Sequence=1 ttl=128 time=2 ms
  Reply from 200.200.200.200: bytes=56 Sequence=2 ttl=128 time=2 ms
  Reply from 200.200.200.200: bytes=56 Sequence=3 ttl=128 time=2 ms
  Reply from 200.200.200.200: bytes=56 Sequence=4 ttl=128 time=2 ms
  Reply from 200.200.200.200: bytes=56 Sequence=5 ttl=128 time=2 ms

--- ftp.com ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 2/2/2 ms
```

The routing configuration between the switch and the domain name sever is omitted here, and refer to the related chapter for the configuration.

**Troubleshooting
Domain Name
Resolution
Configuration**

Fault: Domain name resolution fails.

Troubleshoot: Perform the following procedures:

- Check whether the domain name resolution function is enabled.
- Check whether the IP address of the domain name sever is correctly configured.
- Check whether there is a correct route between the domain name sever and the switch.
- Check whether there is network connection failure, such as network cable break, loose connection, and so on.



The application module described in this chapter refers to 3C17542 Network Monitoring Module (NMM).

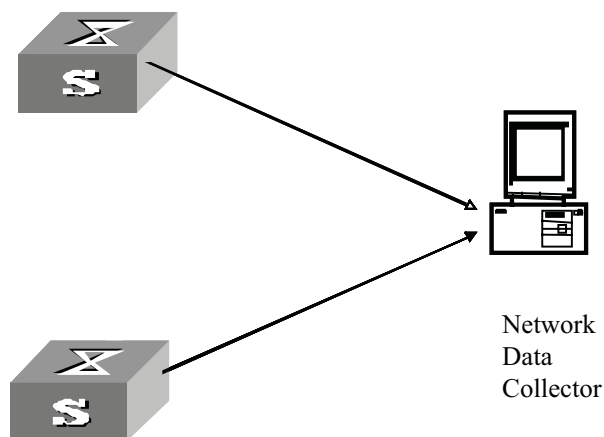
Netstream Overview

Introduction to Netstream

Netstream provides the packet statistics function. It can classify the stream information according to the destination IP address, destination port number, source IP address, source port number, protocol number and ToS of the packet, and performs independent statistics for different stream information.

Figure 168 describes the basic collection and analysis procedure of Netstream data.

Figure 168 The basic collection and analysis procedure of Netstream data



The collection and analysis procedure of Netstream data is as follows:

- 1 The switch regularly sends the collected verbose stream information to the network data collector (NDC);
- 2 The NDC analyses the data and the analysis result is used for accounting and network planning.

Netstream Implementation

When the Netstream feature is enabled, the stream information is first saved to the Netstream cache. After a certain amount of time, the stream information is sent to the NDC in the format of version 5, version 8, or version 9 UDP packets.

- The aged stream information is generally sent in the form of version 5 UDP packets;

- If Netstream Aggregation is configured, the stream information will be classified and aggregated to generate aggregation information according to certain rules, and then sent in the format of version 8 UDP packets.
- The MPLS stream statistics information is sent in the format of version 9 UDP packets.

Netstream Configuration

The following table describes the Netstream configuration tasks:

Table 661 Configure Netstream

Operation	Command	Description
Enter system view	system-view	-
Enable the Netstream statistics function	ip Netstream enable slot <i>slot-no</i>	Required The Netstream statistics function is disabled by default
Enter Netstream aggregation view	ip Netstream aggregation { as destination-prefix prefix prefix-port protocol-port source-prefix tos-as tos-destination-prefix tos-prefix tos- protocol-port tos-source-prefix }	Optional
Enable the aggregation mode corresponding to the current aggregation view.	enable	Optional Aggregation mode is not enabled by default
Configure the destination host address and the UDP port number of the Netstream statistics export packet	ip Netstream export { host <i>ipaddress udpport source</i> <i>ipaddress }</i>	Required By default: In system view, the output destination address and port number are 0 In aggregation view, the output destination address and port number are what they are set in system view The source IP address of export packets is 0 (the system will add an IP address to the destination address automatically)
Configure the version number and AS number of the Netstream statistics export packet	ip Netstream export version <i>versionNo</i> [origin-as peer-as]	Optional The switch currently supports version 5 and version 9 packet configurations By default, the version number and AS number of UDP packets of normal streams are 5 and peer-as respectively; the version number of UDP packets of aggregation streams is 8; the version number of UDP packets of MPLS streams is 9

Table 661 Configure Netstream

Operation	Command	Description
Configure the active aging of Netstream	ip Netstream timeout active <i>minutes</i>	Optional By default, the active aging of Netstream is 30 minutes
Configure the inactive timeout of Netstream	ip Netstream timeout inactive <i>seconds</i>	Optional By default, the inactive timeout of Netstream is 60 seconds
Configure the packet refresh rate of the template	ip Netstream template refresh <i>packets</i>	Optional The refresh rate of the Netstream template is 20 by default
Configure the aging time of the template	ip Netstream template timeout <i>minutes</i>	Optional By default, the aging time of the Netstream template is 30 minutes



For Version 5 packets, the active aging time, inactive aging time, version template refresh rate, and version template aging time are the same as those of version 9 packets.

The switch supports eleven aggregation modes currently:

Table 662 Eleven aggregation modes of Netstream

Aggregation mode	Classification rules
AS aggregation	Source AS number, destination AS number and outbound interface index
Destination-prefix aggregation	Destination AS number, destination address mask length, destination prefix, and outbound interface index
Prefix aggregation	Source AS number, destination AS number, source address mask length, destination address mask length, source prefix, destination prefix, and outbound interface index
Prefix-port aggregation	Source prefix, destination prefix, source port, outbound interface index, and ToS value
Protocol-port aggregation	Protocol number, source port, and destination port
Source-prefix aggregation	Source AS number, source address mask length, and source prefix
ToS-AS aggregation	ToS, Source AS number, destination AS number, source interface and outbound interface index
ToS-destination-prefix aggregation	Destination AS number, destination mask length, destination prefix, and outbound interface index
ToS-prefix aggregation	ToS, source AS number, source prefix, source mask length, destination AS number and destination prefix
ToS-protocol-port aggregation	ToS, protocol type, source port, and destination port
ToS-source-prefix aggregation	ToS, source prefix, source mask length and source interface index

According to the selected aggregation mode, the system aggregates multiple information streams into one aggregation stream, which corresponds to an

aggregation log. The eleven aggregation modes are independent of each other, so they can be configured at the same time.



- The configuration in system view affects version 5 UDP packets. Additionally, this configuration is also effective for version 8 UDP packets when the source port and destination address arguments are not configured in aggregation view.
- The configuration in aggregation view affects version 8 UDP packets only.



CAUTION: When the aging time is configured, the active aging time is in minutes and the inactive aging time is in seconds.

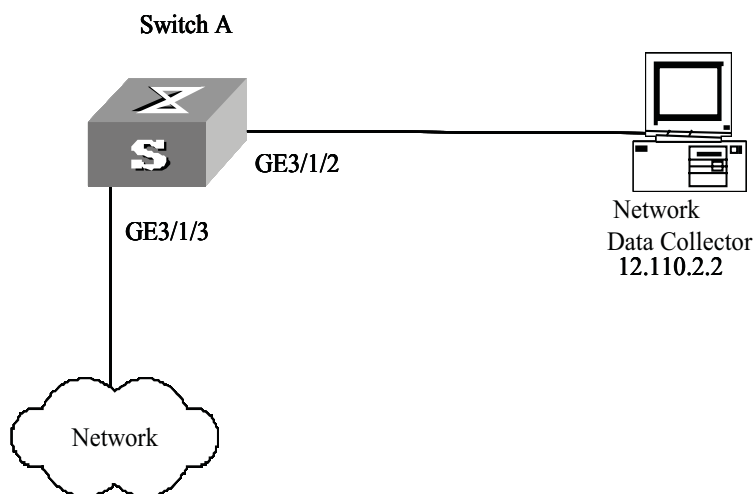
Netstream Configuration Examples

Network requirements

As shown in Figure 169, Netstream is configured on Switch A to perform statistics on the packets received on GigabitEthernet3/1/3. The NMM Application Module to implement the Netstream function is plugged in slot 5 of the switch.

Network diagram

Figure 169 Diagram for 3Com Switch 8800 Family Netstream Configuration



Configuration procedure

Configure the VLAN of GigabitEthernet3/1/2.

```
<Switch_A>system-view
[Switch_A] vlan 2
[Switch_A-vlan2] port GigabitEthernet3/1/2
[Switch_A-vlan2] quit
```

Configure the IP address for the VLAN interface.

```
[Switch_A] interface vlan-interface 2
[Switch_A-vlan-interface2] ip address 12.110.2.1 24
[Switch_A-vlan-interface2] quit
```

Map the packets received on GigabitEthernet3/1/3 to slot 5.

```
[Switch_A] mirror-group 1 inbound GigabitEthernet3/1/3 mirror-to slot 5
```

Enable the Netstream function on the module of slot 5.

```
[Switch_A] ip Netstream enable slot 5
```

Configure the export source address of the Netstream statistics packets.

```
[Switch_A] ip Netstream export source 12.110.2.10
```

Configure the export destination address and destination port number of the Netstream statistics packets.

```
[Switch_A] ip Netstream export host 12.110.2.2 9991
```

Notes:

- *The Network Data Collector may require SNMP read access to the Switch 8800.*
- *The Network Data Collector may require that the Switch 8800 have its time synchronized with the NDC.*
- *The Network Data Collector may use a different default UDP port than shown in the example.*

60

NDP CONFIGURATION

Introduction to NDP

Neighbor discovery protocol (NDP) is used to discover the information about a neighbor device directly connected, including the type, software/hardware version, port connected, ID, port address, and hardware platform of the neighbor device.

A device running NDP periodically sends NDP packets to all ports with NDP enabled while receiving NDP packets from the neighbor device. The device receiving a NDP packet does not forward it, but maintains an NDP neighbor information table on the current device and stores the neighbor information carried in the NDP packets in this table. Besides neighbor device information, NDP packets contain the information about the aging timer for the NDP information, which specifies how long the NDP packets will be stored on the receiving device.

If the NDP neighbor information is not updated even after the aging timer for NDP information expires, the device automatically deletes the entry corresponding to the NDP information from the NDP neighbor information table. If the neighbor information received by the device is different from the original information, the device updates the corresponding entry in the NDP neighbor information table. If the neighbor information received by the device is the same as the original information, the device updates only the aging timer in the NDP neighbor information table.

You can also clear the current NDP information and collect NDP neighbor information again.



Upon receipt of NDP packets, a switch with NDP disabled directly forwards the packets to all ports in the same VLAN, while a switch with NDP enabled does not forward any NDP packet.

Introduction to NDP Configuration Tasks

Table 663 NDP configuration tasks include:

Configuration task	Description	Related section
Configure the NDP in the system	Required	Section "Enabling NDP in the System" "Enabling NDP in the System".
Configure the NDP on a port	Required	Section "Configuring NDP on a Port" "Configuring NDP on a Port".
Configure the aging timer for NDP information	Optional	Section "Configuring the Aging Timer for NDP Information" "Configuring the Aging Timer for NDP Information"
Configure the interval at which NDP packets are sent	Optional	Section "Configuring the interval at which NDP packets are sent" "Configuring the interval at which NDP packets are sent"



- On the management device, NDP must be enabled in the system and on the ports.
- On member devices and candidate devices, the NDP feature must also be enabled in the system and on the corresponding ports. The aging timer for the NDP information sent from the management device is used during NDP operation.

Enabling NDP in the System

To collect the NDP information sent by the neighbor device, you must enable NDP on the switch. With NDP enabled in the system, the switch periodically collects NDP information, which you can query by using the **display ndp** command. With NDP disabled in the system, the switch clears all NDP neighbor information stored on it but will still forwards NDP packets.

Table 664 Enable NDP in the system

Operation	Command	Description
Enter system view	system-view	-
Enable NDP in the system	ndp enable [interface <i>port-list</i> all]	By default, NDP is disabled in the system.



When you try to enable NDP on all ports, NDP is enabled only on the common Ethernet ports and Gigabit Ethernet ports that support NDP interface modules.

Configuring NDP on a Port

You can control the collection of neighbor device information for the specified port by enabling/disabling NDP on the port. With NDP enabled on the port and in the system, the system periodically collects the NDP neighbor information about the adjacent node of the port. With NDP disabled on the port, the system cannot collect NDP information through the port.

Table 665 Enable NDP on a port

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	Currently, only common Ethernet interface modules and Gigabit Ethernet interface modules support NDP.
Enable NDP on the port	ndp enable	By default, NDP is disabled on a port.

Configuring the Aging Timer for NDP Information

Upon receipt of NDP packets, from the aging timer information carried in the packets, the switch can learn about the aging timer for the NDP information of the neighbor device that sent the packets and discards the NDP information of the neighbor device once the aging timer is exceeded. This configuration allows you to set the aging timer for the NDP information of the current device on the neighbor device.

Table 666 Configure the aging timer for NDP information

Operation	Command	Description
Enter system view	system-view	-

Table 666 Configure the aging timer for NDP information

Operation	Command	Description
Configure the aging timer for NDP information	ndp timer aging <i>aging-in-secs</i>	By default, the aging timer for NDP information is 180 seconds. The aging timer for NDP information must be greater than or equal to the interval at which NDP packets are sent; otherwise, the NDP information table will be unstable.

Configuring the interval at which NDP packets are sent

The NDP information of the adjacent device must be updated periodically to ensure that the switch can update the local NDP neighbor information table in time after the configuration of the adjacent device is changed. You can configure the interval at which NDP packets are sent by using the following command.

Table 667 Configure the interval at which NDP packets are sent

Operation	Command	Description
Enter system view	system-view	-
Configure the interval at which NDP packets are sent	ndp timer hello <i>seconds</i>	By default, NDP packets are sent every 60 seconds. The interval at which NDP packets are sent must be less than or equal to the aging timer for NDP information. Otherwise, the NDP information table will be unstable.

Displaying and debugging NDP

After the above-mentioned configuration:

- Use the **display** command in any view to display the operating state of the NDP and verify configuration result.
- You can use the **reset** command to clear the statistics related to NDP in user view.

Table 668 Display and debug NDP

Operation	Command
Display the NDP configuration of the system (including the interval at which packets are sent and the aging timer for NDP information)	display ndp
Display the NDP neighbor information of the specified port	display ndp interface <i>port-list</i>
Clear the statistics of an NDP-enabled port	reset ndp statistics [<i>interface port-list</i>]

NDP Configuration Example

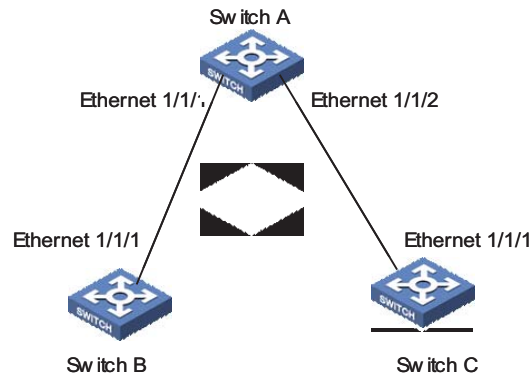
Network requirements

- Switch A, Switch B, and Switch C are interconnected.
- Ethernet 1/1/1 on Switch A is connected to Ethernet 1/1/1 on Switch B and Ethernet 1/1/2 on Switch A is connected to Ethernet 1/1/1 on Switch C.

- The information of the neighbor switches Switch B and Switch C that are connected to Switch A should be visible to Switch A through NDP configuration.

Network diagram

Figure 170 Network diagram for NDP configuration



Configuration procedure

1 Configure Switch A.

Enable NDP in the system and on Ethernet 1/1/1 and Ethernet 1/1/2.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ndp enable
[SW8800] interface ethernet 1/1/1
[3Com-Ethernet1/1/1] ndp enable
[3Com-Ethernet1/1/1] quit
[SW8800] interface ethernet 1/1/2
[3Com-Ethernet1/1/2] ndp enable
```

Configure the aging timer for NDP information as 200 seconds.

```
[3Com-Ethernet1/1/2] quit
[SW8800] ndp timer aging 200
```

Configure NDP packets to be sent every 70 seconds.

```
[SW8800] ndp timer hello 70
```

2 Configure Switch B (Configure Switch C in a similar way).

Enable NDP on the device and Ethernet1/1/1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ndp enable
[SW8800] interface ethernet 1/1/1
[3Com-Ethernet1/1/1] ndp enable
```



After the above-mentioned configuration, you can view the information about the neighbor switch connected to the port by issuing the **display ndp interface port-list** command on Switch A.

61

POE CONFIGURATION

PoE Overview

PoE on the Switch 3Com Switch 8800 Family Series Routing Switches (hereinafter referred to as Switch 8800 Family series) support power-over-Ethernet (PoE). Equipped with external power supply and PoE-capable cards, Switch 8800 Family series can provide 48 VDC power for remote powered devices (PDs, such as IP phones, WLAN APs, and Network cameras) through twisted pairs.

- The Switch 8800 Family series support LEGACY Power Supply standard. While they can also supply power to PDs noncompliant with the standard.

The power supply of the Switch 8800 Family series is administered by the SRP card; each PoE card on the switch can be viewed as a power sourcing equipment (PSE), which administers the power supplying of all the ports on it independently.

The Switch 8800 Family series can transmit data and supply power in the mean time through the signal lines (1, 3, 2, and 6) of the category-3/5 twisted pairs. Using converters, they can also supply power to the PDs that can be powered only through spare lines (4, 5, 7, and 8).

- The Switch 8800 Family series supply power through the Ethernet electrical ports on the service cards. Each service card can supply power to up to 48 remote devices at the maximum distance of 100 m (328 feet).
- The maximum power that can be supplied by each Ethernet port to its PD is 16.8 W.
- When supplying power to remote devices, the maximum total power that can be provided by the Switch 8800 Family series is 4500 W (220 V)/2250 W (110V). The switch determines whether or not to supply power to the next remote PD it discovered depending on the total power it currently supply.



- When a remote PD is powered by an Switch 8800 Family series switch, the PD needs not have any external power supply.
- If the remote PD has an external power supply, the Switch 8800 Family series switch and the external power supply will be redundant with each other for the PD.

External PSE4500-A Power System If PSE4500-A power system is taken as the external power supply of the switch, the power distribution is as follows:

- 1 Input voltage: 110 VAC
 - One or two PSUs (power supply unit) of the PSE4500-A power system can provide 1,200 W of power.
 - If the PSE4500-A power modules work in 2+1 redundancy backup mode, an output power of 2,500 W is provided and one power module works for the purpose of backup.
- 2 Input voltage: 220 VAC
 - In the PSE4500-A power system, one power module can provide a power of up to 2,500 W and two modules can provide a power of up to 4,500 W. When working in the 1+1 backup mode, the system provides a power of up to 2,500 W.
 - If the PSE4500-A power modules are in 2+1 redundancy, an output power of up to 4500 W is provided and one power module works for the purpose of backup.

PoE-Capable Card The following service card of the Switch 8800 Family series supports PoE:

- GV48D



CAUTION:

- When the actual power exceeds the set value, the port with a lower priority stops supplying power so that the port with a higher priority can supply power.
- To ensure power supply to the "last PD" and provide redundant power to prevent a transient rise of module power consumption, by default, a buffer of 19 W is reserved on the chip. For example, if you set the maximum PoE power for the module to 400 W, a power of 381 W only can be guaranteed to respond quickly for stable power supply.
- Currently, you can set a PoE power ranging from 37 W to 806 W on the PoE modules of the Switch 8800 Family series routing switches. By default, the power for a PoE module is 806 W.

PoE Configuration

The Switch 8800 Family series can automatically detect any connected device that needs remote power supply and feeds power to this device.

- Depending on your actual network requirement, you can set the maximum PoE power totally supplied by the switch through the command line.
- You can set the maximum PoE power supplied by a card through the command line.
- You can also control the PoE on each PoE port independently through the command line. The control includes: enabling/disabling the PoE feature, and setting the maximum PoE power, the PoE mode and the PoE priority on the port.

PoE Configuration Tasks

The following table describes the PoE configuration tasks on the Switch 8800 Family series.

Table 669 PoE configuration tasks on the Switch 8800 Family series

No	Operation	Command	Description
1	Enter system view	system-view	- Optional
2	Configure the maximum power of switch	poe power max-value <i>max-value</i>	By default, the maximum power of the switch is 4,500 W. Required
3	Enable PoE on a module	poe enable slot <i>slot-num</i>	By default, PoE is disabled on a module. Optional
4	Enable the module to detect the compatibility of the PD connected to it	poe legacy enable slot <i>slot-num</i>	By default, the module does not detect the compatibility of the PD connected to it. Optional
5	Configure the PoE power management for a module on the switch	poe power-management { auto manual } slot <i>slot-num</i>	By default, you manually manage PoE power supply for the module on the switch. As a result of this command, a port view prompt is displayed, which varies with the port type you selected.
6	Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	Optional
7	Enable PoE on the port	poe enable	By default, PoE is disabled on a port. Optional
8	Set the maximum PoE power supplied by the port	poe max-power <i>max-power</i>	You can set the maximum PoE power supplied by a port depending on the power of the actual PD. By default, the <i>max-power</i> is 16,800 mW.
9	Set the PoE mode on the port	poe mode { signal spare auto }	Switch 8800 Family series supports only signal line PoE mode. By default, the PoE mode on a port is signal. Optional
10	Set the PoE priority on the port	poe priority { critical high low }	You can set the PoE priority on a port depending on the practical situation. By default, the PoE priority on a port is low .

To cancel the configurations, use the corresponding **undo** commands. For details about the parameters, refer to the *Command Manual*.



- Before setting the maximum power supplied by a card, make sure the remaining power of the switch is no less than the full power of the card, and the power you can set for a card ranges from 37 W to 806 W.

- The reserved power for a blank slot will be recycled automatically by the system if you insert a PoE-incapable card into the slot.
- When a card is almost fully loaded and a new PD is added, the switch will respond to the PD according to the PoE priority set on the port.
- The PoE priority of each port is based on its card. In other words, the switch cannot compare the priorities of ports on different cards.
- The sampling cycle of the power, current and voltage of ports is 1 second; the sampling cycle of the peak power and average power of both cards and ports is 5 minutes

Displaying PoE Configuration

After the above-mentioned configuration, you can use the **display** command in any view to view the operating state, so as to verify configuration result.

Table 670 Display PoE configuration on a Switch 8800 Family switch

No	Operation	Command	Description
1	Display the PoE state(s) of a specific or all ports	display poe interface [<i>interface-type interface-num</i>]	You can execute this command in any view. Executing the display poe interface command without any option displays the PoE states about all the ports.
2	Display the PoE power information of a specific or all ports of the switch	display poe interface power [<i>interface-type interface-num</i>]	You can execute this command in any view. Executing the display poe interface power command without any option displays the PoE power information about all the ports.
3	Display the PoE state and PoE power information of each card	display poe pse	You can execute this command in any view.
4	Display the information about a card powered by PoE	display poe slot <i>slotnum</i>	You can execute this command in any view.

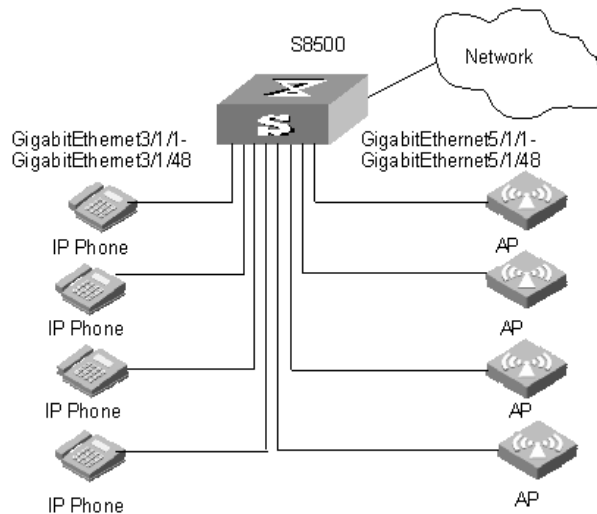
Comprehensive Configuration Example

Network requirements

- Two PoE-capable cards are installed in slots 3 and 5 on an Switch 8800 Family series routing switch.
- GigabitEthernet3/1/1 through GigabitEthernet3/1/48 are connected with IP phones and GigabitEthernet5/1/1 through GigabitEthernet5/1/48 are connected with access point (AP) devices.
- The IP phones connected to GigabitEthernet3/1/23 and GigabitEthernet3/1/24 do not need PoE.
- GigabitEthernet3/1/48 is reserved for the use of network management, so it needs higher priority.
- Slot 3 is provided with 400 W power and slot 5 is provided with full power.
- The input power of the AP device connected to GigabitEthernet5/1/15 cannot be greater than 9000 mW.

Network diagram

Figure 171 PoE remote power supplying



Configuration procedure

Set the maximum power to 400 W on the card in slot 3. By default, the power of each card is full, so the power on the card in slot 5 need not be configured.

```
[SW8800] poe max-power 400 slot 3
```

Enable PoE on the ports GigabitEthernet3/1/1 through GigabitEthernet3/1/48.

```
[3Com-GigabitEthernet3/1/1] poe enable
[3Com-GigabitEthernet3/1/2] poe enable
[3Com-GigabitEthernet3/1/3] poe enable
```

Go on the configuration till the port GigabitEthernet3/1/48.

Enable PoE on the ports GigabitEthernet5/1/1 through GigabitEthernet5/1/48.

```
[3Com-GigabitEthernet5/1/1] poe enable
[3Com-GigabitEthernet5/1/2] poe enable
[3Com-GigabitEthernet5/1/3] poe enable
```

Go on the configuration till the port GigabitEthernet5/1/48.

Set the PoE priority of the port GigabitEthernet3/1/48 to critical, the PD connected with GigabitEthernet3/1/48 will be powered in precedence on the premise that other ports' power supplying is not interrupted.

```
[3Com-GigabitEthernet3/1/48] poe priority critical
```

Set the maximum PoE power on the GigabitEthernet5/1/15 port to 9000 mW.

```
[SW8800] interface GigabitEthernet5/1/15
[3Com-GigabitEthernet5/1/15] poe max-power 9000
```


62

PoE PSU SUPERVISION CONFIGURATION

Introduction to PoE PSU Supervision

The PoE-capable Switch 8800 Family series can monitor the external PoE PSUs through the power supervision module on the PoE external power system.

The PoE PSU supervision module enables you to:

- Set the alarm thresholds for the AC input voltages of the PoE PSUs.
- Set the alarm thresholds for the DC output voltages of the PoE PSUs.
- Query PSU information such as voltage and power.

AC Input Alarm Thresholds Configuration

You can set the AC input alarm thresholds for the PoE PSUs to enable the Switch 8800 Family series to monitor the AC input voltages of the PSUs in real time through the PoE supervision module.

AC Input Alarm Thresholds Configuration Tasks

Table 671 AC input alarm thresholds configuration tasks

No	Operation	Command	Description
1	Enter system view	system-view	-
2	Set the overvoltage alarm threshold of AC input (upper threshold) for the PoE PSUs	poe-power input-thresh upper <i>string</i>	Required, and the max voltage is 264.0 V.
3	Set the undervoltage alarm threshold of AC input (lower threshold) for the PoE PSUs	poe-power input-thresh lower <i>string</i>	Required, and the min voltage is 90.0 V.
4	Display the AC input state of each PoE PSU	display poe-power ac-input state	Optional, and you can execute this command in any view.



- You can set the thresholds to any appropriate values in the range, but make sure the lower threshold is less than the upper threshold.
- For 220 VAC input, it is recommended to set the upper threshold to 264 V and the lower threshold to 181 V.
- For 110 VAC input, it is recommended to set the upper threshold to 132 V and the lower threshold to 90 V.

AC Input Alarm Thresholds Configuration Example

Network requirements

- Set the overvoltage alarm threshold of AC input for PoE PSUs to 264.0 V.
- Set the undervoltage alarm threshold of AC input for PoE PSUs to 181.0 V.

Configuration procedure

```
# Enter system view.
```

```
<SW8800> system-view
```

```
# Set the overvoltage alarm threshold of AC input for PoE PSUs to 264.0 V.
```

```
[SW8800] poe-power input-thresh upper 264.0
```

```
# Set the undervoltage alarm threshold of AC input for PoE PSUs to 181.0 V.
```

```
[SW8800] poe-power input-thresh lower 181.0
```

```
# Display the information about the AC input for the PoE PSUs.
```

```
[SW8800] display poe-power ac-input state
```

DC Output Alarm Thresholds Configuration

You can set the DC output alarm thresholds for the PoE PSUs to enable the Switch 8800 Family series to monitor the DC output voltages of the PSUs in real time through the PoE supervision module.

DC Output Alarm Thresholds Configuration Tasks

Table 672 DC output alarm thresholds configuration tasks

No	Operation	Command	Description
1	Enter system view	system-view	-
2	Set the overvoltage alarm threshold of DC output (upper threshold) for the PoE PSUs	poe-power output-thresh upper <i>string</i>	Required, and the range is 55.0 V to 57.0 V.
3	Set the undervoltage alarm threshold of DC output (lower threshold) for the PoE PSUs	poe-power output-thresh lower <i>string</i>	Required, and the range is 45.0 V to 47.0 V.
4	Display the DC output state of the PoE PSUs.	display poe-power dc-output state	Optional, and you can execute this command in any view.
5	Display the DC output voltage/current value of the PoE PSUs	display poe-power dc-output value	Optional, and you can execute this command in any view.



For both 220 VAC and 110 VAC input, it is recommended to set the upper threshold to 57.0 V and the lower threshold to 45.0 V.

DC Output Alarm Thresholds Configuration Example

Network requirements

- Set the overvoltage alarm threshold of DC output for the PoE PSUs to 57.0 V.
- Set the undervoltage alarm threshold of DC output for the PoE PSUs to 45.0 V.

Configuration procedure

```
# Enter system view.
```

```
<SW8800> system-view
```

```
# Set the overvoltage alarm threshold of DC output for the PoE PSUs to 57.0 V.
```

```
[SW8800] poe-power output-thresh upper 57.0

# Set the undervoltage alarm threshold of DC output for the PoE PSUs to 45.0 V.

[SW8800] poe-power output-thresh lower 45.0

# Display the DC output state of the PoE PSUs.

[SW8800] display poe-power dc-output state

# Display the DC output voltage/current values of the PoE PSUs.

[SW8800] display poe-power dc-output value
```

Displaying PoE Supervision Information

After completing the above configurations, you can execute the **display** command in any view to query the PoE state of the switch. Then you can view the display output to check the effect of these configurations.

Table 673 Display PoE supervision information

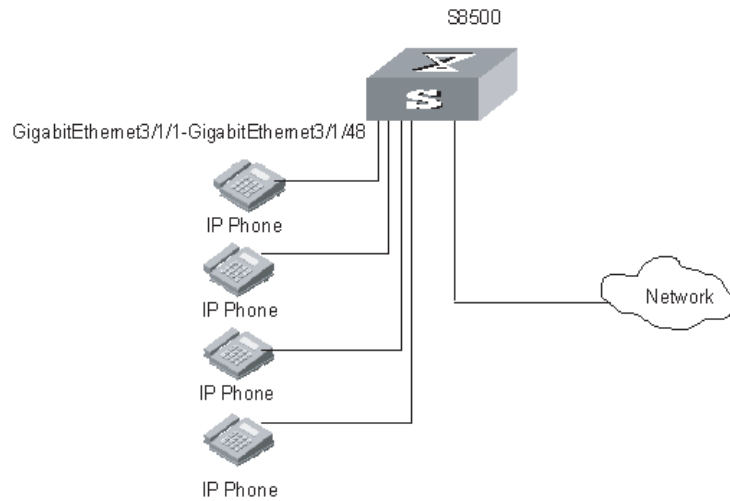
No	Operation	Command	Description
1	Display the basic information about the PoE PSUs.	display supervision-module information	You can execute this command in any view.
2	Display detailed alarm information about the PoE PSUs.	display poe-power alarm	You can execute this command in any view.
3	Display the number and current state of AC power distribution switches of the PSUs.	display poe-power switch state	You can execute this command in any view.

For details about display output, refer to the *Command Manual*.

PoE PSU Supervision Configuration Example

Network requirements

- Insert a PoE-capable card into slot 3 of the Switch 8800 Family series routing switch.
- Connect GigabitEthernet3/1/1 to GigabitEthernet3/1/48 to IP phones.
- Set the AC input and DC output alarm thresholds to appropriate values.

Network diagram**Figure 172** Network diagram for PoE supervision configuration**Configuration procedure**

Enter system view.

```
<SW8800> system-view
```

Set the overvoltage alarm threshold of AC input for PoE PSUs to 264.0 V.

```
[SW8800] poe-power input-thresh upper 264.0
```

Set the undervoltage alarm threshold of AC input for PoE PSUs to 181.0 V.

```
[SW8800] poe-power input-thresh lower 181.0
```

Set the overvoltage alarm threshold of DC output for the PoE PSUs to 57.0 V.

```
[SW8800] poe-power output-thresh upper 57.0
```

Set the undervoltage alarm threshold of DC output for the PoE PSUs to 45.0 V.

```
[SW8800] poe-power output-thresh lower 45.0
```

63

UDP HELPER CONFIGURATION

Overview

UDP Helper functions as a relay that converts UDP broadcast packets into unicast packets and forwards them to a specified server.

With the UDP Helper function enabled, the device decides whether to forward a received UDP broadcast packet according to the UDP port number of the packet. If the packet needs to be forwarded, the device modifies the destination IP address in the IP header and then sends the packet to the specified destination server. Otherwise, the device sends the packet to its upper layer module.

Configuring UDP Helper

UDP helper configuration includes:

- Enabling/disabling the function of forwarding UDP broadcast packets
- Specifying the UDP ports whose packets need to be forwarded
- Configuring the destination server to which the UDP packets are forwarded

Configuration Prerequisites

The router to be configured is reachable.

Configuration Procedure

Table 674 Configure UDP helper

Operation	Command	Description
Enter system view	system-view	-
Enable the function of forwarding UDP broadcast packets	udp-helper enable	Required <ul style="list-style-type: none">■ By default, the function is disabled.■ When the function is enabled, the function is enabled on the six default ports (69, 53, 37, 137, 138, and 49) simultaneously.■ When the function is disabled, the function is disabled on all the ports, including the default ports.

Table 674 Configure UDP helper

Operation	Command	Description
Specify the UDP ports whose packets need to be forwarded	udp-helper port { <i>port</i> dns netbios-ds netbios-ns tacacs tftp time }	Optional <ol style="list-style-type: none"> When the function is enabled, the broadcast packets of the default UDP ports are unicast to the corresponding destination server. Refer to Table 675 for the list of default UDP ports. The system supports up to 256 UDP ports. The UDP port number is in the range of 1 to 65,535. UDP broadcast packets of port 0, port 67, and port 68 cannot be forwarded.
Enter VLAN interface view	Interface Vlan-interface <i>interface -number</i>	-
Configure the destination server to which the UDP packets are forwarded	udp-helper server <i>ip-address</i>	Required <ul style="list-style-type: none"> Up to 20 destination servers are corresponding to a VLAN interface. Suppose a destination server is configured on a VLAN interface. When the function of forwarding UDP broadcast packets is enabled, all the broadcast packets received on the VLAN interface from the specified UDP ports are unicast to the destination server corresponding to the VLAN interface. By default, the destination server to which the UDP packets are forwarded is not configured.

Table 675 shows the list of default UDP ports.

Table 675 List of default UDP ports

Protocol	UDP port number
Trivial file transfer protocol (TFTP)	69
Domain name system (DNS)	53
Time service	37
NetBIOS name server (NetBIOS-NS)	137
NetBIOS datagram server (NetBIOS-DS)	138
Terminal access controller access control system (TACACS)	49

Note that:

- 1 You cannot specify the UDP ports before the function of forwarding UDP broadcast packets is enabled. Otherwise, the system prompts error.
- 2 The **dns | netbios-ds | netbios-ns | tacacs | tftp | time** keyword refers to six default UDP ports. You can specify a default UDP port in one of the two following ways:
 - Specifying the port number.
 - Specifying the keyword.

For example, the **udp-helper port 53** command specifies the same port as the **udp-helper port dns** command.

- 3 The **display current-configuration** command does not display the default port numbers. A default port number is displayed when the function of forwarding UDP broadcast packets is disabled on this port.
- 4 If the **undo udp-helper server** command is executed without any parameters, all destination servers configured on the VLAN interface are removed.

Displaying UDP Helper

After completing the configuration above, you can execute the **display** command in any view to verify the configuration by checking the displayed information.

Table 676 Display UDP helper

Operation	Command
Display the information of the destination servers corresponding to the VLAN interface	display udp-helper { server [interface <i>vlan-interface</i> <i>vlan-id</i>] port }

64

SNMP CONFIGURATION

SNMP Overview

By far, the Simple Network Management Protocol (SNMP) has gained the most extensive application in the computer networks. SNMP has been put into use and widely accepted as an industry standard in practice. It is used for ensuring the transmission of the management information between any two nodes. In this way, network administrators can easily search and modify the information on any node on the network. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating. SNMP adopts the polling mechanism and provides the most basic function set. It is most applicable to the small-sized, fast-speed and low-cost environment. It only requires the unverified transport layer protocol UDP; and is thus widely supported by many other products.

In terms of structure, SNMP can be divided into two parts, namely, Network Management Station and Agent. Network Management Station is the workstation for running the client program. At present, the commonly used NM platforms include Sun NetManager and IBM NetView. Agent is the server software operated on network devices. Network Management Station can send GetRequest, GetNextRequest and SetRequest messages to the Agent. Upon receiving the requests from the Network Management Station, Agent will perform Read or Write operation according to the message types, generate and return the Response message to Network Management Station. On the other hand, Agent will send Trap message on its own initiative to the Network Management Station to report the events whenever the device encounters any abnormalities such as restart.

SNMP Versions and Supported MIB

To uniquely identify the management variables of a device in SNMP messages, SNMP adopts the hierarchical naming scheme to identify the managed objects. It is like a tree. A tree node represents a managed object, as shown in the figure below. Thus the object can be identified with the unique path starting from the root.

- “Setting the Destination Address of Trap”
- “Setting Lifetime of Trap Message”
- “Setting the Engine ID of a Local Device”
- “Setting/Deleting an SNMP Group”
- “Setting the Source Address of Trap”
- “Adding/Deleting a User to/from an SNMP Group”
- “Creating/Updating View Information or Deleting a View”
- “Setting the Size of the SNMP Packet Sent/Received by an Agent”
- “Disabling SNMP Agent”

Setting Community Names

- SNMP V1 and SNMPV2C adopt the community name authentication scheme. SNMP Community is named with a character string, which is called community name. SNMP community name defines the relationship between SNMP manager and SNMP agent. The community name functions like a password, that is, it controls the access of the SNMP manager to the SNMP agent. You can choose to specify one or more community name-related features: Define MIB views of all the accessible MIB subsets.
- Define the read-only or read-write access mode of the community name to the MIB. The community with read-only authority can only query the device information, whereas the community with read-write authority can also configure the device.

Perform the following configuration in system view.

Table 678 Set community names

Operation	Command
Set the community name and the access authority	snmp-agent community { read write } <i>community-name</i> [[mib-view-view-name] [acl acl-list]]
Remove the community name and the access authority	undo snmp-agent community <i>community-name</i>

Setting the System Information

System information includes the ID and the contact method of the administrator, the location of the switch and the version of the SNMP.

The ID and the contact method of the administrator is a character string describing the contact information used for the system maintenance. Through this information, the device maintenance staffs can obtain the manufacturer information of the device so as to contact the manufacturer in case the device is in trouble. You can use the following command to set the contact information.

The location information of the switch is a management variable of the system group in MIB, which represents the location of the managed device.

Perform the following configuration in system view.

Table 679 Set the system information

Operation	Command
Set the system information	snmp-agent sys-info { contact <i>sysContact</i> location <i>sysLocation</i> version { { v1 v2c v3 } * all } }
Restore the default information	undo snmp-agent sys-info { { contact location } * version { { v1 v2c v3 } * all } }

By default, the contact information for system maintenance is "R&D Hangzhou, 3Com 3Com Technology Co., Ltd.", the physical location information is "Hangzhou China", and the version is SNMPv1, SNMPv2C, and SNMPv3.

Enabling/Disabling SNMP Agent to Send Trap

The managed device transmits trap without request to the Network Management Station to report some critical and urgent events (such as restart).

You can use the following commands to enable or disable the managed device to send trap message.

Perform the following configuration in corresponding views.

Table 680 Enable/disable SNMP Agent to send Trap

Operation	Command
Enable the sending of trap(system view)	snmp-agent trap enable [standard [authentication] [coldstart] [linkdown] [linkup]] bgp [backwardtransition] [established] vrrp [authfailure newmaster]]
Disable the sending of trap(system view)	undo snmp-agent trap enable [standard [authentication] [coldstart] [linkdown] [linkup]] bgp [backwardtransition] [established] vrrp [authfailure newmaster]]
Enable the switch ports to send SNMP trap messages (Ethernet port view or VLAN interface view)	enable snmp trap updown
Disable the switch port to send SNMP trap messages (Ethernet port view or VLAN interface view)	undo enable snmp trap updown

By default, the current port or VLAN interface sends trap messages.

Setting the Destination Address of Trap

You can use the following commands to set or delete the destination address of the trap.

Perform the following configuration in system view.

Table 681 Set the destination address of trap

Operation	Command
Set the destination address of trap	snmp-agent target-host trap address udp-domain <i>host-addr</i> [udp-port <i>udp-port-number</i>] params securityname <i>securityname</i> [v1 v2c v3 [authentication privacy]]

Table 681 Set the destination address of trap

Operation	Command
Delete the destination address of trap	undo snmp-agent target-host <i>host-addr</i> securityname <i>securityname</i>

Setting Lifetime of Trap Message

You can use the following command to set lifetime of Trap message. Trap message that exists longer than the set lifetime will be dropped.

Perform the following configuration in system view.

Table 682 Set the lifetime of Trap message

Operation	Command
Set lifetime of Trap message	snmp-agent trap life <i>seconds</i>
Restore lifetime of Trap message	undo snmp-agent trap life

By default, the lifetime of Trap message is 120 seconds.

Setting the Engine ID of a Local Device

You can use the following commands to set the engine ID of a local device.

Perform the following configuration in system view.

Table 683 Set the engine ID of a local device

Operation	Command
Set the engine ID of the device	snmp-agent local-engineid <i>engineid</i>
Restore the default engine ID of the device.	undo snmp-agent local-engineid

The engine ID of the device is in hexadecimal notation and has at least five characters, which can be IP address, MAC address or self-defined text. It defaults to the enterprise number + the device information.

Setting/Deleting an SNMP Group

You can use the following commands to set or delete an SNMP group.

Perform the following configuration in system view.

Table 684 Set/Delete an SNMP Group

Operation	Command
Set an SNMP group	snmp-agent group { v1 v2c } <i>group-name</i> [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-list</i>]
Delete an SNMP group	undo snmp-agent group { v1 v2c } <i>group-name</i> undo snmp-agent group v3 <i>group-name</i> [authentication privacy] [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-list</i>]

Setting the Source Address of Trap

You can use the following commands to set or remove the source address of the trap.

Perform the following configuration in system view.

Table 685 Set the source address of trap

Operation	Command
Set the Source Address of Trap	snmp-agent trap source <i>interface-type interface-number</i>
Remove the source address of trap	undo snmp-agent trap source



Currently, this command takes effect only on the interfaces with *vlan-interface* type.

Adding/Deleting a User to/from an SNMP Group

You can use the following commands to add or delete a user to/from an SNMP group.

Perform the following configuration in system view.

Table 686 Add/Delete a user to/from an SNMP group

Operation	Command
Add a user to an SNMP group.	snmp-agent usm-user { v1 v2c } <i>username groupname</i> [acl <i>acl-list</i>] snmp-agent usm-user v3 <i>username groupname</i> [authentication-mode { md5 sha } <i>authpassstring</i> [privacy-mode { des56 <i>privpassstring</i> }]] [acl <i>acl-list</i>]
Delete a user from an SNMP group.	undo snmp-agent usm-user { v1 v2c } <i>username groupname</i> undo snmp-agent usm-user v3 <i>username groupname</i> { local engineid <i>engine-id</i> }

You must first configure the SNMP engine ID before configuring the remote user for an agent, because the engine ID is required during the authentication. If you forget to configure the engine ID before adding a user, the operation of adding this user will fail.

For SNMP V1 and V2c, this operation is adding a new community name, while for SNMP V3, this operation is adding a user for an SNMP group.

Creating/Updating View Information or Deleting a View

You can specify the view to control the access to the MIB by SNMP manager. You can use either the predefined views or the self-defined views. You can use the following commands to create, update the information of views or delete a view.

Perform the following configuration in system view.

Table 687 Create/Update view information or delete a view

Operation	Command
Create/Update view information	snmp-agent mib-view { included excluded } <i>view-name oid-tree</i>
Delete a view	undo snmp-agent mib-view <i>view-name</i>

Setting the Size of the SNMP Packet Sent/Received by an Agent

You can use the following commands to set the size of SNMP packet sent/received by an agent.

Perform the following configuration in system view.

Table 688 Set the size of the SNMP packet sent/received by an agent

Operation	Command
Set the size of the SNMP packet sent/received by an agent	snmp-agent packet max-size <i>byte-count</i>
Restore the default size of the SNMP packet sent/received by an agent	undo snmp-agent packet max-size

The agent can receive/send the SNMP packets of the sizes ranging from 484 to 17940, measured in bytes. By default, the size of an SNMP packet is 2000 bytes.

Disabling SNMP Agent

To disable SNMP Agent, perform the following configuration in system view.

Table 689 Disable snmp agent

Operation	Command
Disable snmp agent	undo snmp-agent

If users disable NMP Agent, it will be enabled whatever **snmp-agent** command is configured thereafter.

Displaying and Debugging SNMP

After the above configuration, execute the **display** command in any view to display the running of the SNMP configuration, and to verify the effect of the configuration.

Table 690 Display and debug SNMP

Operation	Command
Display the statistics information about SNMP packets	display snmp-agent statistics
Display the engine ID of the active device	display snmp-agent local-engineid
Display the group name, the security mode, the states for all types of views, and the storage mode of each group of the switch.	display snmp-agent group [<i>group-name</i>]
Display SNMP user information in the group user table	display snmp-agent usm-user [<i>engineid engineid</i> <i>group groupname</i> <i>username username</i>]*
Display the current community name	display snmp-agent community [<i>read</i> <i>write</i>]
Display the current MIB view	display snmp-agent mib-view [<i>exclude</i> <i>include</i>] { <i>viewname mib-view</i> }
Display the contact character strings, location character strings, and the SNMP version of the system	display snmp-agent sys-info [<i>contact</i> <i>location</i> <i>version</i>]*

SNMP Configuration Example

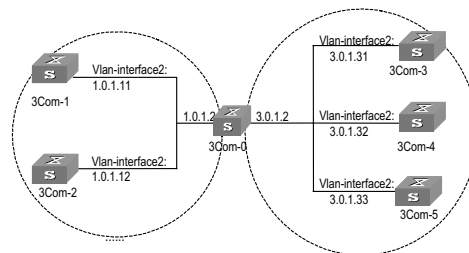
Network requirements

Network Management Station and the switch are connected through the Ethernet. The IP address of Network Management Station is 129.102.149.23 and

that of the VLAN interface on the switch is 129.102.0.1. Perform the following configurations on the switch: setting the community name and access authority, administrator ID, contact and switch location, and enabling the switch to send trap packets.

Network diagram

Figure 174 Network diagram for SNMP configuration



Configuration procedure

Enter the system view.

```
<SW8800> system-view
```

Set the community name, group and user.

```
[SW8800] snmp-agent sys-info version all
[SW8800] snmp-agent community read public
[SW8800] snmp-agent mib include internet 1.3.6.1
[SW8800] snmp-agent group v3 managev3group write internet
[SW8800] snmp-agent usm v3 managev3user managev3group
```

Set the VLAN interface 2 as the interface for network management. Add port GigabitEthernet 2/1/3 to the VLAN 2. This port will be used for network management. Set the IP address of VLAN interface 2 as 129.102.0.1.

```
[SW8800] vlan 2
[3Com-vlan2] port gigabitethernet 2/1/3
[3Com-vlan2] interface vlan 2
[3Com-Vlan-interface2] ip address 129.102.0.1 255.255.0.0
```

Enable SNMP agent to send the trap to network management station whose IP address is 129.102.149.23. The SNMP community is public.

```
[SW8800] snmp-agent trap enable standard authentication
[SW8800] snmp-agent trap enable standard coldstart
[SW8800] snmp-agent trap enable standard linkup
[SW8800] snmp-agent trap enable standard linkdown
[SW8800] snmp-agent target-host trap address udp-domain 129.102.149.23 udp-
port 5000 params securityname public
```

Configure network management system

The PC on which the network management resides requires for login configuration. As for Mib-Browser, the login configuration is as follows: SNMPV1/V2 logs in using the default community name public, and the SNMPV3 logs in using managev3user.

The switch supports 3Com's network management products. Users can query and configure the switch through the network management system. For details, see the manuals for the network management products.

RMON Overview

Remote Network Monitoring (RMON) is a type of IETF-defined MIB. It is the most important enhancement to the MIB II standard. It mainly used for monitoring the data traffic on a segment and even on a whole network. It is one of the widely used Network Management standards by far.

RMON is implemented fully based on the SNMP architecture (which is one of its outstanding advantages) and compatible with the existing SNMP framework, and therefore it is unnecessary to adjust the protocol. RMON includes NMS and the Agent running on the network devices. On the network monitor or detector, RMON Agent tracks and accounts different traffic information on the segment connected to its port, such as the total number of packets on a segment in a certain period of time or that of the correct packets sent to a host. RMON helps the SNMP monitor the remote network device more actively and effectively, which provides a highly efficient means for the monitoring of the subnet operations. RMON can reduce the communication traffic between the NMS and the agent, thus facilitates an effective management over the large interconnected networks.

RMON allows multiple monitors. It can collect data in two ways.

- One is to collect data with a special RMON probe. NMS directly obtains the management information from the RMON probe and controls the network resource. In this way, it can obtain all the information of RMON MIB
- Another way is to implant the RMON Agent directly into the network devices (for example router, switch and HUB), so that the devices become network facilities with RMON probe function. RMON NMS uses the basic SNMP commands to exchange data information with SNMP Agent and collect NM information. However, limited by the device resources, normally, not all the data of RMON MIB can be obtained with this method. In most cases, only four groups of information can be collected. The four groups include alarm information, event information, history information and statistics information.

The switch implements RMON in the second method by far. With the RMON-supported SNMP Agent running on the network monitor, NMS can obtain such information as the overall traffic of the segment connected to the managed network device port, the error statistics and performance statistics, thereby implementing the management (generally remote management) over the network.

Configuring RMON

Before configuring RMON, you must ensure that the SNMP agent is properly configured. See "SNMP Configuration" for the SNMP agent configuration.

The following sections describe the RMON configuration tasks.

- “Adding/Deleting an Entry to/from the Event Table”
- “Adding/Deleting an Entry to/from the Alarm Table”
- “Adding/Deleting an Entry to/from the Extended RMON Alarm Table”
- “Adding/Deleting an Entry to/from the History Control Table”
- “Adding/Deleting an Entry to/from the Statistics Table”

Adding/Deleting an Entry to/from the Event Table

RMON event management defines the event ID and the handling of the event.

You can handle the event in the following ways:

- Keeping logs
- Sending the trap messages to NMS
- Keeping logs and sending the trap messages to NMS

Perform the following configuration in system view.

Table 691 Add/delete an entry to/from the event table

Operation	Command
Add an entry to the event table	rmon event <i>event-entry</i> [description <i>string</i>] { log trap <i>trap-community</i> log-trap <i>log-trapcommunity</i> none } [owner <i>rmon-station</i>]
Delete an entry from the event table	undo rmon event <i>event-entry</i>

Adding/Deleting an Entry to/from the Alarm Table

RMON alarm management can monitor the specified alarm variables such as the statistics on a port. When a value of the monitored data exceeds the defined threshold, an alarm event will be generated. And then the events are handled according to the definition, which is decided in the event management.



*Before adding an entry to the alarm table, you need to define the event referenced in the alarm table by using the **rmon event** command.*

Perform the following configuration in system view.

Table 692 Add/delete an entry to/from the alarm table

Operation	Command
Add an entry to the alarm table	rmon alarm <i>entry-number</i> <i>alarm-variable</i> <i>sampling-time</i> { delta absolute } rising-threshold <i>threshold-value1</i> <i>event-entry1</i> falling-threshold <i>threshold-value2</i> <i>event-entry2</i> [owner <i>text</i>]
Delete an entry from the alarm table	undo rmon alarm <i>entry-number</i>

After you defined the alarm entry, the system then processes the entry in the following way:

- 1 Sampling the defined alarm-variable according to the time interval sampling-time that you have set
- 2 Comparing the sampled value with the configured threshold and handling them in the way described in the following table

Table 693 Handling the alarm entry

Case	Processing
The sampled value is greater than the configured upper limit threshold-value1	The defined event event-entry1 is triggered
The sampled value is less than the configured lower limit threshold-value2	The defined event event-entry2 is triggered

Adding/Deleting an Entry to/from the Extended RMON Alarm Table

You can use the command to add/delete an entry to/from the extended RMON alarm table. The extended alarm entry performs mathematical operation to the sampled value of the alarm variable, and then the result will be compared with the configured threshold to implementing the alarm function.



*Before adding extended alarm entry, you need to define the referenced event in the extended alarm entry by using the **rmon event** command.*

You can define up to 50 prialarm entries.

Perform the following configuration in system view.

Table 694 Add/delete an entry to/from the extended RMON alarm table

Operation	Command
Add an entry to the extended RMON alarm table	rmon prialarm <i>entry-number alarm-var</i> [<i>alarm-des</i>] <i>sampling-timer</i> { delta absolute changeratio } rising-threshold <i>threshold-value1 event-entry1</i> falling-threshold <i>threshold-value2 event-entry2</i> entrytype { forever cycle <i>cycle-period</i> } [owner <i>text</i>]
Delete an entry from the extended RMON alarm table	undo rmon prialarm <i>entry-number</i>

After you define the extended alarm entry, the system processes the entry in the following way:

- 1 Sampling the defined prialarm-formula according to the time interval sampling-time that you have set
- 2 Performing the operation to the sampled value according to the defined formula *prialarm-formula*
- 3 Comparing the result with the configured threshold and handling them in the way described in the following table

Table 695 Handling the extended alarm entry

Case	Processing
The result is greater than the configured upper limit threshold-value1	The defined event event-entry1 is triggered

Table 695 Handling the extended alarm entry

Case	Processing
The result is less than the configured lower limit threshold-value2	The defined event event-entry2 is triggered

Adding/Deleting an Entry to/from the History Control Table

The history data management helps you set the history data collection, periodical data collection and storage of the specified ports. The sampling information includes the utilization ratio, error counts and total number of packets.

You can use the following commands to add/delete an entry to/from the history control table.

Perform the following configuration in Ethernet port view.

Table 696 Add/delete an entry to/from the history control table

Operation	Command
Add an entry to the history control table.	rmon history <i>entry-number</i> buckets <i>number</i> interval <i>sampling-interval</i> [owner <i>text-string</i>]
Delete an entry from the history control table.	undo rmon history <i>entry-number</i>

History control entry calculates various data at the sampling time interval. You can use the **display rmon history** command to view the information of the history control entry.

Adding/Deleting an Entry to/from the Statistics Table

The RMON statistics management concerns the port usage monitoring and error statistics when using the ports. The statistics include collision, CRC and queuing, undersize packets or oversize packets, timeout transmission, fragments, broadcast, multicast and unicast messages and the usage ratio of bandwidth.

You can use the following commands to add/delete an entry to/from the statistics table.

Perform the following configuration in Ethernet port view.

Table 697 Add/delete an entry to/from the statistics table

Operation	Command
Add an entry to the statistics table	rmon statistics <i>entry-number</i> [owner <i>text-string</i>]
Delete an entry from the statistics table	undo rmon statistics <i>entry-number</i>

Statistics entry calculates the accumulated information starting from the time defined by an event. You can use the **display rmon history** command to view the information of the statistics entry.

Displaying and Debugging RMON

After the above configuration, execute the **display** command in any view to display the running of the RMON configuration, and to verify the effect of the configuration.

Table 698 Display and debug RMON

Operation	Command
Display the RMON statistics	display rmon statistics [port-num]
Display the history information of RMON	display rmon history [port-num]
Display the alarm information of RMON	display rmon alarm [alarm-table-entry]
Display the extended alarm information of RMON	display rmon prialarm [prialarm-table-entry]
Display the RMON event	display rmon event [event-table-entry]
Display the event log of RMON	display rmon eventlog [event-number]

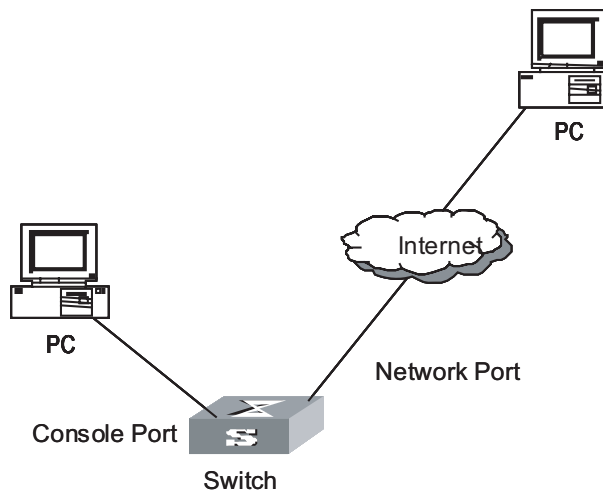
RMON Configuration Example

Network requirements

Set an entry in RMON Ethernet statistics table for the Ethernet port performance, which is convenient for network administrators' query.

Network diagram

Figure 175 Network diagram for RMON configuration



Configuration procedure

Configure RMON.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Ethernet 3/1/1
[3Com-Ethernet3/1/1] rmon statistics 1 owner 3Com-rmon
```

View the configurations in user view.

```
<SW8800> display rmon statistics Ethernet 3/1/1
Statistics entry 1 owned by 3Com-rmon is VALID.
Interface : Ethernet3/1/1<ifIndex.201326602>
etherStatsOctets      : 0          , etherStatsPkts      : 0
etherStatsBroadcastPkts : 0          , etherStatsMulticastPkts : 0
etherStatsUndersizePkts : 0          , etherStatsOversizePkts : 0
etherStatsFragments   : 0          , etherStatsJabbers    : 0
etherStatsCRCAlignErrors : 0          , etherStatsCollisions : 0
etherStatsDropEvents (insufficient resources): 0
Packets received according to length (etherStatsPktsXXXtoYYYOctets):
```

```

64      : 0          , 65-127 : 0          , 128-255 : 0
256-511: 0          , 512-1023: 0        , 1024-max : 0

```

Configure an event before configuring alarm and prialarm.

```

[SW8800]rmon event 1 log owner 3Com-rmon
[SW8800]display rmon event 1
Event table 1 owned by 3Com-rmon is VALID.
  Description: null.
  Will cause log when triggered, last triggered at 1days 01h:42m:09s.

```

#Configure an alarm group.

```

[SW8800]rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 delta rising_threshold 1000
 1 falling_threshold 100 1 owner 3Com-rmon
[SW8800]dis rmon alarm 1
Alarm table 1 owned by 3Com-rmon is VALID.
  Samples type           : delta
  Variable formula       : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Description            : Ethernet2/1/1
  Sampling interval      : 10(sec)
  Rising threshold       : 1000(linked with event 1)
  Falling threshold      : 100(linked with event 1)
  When startup enables   : risingOrFallingAlarm
  Latest value           : 0

```

Configure an extended alarm group.

```

[SW8800]rmon prialarm 1 ((.1.3.6.1.4.1.2011.6.1.2.1.1.2.0-.1.3.6.1.4.1.2011.
6.1.2.1.1.3.0)*100/.1.3.6.1.4.1.2011.6.1.2.1.1.2.0) prialarm1 10 delta risi
ng_threshold 70 1 falling_threshold 50 1 entrytype forever
[SW8800]display rmon prialarm 1
Prialarm table 1 owned by null is VALID.
  Samples type           : delta
  Variable formula       : ((.1.3.6.1.4.1.2011.6.1.2.1.1.2.0-.1.3.6.1.4.1.
2011.6.1.2.1.1.
3.0)*100/.1.3.6.1.4.1.2011.6.1.2.1.1.2.0)
  Description            : prialarm1
  Sampling interval      : 10(sec)
  Rising threshold       : 70(linked with event 1)
  Falling threshold      : 50(linked with event 1)
  When startup enables   : risingOrFallingAlarm
  This entry will exist : forever.
  Latest value           : 0

```



The "0" in black means the memory of slot 0 is queried.

66

NTP CONFIGURATION

Brief Introduction to NTP

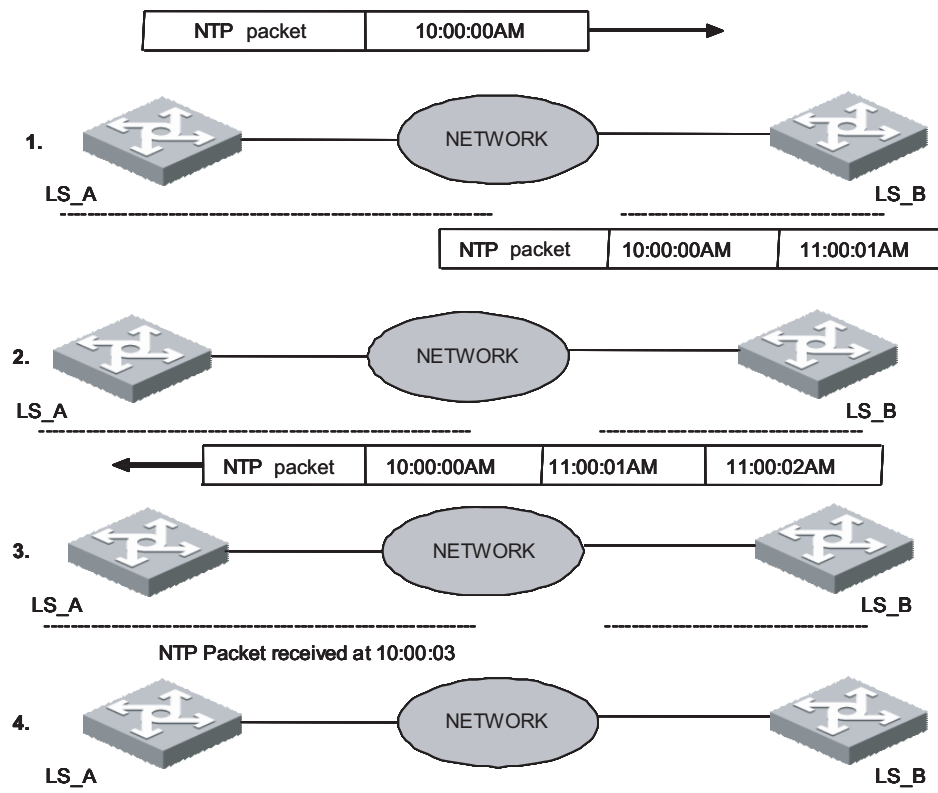
NTP Functions As the network topology gets more and more complex, it becomes important to synchronize the clocks of the equipment on the whole network. Network Time Protocol (NTP) is the TCP/IP that advertises the accurate time throughout the network.

NTP ensures the consistency of the following applications:

- For the increment backup between the server and the client, NTP ensures the clock synchronization between the two systems.
- For multiple systems that coordinate to process a complex event, NTP ensures them to reference the same clock and guarantee the right order of the event.
- Guarantee the normal operation of the inter-system Remote Procedure Call (RPC).
- Record for an application when a user logs in to a system, a file is modified, or some other operation is performed.

Basic Operating Principle of NTP

The following figure illustrates the basic operating principle of NTP:

Figure 176 Basic operating principle of NTP

In the figure above, Switch A and Switch B are connected through the Ethernet port. They have independent system clocks. Before implement automatic clock synchronization on both switches, we assume that:

- Before synchronizing the system clocks on Switch A and B, the clock on Switch A is set to 10:00:00am, and that on B is set to 11:00:00am.
- Switch B serves as an NTP time server. That is, Switch A synchronizes the local clock with the clock of B.
- It takes one second to transmit a data packet from either A or B to the opposite end.

The system clocks are synchronized as follows:

- Switch A sends an NTP packet to Switch B. The packet carries the timestamp 10:00:00am (T_1) that tells when it left Switch A.
- When the NTP packet arrives at Switch B, Switch B adds a local timestamp 11:00:01am (T_2) to it.
- When the NTP packet leaves Switch B, Switch B adds another local timestamp 11:00:02am (T_3) to it.
- When Switch A receives the acknowledgement packet, it adds a new timestamp 10:00:03am (T_4) to it.

Now, Switch A collects enough information to calculate the following two important parameters:

- The delay for a round trip of an NTP packet traveling between Switch A and B: $\text{Delay} = (T_4 - T_1) - (T_3 - T_2)$.
- Offset of Switch A clock relative to Switch B clock: $\text{offset} = ((T_2 - T_1) + (T_4 - T_3)) / 2$.

In this way, Switch A uses the above-mentioned information to set the local clock and synchronize it with the clock on Switch B.

The operating principle of NTP is briefly introduced above. For details, refer to RFC1305.

NTP Configuration

NTP is used for time synchronization throughout a network. The following sections describe the NTP configuration tasks.

- "Configuring NTP Operating Mode"
- "Configuring NTP ID Authentication"
- "Setting NTP Authentication Key"
- "Setting Specified Key as Reliable"
- "Designating an Interface to Transmit NTP Messages"
- "Setting NTP Master Clock"
- "Setting Authority to Access a Local Switch"
- "Setting Maximum Local Sessions"

Configuring NTP Operating Mode

You can set the NTP operating mode of a Switch according to its location in the network and the network structure. The following settings are for your reference:

- If you set a remote server as the time server of the local equipment, the local Switch works as an NTP Client.
- If you set a remote server as a peer of the local Switch, the local equipment operates in Symmetric Active mode.
- If you configure an interface on the local Switch to transmit NTP broadcast packets, the local Switch will operate in Broadcast mode.
- If you configure an interface on the local Switch to receive NTP broadcast packets, the local Switch will operate in Broadcast Client mode.
- If you configure an interface on the local Switch to transmit NTP multicast packets, the local Switch will operate in Multicast mode.
- If you configure an interface on the local Switch to receive NTP multicast packets, the local Switch will operate in Multicast Client mode.

To configure NTP:

- Configure NTP server mode
- Configure NTP peer mode
- Configure NTP broadcast server mode
- Configure NTP broadcast client mode
- Configure NTP multicast server mode
- Configure NTP multicast client mode

Configuring NTP Server Mode

Set a remote server whose ip address is *ip-address* as the local time server. *ip-address* specifies a host address other than a broadcast, multicast or reference clock IP address. In this case, the local Switch operates in Client mode. In this mode, only the local client synchronizes its clock with the clock of the remote server, while the reverse synchronization will not happen.

Perform the following configuration in system view.

Table 699 Configure NTP time server

Operation	Command
Configure NTP time server	ntp-service unicast-server <i>ip-address</i> [version <i>number</i> authentication-keyid <i>keyid</i> source-interface <i>interface-type interface-number</i> priority]*
Cancel NTP server mode	undo ntp-service unicast-server <i>ip-address</i>

NTP version number *number* ranges from 1 to 3 and defaults to 3; it supports authentication but will not be the first choice for time server..

Configuring NTP Peer Mode

Set a remote server whose ip address is *ip-address* as the peer of the local equipment. In this case, the local equipment operates in Symmetric Active mode. *ip-address* specifies a host address other than a broadcast, multicast or reference clock IP address. In this mode, both the local Switch and the remote server can synchronize their clocks with the clock of opposite end.

Perform the following configuration in system view.

Table 700 Configure NTP peer mode

Operation	Command
Configure NTP peer mode	ntp-service unicast-peer <i>ip-address</i> [version <i>number</i> authentication-keyid <i>keyid</i> source-interface <i>interface-type interface-number</i> priority]*
Cancel NTP peer mode	undo ntp-service unicast-peer <i>ip-address</i>

NTP version number *number* ranges from 1 to 3 and defaults to 3; it does not support authentication and will not be the first choice for time server.

Configuring NTP Broadcast Server Mode

Designate an interface on the local Switch to transmit NTP broadcast packets. In this case, the local equipment operates in broadcast mode and serves as a broadcast server to broadcast messages to its clients regularly.

Perform the following configuration in VLAN interface view.

Table 701 Configure NTP broadcast server mode

Operation	Command
Configure NTP broadcast server mode	ntp-service broadcast-server [authentication-keyid <i>keyid</i> version <i>number</i>]*
Cancel NTP broadcast server mode	undo ntp-service broadcast-server

By default, no broadcast service is configured and the version number *number* defaults to 3.

This command can only be configured on the interface where the NTP broadcast packets will be transmitted.

Configuring NTP Broadcast Client Mode

Designate an interface on the local Switch to receive NTP broadcast messages and operate in broadcast client mode. The local Switch listens to the broadcast from the server. When it receives the first broadcast packets, it starts a brief client/server mode to switch messages with a remote server for estimating the network delay. Thereafter, the local Switch enters broadcast client mode and continues listening to the broadcast and synchronizes the local clock according to the broadcast message that arrived .

Perform the following configuration in VLAN interface view.

Table 702 Configure NTP broadcast client mode

Operation	Command
Configure NTP broadcast client mode	ntp-service broadcast-client
Disable NTP broadcast client mode	undo ntp-service broadcast-client

This command can only be configured on the interface where the NTP broadcast packets will be received.

Configuring NTP Multicast Server Mode

Designate an interface on the local Switch to transmit NTP multicast packets. In this case, the local equipment operates in Multicast mode and serves as a Multicast server to multicast messages to its clients regularly.

Perform the following configuration in VLAN interface view.

Table 703 Configure NTP Multicast server mode

Operation	Command
Configure NTP Multicast server mode	ntp-service multicast-server [<i>ip-address</i>] [authentication-keyid <i>keyid</i> ttl <i>ttl-number</i> version <i>number</i>]*
Cancel NTP Multicast server mode	undo ntp-service multicast-server [<i>ip-address</i>]

NTP version number *number* ranges from 1 to 3 and defaults to 3; the authentication key ID *keyid* ranges from 1 to 4294967295; *ttl-number* of the multicast packets ranges from 1 to 255; And the multicast IP address defaults to 224.0.1.1. Actually, for the Switch 8800 Family series, you can set 224.0.1.1 as the multicast IP address only.

This command can only be configured on the interface where the NTP multicast packet will be transmitted.

Configuring NTP Multicast Client Mode

Designate an interface on the local Switch to receive NTP multicast messages and operate in multicast client mode. The local Switch listens to the multicast from the server. When it receives the first multicast packets, it starts a brief client/server mode to switch messages with a remote server for estimating the network delay. Thereafter, the local Switch enters multicast client mode and continues listening to the multicast and synchronizes the local clock by the multicast message that arrived.

Perform the following configuration in VLAN interface view.

Table 704 Configure NTP multicast client mode

Operation	Command
Configure NTP multicast client mode	ntp-service multicast-client [<i>ip-address</i>]
Cancel NTP multicast client mode	undo ntp-service multicast-client

Multicast IP address *ip-address* defaults to 224.0.1.1; this command can only be configured on the interface where the NTP multicast packets will be received. Actually, for the Switch 8800 Family series, you can set 224.0.1.1 as the multicast IP address only.

Configuring NTP ID Authentication

Enable NTP authentication, set MD5 authentication key, and specify the reliable key. A Client will synchronize itself by a server only if the server can provide a reliable key.

Perform the following configuration in system view.

Table 705 Configure NTP authentication

Operation	Command
Enable NTP authentication	ntp-service authentication enable
Disable NTP authentication	undo ntp-service authentication enable

Setting NTP Authentication Key

This configuration task is to set NTP authentication key.

Perform the following configuration in system view.

Table 706 Configure NTP authentication key

Operation	Command
Configure NTP authentication key	ntp-service authentication-keyid <i>number</i> authentication-mode md5 <i>value</i>
Remove NTP authentication key	undo ntp-service authentication-keyid <i>number</i>

Key number *number* ranges from 1 to 4294967295; the key *value* contains 1 to 16 ASCII characters.

Setting Specified Key as Reliable

This configuration task is to set the specified key as reliable.

Perform the following configuration in system view.

Table 707 Set the specified key as reliable

Operation	Command
Set the specified key as reliable	ntp-service reliable authentication-keyid <i>key-number</i>
Cancel the specified reliable key.	undo ntp-service reliable authentication-keyid <i>key-number</i>

Key number *key-number* ranges from 1 to 4294967295

Designating an Interface to Transmit NTP Messages

If the local equipment is configured to transmit all the NTP messages, these packets will have the same source IP address, which is taken from the IP address of the designated interface.

Perform the following configuration in system view.

Table 708 Designate an interface to transmit NTP messages

Operation	Command
Designate an interface to transmit NTP messages	ntp-service source-interface <i>interface-type interface-number</i>
Cancel the interface to transmit NTP messages	undo ntp-service source-interface

An interface is specified by *interface-type interface-number*. The source address of the packets will be taken from the IP address of the interface. If the **ntp-service unicast-server** or **ntp-service unicast-peer** command also designates a transmitting interface, use the one designated by them.

Setting NTP Master Clock

This configuration task is to set the external reference clock or the local clock as the NTP master clock.

Perform the following configuration in system view.

Table 709 Set the external reference clock or the local clock as the NTP master clock

Operation	Command
Set the external reference clock or the local clock as the NTP master clock.	ntp-service refclock-master [<i>ip-address</i>] [<i>stratum</i>]
Cancel the NTP master clock settings	undo ntp-service refclock-master [<i>ip-address</i>]

ip-address specifies the IP address 127.127.1.u of a reference clock, in which u ranges from 0 to 3. *stratum* specifies how many stratum the local clock belongs to and ranges from 1 to 15.

The IP address defaults 127.127.1.0, and the stratum defaults to 8.

Setting Authority to Access a Local Switch

Set authority to access the NTP services on a local Switch. This is a basic and brief security measure, compared to authentication. An access request will be matched with **peer**, **server**, **server only**, and **query only** in an ascending order of the limitation. The first matched authority will be given.

Perform the following configuration in system view.

Table 710 Set authority to access a local switch

Operation	Command
Set authority to access a local switch	ntp-service access { query synchronization server peer } <i>acl-number</i>
Cancel settings of the authority to access a local switch	undo ntp-service access { query synchronization server peer }

IP address ACL number is specified through the *acl-number* parameter and ranges from 2000 to 2999. The meanings of other authority levels are as follows:

query: Allow control query for the local NTP service only.

synchronization: Allow request for local NTP time service only.

server: Allow local NTP time service request and control query. However, the local clock will not be synchronized by a remote server.

peer: Allow local NTP time service request and control query. And the local clock will also be synchronized by a remote server.

Setting Maximum Local Sessions

This configuration task is to set the maximum local sessions.

Perform the following configurations in system view.

Table 711 Set the maximum local sessions

Operation	Command
Set the maximum local sessions	ntp-service max-dynamic-sessions <i>number</i>
Resume the maximum number of local sessions	undo ntp-service max-dynamic-sessions

number specifies the maximum number of local sessions, ranges from 0 to 100, and defaults to 100.

Displaying and Debugging NTP

After completing the above configurations, you can use the **display** command to show how NTP runs and verify the configurations according to the outputs.

In user view, you can use the **debugging** command to debug NTP.

Table 712 Display and debug NTP

Operation	Command
Display the status of NTP service	display ntp-service status
Display the status of sessions maintained by NTP service	display ntp-service sessions [verbose]
Display the brief information about every NTP time server on the way from the local equipment to the reference clock source.	display ntp-service trace
Enable NTP debugging	debugging ntp-service { access adjustment authentication event filter packet parameter refclock selection synchronization validity all }

NTP Configuration Example

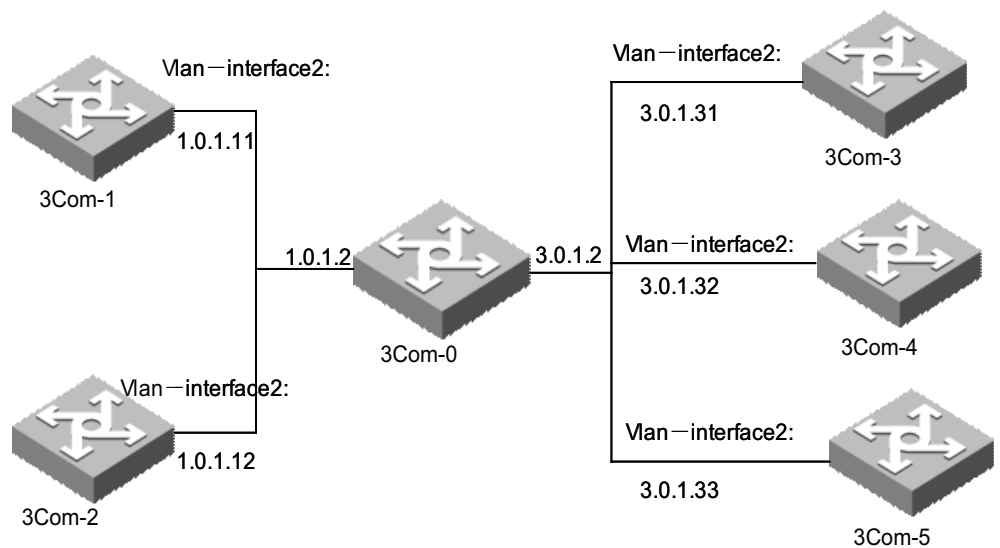
Configuring a NTP Server

Network requirements

On 3Com1, set local clock as the NTP master clock at stratum 2. On 3Com2, configure 3Com1 as the time server in server mode and set the local equipment as in client mode. (Note: 3Com1 supports to configure the local clock as the master clock)

Network diagram

Figure 177 Typical NTP configuration network diagram



Configuration procedure

Configure Switch 3Com1:

Enter system view.

```
<3Com1> system-view
```

Set the local clock as the NTP master clock at stratum 2.

```
[3Com1] ntp-service refclock-master 2
```

Configure Switch 3Com2:

Enter system view.

```
<3Com2> system-view
```

Set 3Com1 as the NTP server.

```
[3Com2] ntp-service unicast-server 1.0.1.11
```

The above examples synchronized 3Com2 by 3Com1. Before the synchronization, the 3Com2 is shown in the following status:

```
[3Com2] display ntp-service status
clock status: unsynchronized
clock stratum: 16
reference clock ID: none
nominal frequency: 100.0000 Hz
actual frequency: 100.0000 Hz
clock precision: 2^17
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 0.00 ms
peer dispersion: 0.00 ms
reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

After the synchronization, 3Com2 turns into the following status:

```
[3Com2] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequency: 60.0002 Hz
Actual frequency: 60.0002 Hz
Clock precision: 2^17
Clock offset: -9.8258 ms
Root delay: 27.10 ms
Root dispersion: 49.29 ms
Peer dispersion: 10.94 ms
Reference time: 19:21:32.287 UTC Oct 24 2004(C5267F3C.49A61E0C)
```

By this time, 3Com2 has been synchronized by 3Com1 and is at stratum 3, higher than 3Com1 by 1.

Display the sessions of 3Com2 and you will see 3Com2 has been connected with 3Com1.

```
[3Com2] display ntp-service sessions
source      reference stratum reach poll  now offset  delay disper
*****
[12345]1.0.1.11 LOCAL(0) 3 377 64 16 -0.4 0.0 0.9
note: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured
```

NTP Peer Configuration Example

Network requirements

On 3Com3, set local clock as the NTP master clock at stratum 2. On 3Com2, configure 3Com1 as the time server in server mode and set the local equipment as in client mode. At the same time, 3Com5 sets 3Com4 as its peer. (Note: 3Com3 supports to configure the local clock as the master clock)

Network diagram

See Figure 7-2.

Configuration procedure

Configure Switch 3Com3.

Enter system view.

```
<3Com3> system-view
```

Set the local clock as the NTP master clock at stratum 2.

```
[3Com3] ntp-service refclock-master 2
```

Configure Switch 3Com4.

Enter system view.

```
<3Com4> system-view
```

Set 3Com1 as the NTP server at stratum 3 after synchronization.

```
[3Com4] ntp-service unicast-server 3.0.1.31
```

Set 3Com5 as peer

```
[3Com4] ntp-service unicast-peer 3.0.1.33
```

Configure Switch 3Com5.(3Com4 has been synchronized by 3Com3)

Enter system view.

```
<3Com5> system-view
```

Set the local clock as the NTP master clock at stratum 1.

```
[3Com5] ntp-service refclock-master 1
```

After performing local synchronization, set 3Com4 as a peer.

```
[3Com5] ntp-service unicast-peer 3.0.1.32
```

The above examples configure 3Com4 and 3Com5 as peers and configure 3Com5 as in active peer mode and 3Com4 in passive peer mode. Since 3Com5 is at stratum 1 and 3Com4 is at stratum 3, synchronize 3Com4 by 3Com5.

After synchronization, 3Com4 status is shown as follows:

```
[3Com4] display ntp-service status
Clock status: synchronized
Clock stratum: 2
Reference clock ID: 3.0.1.31
Nominal frequency: 60.0002 Hz
Actual frequency: 60.0002 Hz
Clock precision: 2^17
Clock offset: -9.8258 ms
Root delay: 27.10 ms
Root dispersion: 49.29 ms
Peer dispersion: 10.94 ms
Reference time: 19:21:32.287 UTC Oct 24 2004 (C5267F3C.49A61E0C)
```

By this time, 3Com4 has been synchronized by 3Com5 and it is at stratum 2, or higher than 3Com5 by 1.

Display the sessions of 3Com4 and you will see 3Com4 has been connected with 3Com5.

```
[Quidwa4] display ntp-service sessions
source      reference strata reach poll  now offset  delay disper
*****
[12345]3.0.1.33 LOCAL(0)  2    377   64   16    0.0   0.0   0.9
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

Configure NTP Broadcast Mode

Network requirements

On 3Com3, set local clock as the NTP master clock at stratum 2 and configure to broadcast packets from Vlan-interface2. Configure 3Com4 and 3Com1 to listen to the broadcast from their Vlan-interface2 respectively. (Note: 3Com3 supports to configure the local clock as the master clock)

Network diagram

See Figure 7-2.

Configuration procedure

Configure Switch 3Com3:

Enter system view.

```
<3Com3> system-view
```

Set the local clock as the NTP master clock at stratum 2.

```
[3Com3] ntp-service refclock-master 2
```

Enter Vlan-interface2 view.

```
[3Com3] interface vlan-interface 2
```

Set it as broadcast server.

```
[3Com3-Vlan-Interface2] ntp-service broadcast-server
```

Configure Switch 3Com4:

Enter system view.

```
<3Com4> system-view
```

Enter Vlan-interface2 view.

```
[3Com4] interface vlan-interface 2
[3Com4-Vlan-Interface2] ntp-service broadcast-client
```

Configure Switch 3Com1:

Enter system view.

```
<3Com1> system-view
```

Enter Vlan-interface2 view.

```
[3Com1] interface vlan-interface 2
[3Com1-Vlan-Interface2] ntp-service broadcast-client
```

The above examples configured 3Com4 and 3Com1 to listen to the broadcast through Vlan-interface2, 3Com3 to broadcast packets from Vlan-interface2. Since 3Com1 and 3Com3 are not located on the same segment, they cannot receive any broadcast packets from 3Com3, while 3Com4 is synchronized by 3Com3 after receiving its broadcast packet.

After the synchronization, you can find the state of 3Com4 as follows:

```
[3Com4] display ntp-service status
clock status: synchronized
clock stratum: 3
reference clock ID: LOCAL(0)
nominal frequency: 100.0000 Hz
actual frequency: 100.0000 Hz
clock precision: 2^17
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 10.94 ms
peer dispersion: 10.00 ms
reference time: 20:54:25.156 UTC Mar 7 2002(C0325201.2811A112)
```

By this time, 3Com4 has been synchronized by 3Com3 and it is at stratum 3, higher than 3Com3 by 1.

Display the status of 3Com4 sessions and you will see 3Com4 has been connected to 3Com3.

```
[3Com2] display ntp-service sessions
source      reference      stra reach poll now offset delay disper
[12345]127.127.1.0 LOCAL(0) 7 377 64 57 0.0 0.0 1.0
[5]1.0.1.11 LOCAL(0) 3 0 64 - 0.0 0.0 0.0
[5]128.108.22.44 0.0.0.0 16 0 64 - 0.0 0.0 0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

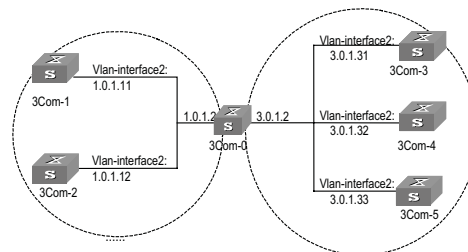
Configure NTP Multicast Mode

Network requirements

3Com3 sets the local clock as the master clock at stratum 2 and multicast packets from Vlan-interface2. Set 3Com4 and 3Com1 to receive multicast messages from their respective Vlan-interface2. (Note: 3Com3 supports to configure the local clock as the master clock)

Network diagram

Figure 178 Network diagram for NTP configuration example



Configuration procedure

Configure Switch 3Com3:

```

# Enter system view.

<3Com3> system-view

# Set the local clock as a master NTP clock at stratum 2.

[3Com3] ntp-service refclock-master 2

# Enter Vlan-interface2 view.

[3Com3] interface vlan-interface 2

# Set it as a multicast server.

[3Com3-Vlan-Interface2] ntp-service multicast-server

```

Configure Switch 3Com4:

```

# Enter system view.

<3Com4> system-view

# Enter Vlan-interface2 view.

[3Com4] interface vlan-interface 2

# Enable multicast client mode.

[3Com4-Vlan-Interface2] ntp-service multicast-client

```

Configure Switch 3Com1:

```

# Enter system view.

<3Com1> system-view

# Enter Vlan-interface2 view.

[3Com1] interface vlan-interface 2

# Enable multicast client mode.

[3Com1-Vlan-Interface2] ntp-service multicast-client

```

The above examples configure 3Com4 and 3Com1 to receive multicast messages from Vlan-interface2, 3Com3 multicast messages from Vlan-interface2. Since 3Com1 and 3Com3 are not located on the same segments, 3Com1 cannot receive the multicast packets from 3Com3, while 3Com4 is synchronized by 3Com3 after receiving the multicast packet.

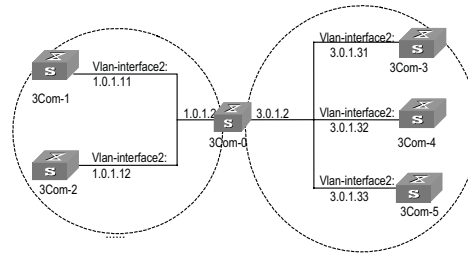
Configure Authentication-Enabled NTP Server Mode

Network requirements

3Com1 sets the local clock as the NTP master clock at stratum 2. 3Com2 sets 3Com1 as its time server in Server mode and itself in Client mode and enables authentication. (Note: 3Com1 supports to configure the local clock as the master clock)

Network diagram

Figure 179 Network diagram for NTP configuration example



Configuration procedure

Configure Switch 3Com1.

Enter system view.

```
<3Com1> system-view
```

Set the local clock as the master NTP clock at stratum 2.

```
[3Com1] ntp-service refclock-master 2
```

Configure Switch 3Com2.

Enter system view.

```
<3Com2> system-view
```

Set 3Com1 as time server.

```
[3Com2] ntp-service unicast-server 1.0.1.11
```

Enable authentication.

```
[3Com2] ntp-service authentication enable
```

Set the key.

```
[3Com2] ntp-service authentication-keyid 42 authentication-mode md5
aNiceKey
```

Set the key as reliable.

```
[3Com2] ntp-service reliable authentication-keyid 42
[Qudiway2] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

The above examples synchronized 3Com2 by 3Com1. Since 3Com1 has not been enabled authentication, it cannot synchronize 3Com2. And now let us do the following additional configurations on 3Com1.

Enable authentication.

```
[3Com1] ntp-service authentication enable
```

Set the key.

```
[3Com1] ntp-service authentication-keyid 42 authentication-mode md5  
aNiceKey
```

Configure the key as reliable.

```
[3Com1] ntp-service reliable authentication-keyid 42
```


67

SSH TERMINAL SERVICE

SSH Terminal Service

SSH Overview This chapter introduces the secure shell (SSH) feature. When a user telnets to the switch from an insecure network, the SSH feature can provide secure information and powerful authentication functionality, thereby protecting the switch from attacks such as IP address spoofing and clear text password interception attacks.

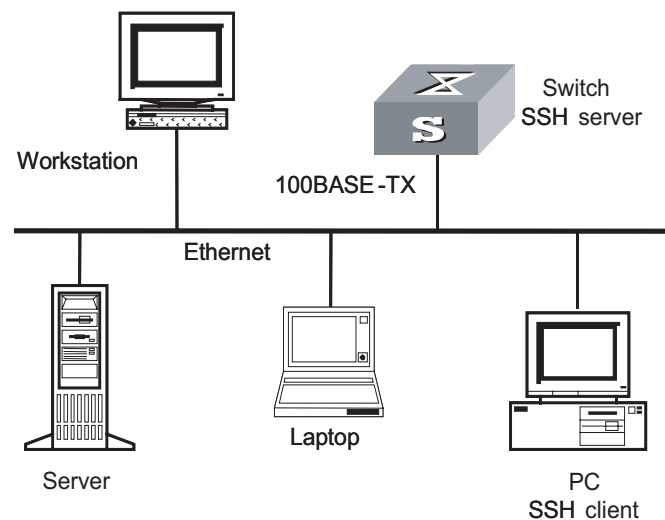
The switch can act as either SSH server or SSH client. When used as an SSH server, the switch supports multiple connections with SSH clients; when used as an SSH client, the switch supports SSH connections with the SSH server-enabled switch, UNIX hosts, and so on.

Currently, the switch supports SSH 2.0.

Figure 180 and Figure 181 illustrate two methods for establishing an SSH channel between a client and the server:

- Connect through a LAN
- Connect through a WAN

Figure 180 Establish an SSH channel through a LAN



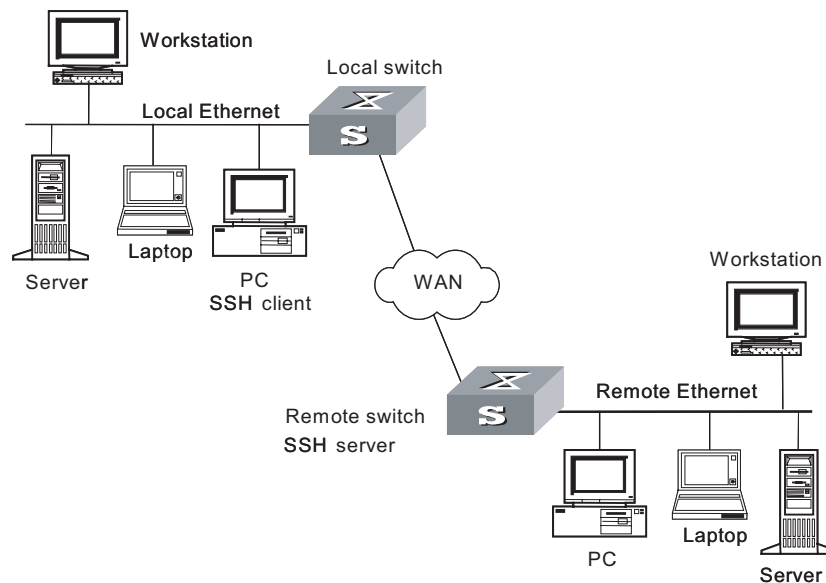


Figure 181 Establish an SSH channel through a WAN

To establish an SSH authentication secure connection, the server and the client must go through the following five phases:

1 Version number negotiation:

- The client sends a TCP connection request.
- After the TCP connection is established, the server and the client negotiate the version number.
- If the negotiation succeeds, the key algorithm negotiation phase starts; otherwise, the server tears down the TCP connection.

2 Key algorithm negotiation:

- The server generates an RSA key pair randomly, and sends the public key in the key pair to the client.
- The client uses the public key from the server and a random number generated locally (in length of eight bytes) as parameters to calculate the session key.
- Using the public key from the server, the client encrypts the random number for calculating the session key and sends the result to the server.
- Using the local private key, the server decrypts the data sent by the client and obtains the random number used by the client.
- The server uses the public key and the random number from the client as parameters to calculate the session key with the same algorithm as on the client. The resulting key is 16 bytes long.

On completion of the above steps, the server and the client obtains the same session key. During the session, both ends use the same session key to perform encryption and decryption, thereby guaranteeing the security of data transfer.

3 Authentication mode negotiation:

- The client sends its username information to the server.

- The server initiates a procedure to authenticate the user. If the server is configured not to authenticate the user, the process proceeds to session request phase directly.
- The client employs an authentication mode to authenticate the server till the authentication succeeds or the server tears down the connection because of timeout.



SSH provides two authentication modes: password authentication and RSA authentication.

- 1 Password authentication procedure:
 - The client sends the username and password to the server;
 - The server compares the username and password sent from the client with the local configuration. If it finds an exact match, the authentication succeeds.
- 2 RSA authentication procedure:
 - The server configures an RSA public key for the client;
 - The client sends its RSA public key member module to the server;
 - The server performs validity authentication on the member module. If the authentication succeeds, the server generates a random number, encrypts it using the RSA public key from the client, and sends the encrypted information back to the client;
 - Both the server and the client uses the random number and the session ID with the length of 16 characters as parameters to calculate the authentication data;
 - The client sends the authentication data it generates to the server;
 - The server compares the authentication data from the client with that locally calculated. If they match, the authentication succeeds.
- 3 Session request: If the authentication succeeds, the client sends a session request to the server. When the server has successfully processed the request, SSH enters the interactive session phase.
- 4 Interactive session: The client and the server exchange data till the session is over.

SSH Server Configuration

The following table describes the SSH server configuration tasks.

Table 713 SSH2.0 configuration tasks

Operation	Command	Description
Enter system view	system-view	-
Enter user interface view of VTY type	user-interface vty X X	-
Set the protocol supported by current user interface	protocol inbound { all ssh telnet }	Optional
Return to system view	quit	-
Generate a local RSA key pair	rsa local-key-pair create	Required
Destroy a local RSA key pair	rsa local-key-pair destroy	Optional
Configure the SSH user authentication mode	ssh user <i>username</i> [authentication-type { password rsa password-publickey all }]	Required By default, users are unable to log in.

Table 713 SSH2.0 configuration tasks

Operation	Command	Description
Configure default authentication type for SSH users	ssh authentication-type default [password rsa all password-publickey]	Required; By default, users are unable to log in to the system.
Configure the updating cycle of the server key	ssh server rekey-interval <i>hours</i>	Optional By default, the system does not update the server key.
Configure the SSH authentication timeout	ssh server timeout <i>seconds</i>	Optional By default, it is 60 seconds.
Configure the number of SSH authentication retries	ssh server authentication-retries <i>times</i>	Optional By default, it is three times.
Enter public key view	rsa peer-public-key <i>key-name</i>	Required
Enter public key edit view to edit the key	public-key-code begin	Required
Exit public key edit view	peer-public-key end	Required
Assign the public key for an SSH user	ssh user <i>username</i> assign rsa-key <i>keyname</i>	Required
Configure first-authentication SSH server	ssh client first-time enable	Optional By default, the system does not perform the first authentication.
Configure the SSH compatibility mode	ssh server compatible_ssh1x enable	Optional By default, the server is compatible with the SSH1.x client.

Configuring the protocol the current user interface supports

Use this configuration task to specify the protocol the current user interface supports.

Perform the following configuration in VTY user interface view.

Table 714 Configure the protocol the current user interface supports

Operation	Command
Configure the protocol supported by the current user interface	protocol inbound { all ssh telnet }

By default, the system supports all protocols.



CAUTION:

- If the supported protocol configured in the user interface is SSH, make sure to configure the authentication mode for logging into the user interface to authentication-mode scheme (using AAA authentication mode).
- If the authentication mode is configured as **authentication-mode password** or **authentication-mode none**, the configuration of **protocol inbound ssh** will fail, and vice versa.

Generating or destroying an RSA key pair

Use this configuration task to generate or destroy an RSA key pair (including the host key and server key) of the server. The naming conventions for the keys are *switchname + host* and *switchname + server* respectively.

After this command is entered, the system prompts you to input the number of the key pair bits. Pay attention to the following:

- The host key and the server key must have a difference of at least 128 bits in length.
- The minimum and maximum lengths for the host key and the server key are 512 bits and 2048 bits respectively.

Perform the following configuration in system view.

Table 715 Generate an RSA key pair

Operation	Command
Generate an RSA key pair	rsa local-key-pair create
Destroy an RSA key pair	rsa local-key-pair destroy



CAUTION:

- Generating the RSA key pair of the server is the first step to perform after SSH login.
- This command needs to be performed only once; you need not re-perform it after rebooting the switch.
- If a key pair exists before the configuration, a prompt will appear asking if you want to replace it.
- When an SSH user logs in, the key generated by the server must be longer than 768 bits. By default, the key generated by the server is 1,024 bits.

Configuring the user authentication mode

Use this configuration task to specify the authentication mode for an SSH user. You must specify an authentication mode for a new user; otherwise, the new user will not be able to log in.

Table 716 Configure the authentication mode for an SSH user

Operation	Command	Description
Enter system view	system-view	-
Configure an authentication mode for SSH users	ssh user <i>username</i> authentication-type { password rsa password-publickey all }	By default, no login authentication mode is specified, that is, SSH users are unable to log in.

Note the following points:

- 1 The authentication mode configured for SSH users is used preferably. For example, an SSH user is added whose service type is set to *stelnet* but configured with no

authentication mode. In this case, whatever the default authentication mode, the user cannot log in because the user's authentication mode is null.

- 2 Standard radius does not support user-level attributes. Therefore, during remote authentication, you must specify the server type in the radius scheme as 3Com or extend and specify the correct user level on the radius server before the corresponding user level can be obtained after successful login; otherwise, you can log in only as a 0-level user.

Configure the default user authentication mode

Use this configuration to specify the default authentication mode for SSH users.

An SSH user is authenticated in one of the following two cases:

- 1 A user configured with an authentication mode will be authenticated in the authentication mode configured.
- 2 A user not configured with any authentication mode will be authenticated in the default authentication mode:
 - If the default authentication mode is **password** or **all**, the user can log in successfully by using a local or remote SSH username and password.
 - If the default authentication mode is **rsa** or **password-publickey**, the user must be assigned a key and authenticated in key mode through a local SSH user. An SSH user in key mode does not support remote authentication.

If no default authentication mode is available, the user cannot log in because the user is not configured with any authentication mode; therefore, a user must be configured with an authentication mode before logging in successfully.

The default authentication mode is NULL; that is, no authentication mode is configured.

Table 717 Configure the default authentication mode for SSH users

Operation	Command	Description
Enter system view	system-view	-
Configure the default authentication mode for SSH users	ssh authentication-type default { password rsa all password-publickey }	If no default authentication mode is available and no authentication mode is configured for a user, the user will not be able to log in.

Configuring the updating cycle of the server key

Use this configuration task to set the updating cycle of the server key to secure the SSH connection in best effort.

Perform the following configuration in system view

Table 718 Configure the updating cycle of the server key

Operation	Command
Configure the updating cycle of the server key	ssh server rekey-interval hours
Cancel the updating cycle configuration	undo ssh server rekey-interval

By default, the system does not update the server key.

Configuring the authentication timeout

Use this configuration task to set the authentication timeout of SSH connections.

Perform the following configuration in system view.

Table 719 Set the SSH authentication timeout

Operation	Command
Set the SSH authentication timeout	ssh server timeout <i>seconds</i>
Restore the default SSH authentication timeout	undo ssh server timeout

By default, the authentication timeout is 60 seconds.

Configuring the number of authentication retries

Use this configuration task to set the number of authentication retries an SSH user can request for a connection, thereby preventing illegal behaviors such as malicious guessing.

Perform the following configuration in system view.

Table 720 Configure the number of SSH authentication retries

Operation	Command
Configure the number of SSH authentication retries	ssh server authentication-retries <i>times</i>
Restore the default number of SSH authentication retries	undo ssh server authentication-retries

By default, the number of authentication retries is 3.

Entering the public key view

Use this configuration command to enter the public key view and specify the name of the public key of the client.

Perform the first configuration in the following table in system view.

Table 721 Public key configuration

Operation	Command
Enter the public key view	rsa peer-public-key <i>key-name</i>
Exit the public view and return to the system view	peer-public-key end



*The configuration commands are applicable to the environments where the server employs RSA authentication and **password-publickey** authentication on SSH users. If the server adopts password authentication on SSH users, these configurations are not necessary.*

Entering the public key edit view

After entering the public key view by the **rsa peer-public-key** command, you can use the **public-key-code begin** command to enter the public key edit view and input the public key of the client.

When inputting the public key, you may type spaces between the characters (the system will delete the spaces automatically), or press <Enter> and then continue to input the key. Note that the public key must be a hexadecimal string coded in the public key format.

Perform the following configuration in public key view.

Table 722 Enter the public key edit view

Operation	Command
Enter the public key edit view	public-key-code begin

Exiting the public key edit view

Use this configuration task to return from the public key edit view to the public key view and save the input public key. Before saving the input public key, the system will check the validity of the key:

- If the public key string contains any illegal character, the configured key is invalid;
- If the configured key is valid, it will be saved to the public keys in the system.

Perform the following configuration in public key edit view.

Table 723 Exit the public key edit view

Operation	Command
Exit the public key edit view	public-key-code end

Specifying the public key for an SSH user

Use this configuration task to specify an existing public key for an SSH user.

Perform the following configuration in system view.

Table 724 Specify the public key for an SSH user

Operation	Command
Specify the public key for an SSH user	ssh user <i>username</i> assign rsa-key <i>keyname</i>
Cancel the corresponding relationship between the user and the public key	undo ssh user <i>username</i> assign rsa-key

Configuring the server compatibility mode

Use this configuration task to set whether the server should be compatible with the SSH 1.x client.

Perform the following configuration in system view.

Table 725 Configure the compatibility mode

Operation	Command
Set the server to be compatible with the SSH 1.x client	ssh server compatible_ssh1x enable
Set the server to be incompatible with the SSH 1.x client	undo ssh server compatible_ssh1x

By default, the server is compatible with the SSH 1.x client.

SSH Client Configuration

The following sections describe the SSH client configuration tasks.

- Set to perform the first-time authentication on the SSH server to be accessed
- Specifying the public key of the server
- Configuring the first-time authentication of the server

Starting the SSH client

Use this configuration task to enable the SSH client, establish the connection with the server, and carry out interactive session.

Perform the following configuration in system view.

Table 726 Start the SSH client

Operation	Command
Start the SSH client	ssh2 { <i>host-ip</i> <i>host-name</i> } [<i>port-num</i>] [prefer_kex { <i>dh_group1</i> <i>dh_exchange_group</i> }] [prefer_ctos_cipher { <i>des</i> <i>3des</i> <i>aes128</i> }] [prefer_stoc_cipher { <i>des</i> <i>3des</i> <i>aes128</i> }] [prefer_ctos_hmac { <i>sha1</i> <i>sha1_96</i> <i>md5</i> <i>md5_96</i> }] [prefer_stoc_hmac { <i>sha1</i> <i>sha1_96</i> <i>md5</i> <i>md5_96</i> }]

Specifying the public key of the server

Use this configuration task to allocate an existing public key to the client.

Perform the following configuration in system view.

Table 727 Specify the public key of the server

Operation	Command
Specify the public key of the server	ssh client <i>server-ip</i> assign rsa-key <i>keyname</i>
Cancel the corresponding relationship between the server and the public key	undo ssh client <i>server-ip</i> assign rsa-key

Configuring the first-time authentication of the server

Use this configuration task to configure or cancel the first-time authentication of the server performed by the SSH client.

The first-time authentication means that when the SSH client accesses the server for the first time in the case that there is no local copy of the server's public key, the user can choose to proceed to access the server and save a local copy of the server's public key; when the client accesses the server next time, it uses the saved public key to authenticate the server.

Perform the following configuration in system view.

Table 728 Configure/cancel the first-time authentication of the server

Operation	Command
Configure the first-time authentication of the server	ssh client first-time enable
Cancel the first-time authentication of the server	undo ssh client first-time

By default, the client does not perform the first-time authentication.

Displaying and Debugging SSH

On completion of the above configurations, you can use the **display** command in any view to view the operation of the configured SSH and further verify the result of the configurations. You can also debug SSH by performing the **debugging** command in user view.

Table 729 Display information relevant to SSH

Operation	Command
Display the public key of the host key pair and the server key pair of the server	display rsa local-key-pair public
Display the public key of the specified RSA key pair of the client	display rsa peer-public-key [brief name keyname]
Display the SSH status information and session information	display ssh server { status session }
Display information about the SSH user	display ssh user-information [username]

Perform the following **debugging** command configuration in user view.

Table 730 Debug information relevant to SSH

Operation	Command
Enable SSH debugging	debugging ssh server { vty index all }
Disable SSH debugging	undo debugging ssh server { vty index all }

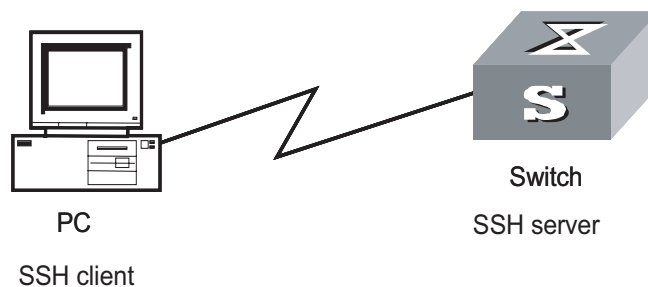
SSH Server Configuration Example

Network requirements

As shown in Figure 182, a PC (SSH client) running SSH 2.0-enabled client software establishes a local connection with the switch (SSH server) to better guarantee the security of exchanged information.

Network diagram

Figure 182 Network diagram for SSH server



Configuration procedure

1 Generate the RSA key.

```
[SW8800] rsa local-key-pair create
```



If the configuration for generating the local key has already been completed, skip this step.

2 Set the user login authentication mode.

The following shows the configuration methods for both password authentication and RSA public key authentication.

■ Password authentication.

Create the local user client001, and set the authentication mode of the user interface to AAA.

```
[SW8800] user-interface vty 0 4
[3Com-ui-vty0-4] authentication-mode scheme
```

Specify the login protocol for user client001 as SSH.

```
[3Com-ui-vty0-4] protocol inbound ssh
[SW8800] local-user client001
New local user added
[3Com-luser-client001] password simple 3Com
[3Com-luser-client001] service-type ssh
[3Com-luser-client001] quit
[SW8800] ssh user client001 authentication-type password
```



You can use the default values for SSH authentication timeout and retries. After completing the above configurations, you can run the SSH 2.0-enabled client software on any other terminal connected with the switch and access the switch with the username client001 and password 3Com.

■ RSA authentication.

Create the local user client001, and set the authentication mode of the user interface to AAA.

```
[SW8800] user-interface vty 0 4
[3Com-ui-vty0-4] authentication-mode scheme
```

Specify the login protocol for user client002 as SSH.

```
[3Com-ui-vty0-4] protocol inbound ssh
```

Set the authentication mode for the remote user on the switch to RSA.

```
[SW8800] ssh user client002 authentication-type rsa
```

Using the SSH 2.0-enabled client software, randomly generate an RSA key pair and send the public key to the server.

Configure the public key of the client.

```
[SW8800] rsa peer-public-key sw8800002
[3Com-rsa-public-key] public-key-code begin
[8505A-rsa-public-key]public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[8505A-rsa-key-code]30818602 8180507E DB32853A 58D19A3E B216BDC9 AA37535A
[8505A-rsa-key-code]6F6B0FE8 B5D4BCD2 A1C8B127 93212202 938D98D8 8A6AB88B
[8505A-rsa-key-code]C8E96A97 3774B383 036CFBE2 59C24887 585D97AA 88616CB9
[8505A-rsa-key-code]4C35029B B4929D58 B9F2A372 99C0F029 D69FE3D3 0469894B
[8505A-rsa-key-code]417BAD0D 921AA895 2F9B6ADE 9E755B66 4E6CAE2F 94C339E3
[8505A-rsa-key-code]5E301FD0 31FC490B 67E1B657 49750201 25
[3Com-rsa-key-code] public-key-code end
[3Com-rsa-public-key] peer-public-key end
[SW8800]
```

#Allocate an existent public key sw8800002 to user client002.

```
[SW8800] ssh user client002 assign rsa-key sw8800002
```

Start the SSH client software on the terminal preserving the RSA private key, and perform the corresponding configurations to establish the SSH connection.

SSH Client Configuration Example

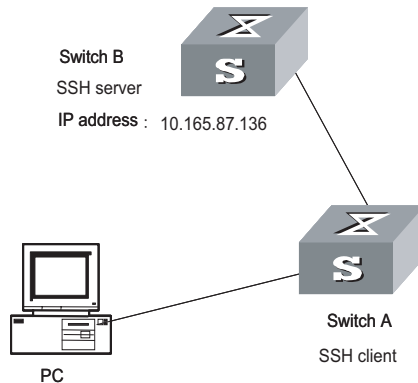
Network requirements

As shown in Figure 183:

- Switch A is used as an SSH client.
- Switch B is used as the SSH server, and the IP address is 10.165.87.136.

Network diagram

Figure 183 Network diagram for SSH client



Configuration procedure

Configure the client to perform the first-time authentication of the server.

- Employ password authentication mode, and start using the default encryption algorithm.

Log onto the SSH2 server with IP address 10.165.87.136.

```
[SW8800] ssh2 10.165.87.136
Please input the username:sshuser1
Trying 10.165.87.136
Press CTRL+K to abort
```

```

Connected to 10.165.87.136 ...
Enter password:
*****
*           All rights reserved (1997-2004)           *
*   Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*****
<SW8800>

```

Configure the client to authenticate the server for the first time.

```

<SW8800> system-view
[SW8800] ssh client first-time enable

```

Access the remote server and perform operations.

- Employ RSA public key authentication mode, and start using the corresponding encryption algorithm configured.

```

[SW8800] ssh2 10.165.87.136 22 prefer_kex dh_group1 prefer_ctos_cipher des
prefer_stoc_cipher 3des prefer_ctos_hmac md5 prefer_stoc_hmac md5
Please input the username: sshuser1
Trying 10.165.87.136...
Press CTRL+K to abort
Connected to 10.165.87.136...
*****
*           All rights reserved (1997-2004)           *
*   Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*****
<SW8800>

```

Configure the client to authenticate the server for the first time.

```

<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh client first-time enable

```

Access the remote server and perform operations.

SFTP Service

- | | |
|----------------------------------|--|
| SFTP Overview | Secure FTP is established on SSH connections, which makes remote users able to securely log in to the switch and perform file management and transfer operations such as system upgrade, and thereby providing higher security for data transfer. At the same time, since the switch can be used as a client, users can log in to remote devices to transfer files securely. |
| SFTP Server Configuration | <p>SFTP server configuration tasks are described in this section:</p> <ul style="list-style-type: none"> ■ Configuring the default service type and the default directory for SFTP users ■ Configure the service type to be used by the user ■ Starting or shutting down the SFTP server |

Configuring the default service type and the default directory for SFTP users

Perform the following configuration in system view.

Table 731 Configure the default service type and the default directory for SFTP users

Operation	Command
Configure the default service type and the default directory for SFTP users	ssh service-type default { all [sftp-directory <i>directory</i>] sftp [sftp-directory <i>directory</i>] stelnet }
Restore the default service type and the default directory for SFTP users	undo ssh service-type default

The default service type is NULL and the default directory for SFTP users is NULL. If a user is configured with a service type and directory, the service type and directory of the user, rather than the default service type, are used. Therefore, if a single user is configured, the user must be configured with complete authentication type and service type; otherwise, the user may not be able to log in because of being configured incompletely.

Note the following points:

- The default SFTP directory flash: is configured for a user whose service type is set to SFTP or all. In this case, the priority of the directory is higher than the default priority.
- Currently, for remote authentication, the default authentication mode must be configured in the system before a remote user can log in successfully.

Configuring the service type to be used

Use this configuration to set the type of SSH service to be used.

Perform the following configuration in system view.

Table 732 Configure the service type to be used

Operation	Command
Configure the service type to be used	ssh user <i>username</i> service-type { stelnet sftp [sftp-directory <i>directory</i>] all [sftp-directory <i>directory</i>] }
Restore the default service type	undo ssh user <i>username</i> service-type

By default, the service type is **stelnet**.

Starting the SFTP server

Perform the following configuration in system view.

Table 733 Start the SFTP server

Operation	Command
Start the SFTP server	sftp server enable
Shut down the SFTP server	undo sftp server enable

By default, the SFTP server is shut down.

SFTP Client Configuration

The following table describes the SFTP client configuration tasks.

Table 734 SFTP client configuration tasks

Num	Operation	Command	Description
1	Enter system view	<SW8800> system-view [SW8800]	-
2	Starting the SFTP client	sftp ipaddr [prefer_kex { dh_group1 dh_exchange_group }] [prefer_ctos_cipher { des 3des aes128 }] [prefer_stoc_cipher { des 3des aes128 }] [prefer_ctos_hmac { sha1 sha1_96 md5 md5_96 }] [prefer_stoc_hmac { sha1 sha1_96 md5 md5_96 }]	Required
3	Shut down the SFTP client	sftp-client> bye sftp-client> exit sftp-client> quit	Optional
4	SFTP directory operation	Chang the current directory	sftp-client> cd [remote-path]
		Return to the upper directory	sftp-client> cdup
		Display the current directory	sftp-client> pwd
		Display the file list in the specified directory	sftp-client> dir [remote-path] sftp-client> ls [remote-path]
		Delete a directory on the server	sftp-client> rmdir remote-path
		Change the name of the specified file on the server	sftp-client> rename oldname newname
5	SFTP file operation	Download a file from the remote server	sftp-client> get remote-file [local-file]
		Upload a local file to the remote server	sftp-client> put local-file [remote-file]
		Display the file list in the specified directory	sftp-client> dir [remote-path] sftp-client> ls [remote-path]
		Delete a file from the server	sftp-client> remove remote-file sftp-client> delete remote-file
6	Command help on the client	sftp-client> help [command]	Optional

Starting the SFTP client

Use this configuration task to start the SFTP client program, establish a connection with the remote SFTP server, and enter the SFTP client view.

Perform the following configuration in system view.

Table 735 Start the SFTP client

Operation	Command
Start the SFTP client	<code>sftp ipaddr [prefer_kex { dh_group1 dh_exchange_group }] [prefer_ctos_cipher { des 3des aes128 }] [prefer_stoc_cipher { des 3des aes128 }] [prefer_ctos_hmac { sha1 sha1_96 md5 md5_96 }] [prefer_stoc_hmac { sha1 sha1_96 md5 md5_96 }]</code>

Shutting down the SFTP client

Use this configuration task to shut down the SFTP client program.

Perform the following configuration in SFTP client view.

Table 736 Shut down the SFTP client

Operation	Command
	<code>bye</code>
Shut down the SFTP client	<code>exit</code>
	<code>quit</code>



The three commands, **bye**, **exit**, and **quit**, have the same functionality. You can also use the **quit** command in port group view.

SFTP directory operations

As shown in Table 737, available SFTP directory operations include: change or display the current directory, create or delete a directory, display the specified file or directory.

Perform the following configuration in SFTP client view.

Table 737 SFTP directory operations

Operation	Command
Change the current directory	<code>cd remote-path</code>
Return to the upper directory	<code>cdup</code>
Display the current directory	<code>pwd</code>
Display the list of files in the specified directory	<code>dir [remote-path]</code> <code>ls [remote-path]</code>
Create a new directory on the server	<code>mkdir remote-path</code>
Delete a directory from the server	<code>rmdir remote-path</code>



The **dir** command and the **ls** command have the same functionality.

SFTP file operations

As shown in Table 738, available SFTP file operations include: change the name of a file, download a file, upload a file, display the list of files, and delete a file.

Perform the following configuration in SFTP user view.

Table 738 SFTP file operations

Operation	Command
Change the name of the specified file on the server	rename <i>old-name new-name</i>
Download a file from the remote server	get <i>remote-file</i> [<i>local-file</i>]
Upload a local file to the remote server	put <i>local-file</i> [<i>remote-file</i>]
Display the list of files in the specified directory	dir [<i>remote-path</i>] ls [<i>remote-path</i>]
Delete a file from the server	delete <i>remote-file</i> remove <i>remote-file</i>



- The **dir** command and the **ls** command have the same functionality.
- The **delete** command and the **remove** command have the same functionality.

Displaying help information

Use this command to display command-relevant help information such as the format of the command, parameter configurations, and so on.

Perform the following configuration in SFTP client view.

Table 739 Display help information for client commands

Operation	Command
Display help information for client commands	help [<i>command-name</i>]

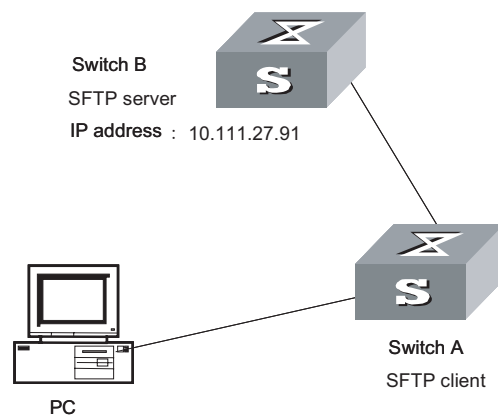
SFTP Configuration Example

Network requirements

As shown in Figure 184:

- Switch A is used as the SFTP server, and its IP address is 10.111.27.91;
- Switch B is used as the SFTP client;
- An SFTP user is configured with the username "8040" and password "3com".

Network diagram

Figure 184 Network diagram for SFTP

Configuration procedure**1** Configure Switch B.

Start the SFTP server.

```
[SW8800] sftp server enable
```

Specify the service type as SFTP.

```
[SW8800] ssh user 8040 service-type sftp
```

Set the authentication mode to password.

```
[SW8800] ssh user 8040 authentication-type password
```

2 Configure Switch A

Configure the server with a public key whose name is the IP address of the server.

```
[SW8800] rsa peer-public-key 10.111.27.91
[3Com-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[8505A-rsa-key-code]30818602 8180507E DB32853A 58D19A3E B216BDC9 AA37535A
[8505A-rsa-key-code]6F6B0FE8 B5D4BCD2 A1C8B127 93212202 938D98D8 8A6AB88B
[8505A-rsa-key-code]C8E96A97 3774B383 036CFBE2 59C24887 585D97AA 88616CB9
[8505A-rsa-key-code]4C35029B B4929D58 B9F2A372 99C0F029 D69FE3D3 0469894B
[8505A-rsa-key-code]417BAD0D 921AA895 2F9B6ADE 9E755B66 4E6CAE2F 94C339E3
[8505A-rsa-key-code]5E301FD0 31FC490B 67E1B657 49750201 25
[3Com-rsa-key-code] public-key-code end
[3Com-rsa-public-key] peer-public-key end
[SW8800] ssh client 10.111.27.91 assign rsa-key 10.111.27.91
```

Establish the SSH connection between the client and the server.

```
[SW8800] ssh2 10.111.27.91
Please input the username:8040
Trying
Press CTRL+K to abort
Connected to 10.111.27.91 ...
Enter password:3com
*****
*           All rights reserved (1997-2004)           *
*   Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*****
<SW8800>
```

Establish a connection with the remote SFTP server and enter the SFTP client view.

```
<SW8800> system-view
[SW8800] sftp 10.111.27.91
```

Display the current directory of the server, delete file z, and check if the directory has been deleted successfully.

```
sftp-client> dir
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 vrpcfg.cfg
```

```

-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey1
drwxrwxrwx 1 noone nogroup 0 Sep 01 06:22 new
-rwxrwxrwx 1 noone nogroup 225 Sep 01 06:55 pub
-rwxrwxrwx 1 noone nogroup 0 Sep 01 08:00 z
sftp-client> delete z
Remove this File? (Y/N)
flash:/zy
File successfully Removed
sftp-client> dir
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 vrpcfg.cfg
-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey1
drwxrwxrwx 1 noone nogroup 0 Sep 01 06:22 new
-rwxrwxrwx 1 noone nogroup 225 Sep 01 06:55 pub

```

Create a new directory new1, and check if the new directory has been created successfully.

```

sftp-client> mkdir new1
New path created
sftp-client> dir
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 vrpcfg.cfg
-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey1
drwxrwxrwx 1 noone nogroup 0 Sep 01 06:22 new
-rwxrwxrwx 1 noone nogroup 225 Sep 01 06:55 pub
drwxrwxrwx 1 noone nogroup 0 Sep 02 06:30 new1

```

Change the directory name new1 to new2, and check if the directory name has been changed successfully.

```

sftp-client> rename new1 new2
sftp-client> dir
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 vrpcfg.cfg
-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey1
drwxrwxrwx 1 noone nogroup 0 Sep 01 06:22 new
-rwxrwxrwx 1 noone nogroup 225 Sep 01 06:55 pub
drwxrwxrwx 1 noone nogroup 0 Sep 02 06:33 new2

```

Download file pubkey2 from the server to a local device, and change the file name to pu.

```

sftp-client> get pubkey2 pu
Downloading file successfully ended

```

Upload local file pu to the server, change the file name to puk, and check if the operations are successful.

```

sftp-client> put pu puk
Uploading file successfully ended
sftp-client> dir
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 vrpcfg.cfg
-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey1
drwxrwxrwx 1 noone nogroup 0 Sep 01 06:22 new

```

```
drwxrwxrwx  1 noone  nogroup          0 Sep 02 06:33 new2
-rwxrwxrwx  1 noone  nogroup        283 Sep 02 06:35 pu
-rwxrwxrwx  1 noone  nogroup        283 Sep 02 06:36 puk
sftp-client>
```

```
# Exit SFTP.
```

```
sftp-client> quit
Bye
[SW8800]
```

File System Configuration

File System Overview The switch provides a file system module for user's efficient management over the storage devices such as Flash memory. The file system offers file access and directory management, mainly including creating the file system, creating, deleting, modifying and renaming a file or a directory and opening a file.

By default, the file system needs user's confirmation before executing the commands, such as deleting or overwriting a file, which may make losses.

Based on the operated objects, the file system operation can be divided as follows. The following sections describe the file system configuration tasks.

- "Directory Operation"
- "File Operation"
- "Storage Device Operation"
- "Setting the Prompt Mode of the File System"



3Com Switch 8800 Family series switches (hereinafter referred to as Switch 8800 Family series) support master/slave fabric switchover. The two modules both have a program system. The program user can operate the programs on both modules. When you specify the bootstrap APP program for use by the slave module at the next startup, make sure that the URL of the program starts with "slot[No.]#[flash: | cf:]/", where [No.] is the slave module number, and [flash: | cf:] is the name of the equipment, which can be a flash card or CR card. For example, if the slave module is on slot 1, the URL of 8500.app program on the slave module is "slot1#flash:/8500.app".

Directory Operation The file system can be used to create or delete a directory, display the current working directory, and display the information about the files or directories under a specified directory. You can use the following commands to perform directory operations.

Perform the following configuration in user view.

Table 740 Directory operation

Operation	Command
Create a directory	mkdir <i>directory</i>
Delete a directory	rmdir <i>directory</i>

Table 740 Directory operation

Operation	Command
Display the current working directory	pwd
Display the information about directories or files	dir [/ all] [file-url]
Change the current directory	cd directory

File Operation

The file system can be used to delete or undelete a file and permanently delete a file. Also, it can be used to display file contents, rename, copy and move a file and display the information about a specified file. You can use the following commands to perform file operations.

Perform the following configuration in user view.

Table 741 File operation

Operation	Command
Delete a file	delete [/unreserved] file-url
Undelete a file	undelete file-url
Delete a file from the recycle bin permanently	reset recycle-bin [file-url]
View contents of a file	more file-url
Rename a file	rename fileurl-source fileurl-dest
Copy a file	copy fileurl-source fileurl-dest
Move a file	move fileurl-source fileurl-dest
Display the information about directories or files	dir [/ all] [file-url]
Execute the specified batch file (system view)	execute filename



CAUTION: When you use the **delete** command without the **unreserved** option to delete a file, the file is in fact saved in the recycle bin and still occupies some of the storage space. So, the frequent uses of this command may results in insufficient storage space of the switch. In this case, you should find out the unused files kept in the recycle bin and permanently delete them with the **reset recycle-bin** command to reclaim the storage space.



The directory and file names on the switch have the following limitation:

- The maximum length of a directory or file name is 64 characters.
- The maximum length of a full path name (containing the device name, single directory name and file name) is 136 characters.
- The **move** command takes effect only when the source and destination files are in the same device.

Storage Device Operation

The file system can be used to format a specified memory device. You can use the following commands to format a specified memory device.

Switch supports compact flash (CF) card. After a CF card is inserted successfully, you can use such common commands as **dir**, **cd**, **copy**, **delete**, **move** to perform operations on the files in the card. You can also stop the CF card through a command before dismounting it.

Considering that when dismounting the CF card you may be performing the write operation on it, the switch provides the **umount** command which can stop the CF card to ensure the safety and consistency of the file operations on it, that is, you must execute the **umount** command to stop the CF card before dismounting it.

The system saves logs in the CF card. The log file is saved in the root directory with the name logfileX.txt, where the X is an integral number ranging from 1 to 5.

The log file is recorded in the CF card in text format. You can use the **more** command to display the log file on the switch.

Note that:

- Before dismounting the CF card, you must use the **umount** command first to avoid the data lost in the buffer.
- After using the **umount** command, you can dismount the CF card from the slot. When inserted, the CF card is enabled automatically.
- When the light of the CF card is in the constant bright state, there may be no write or read operation. But you are recommended not to hot insert/dismount the CF card for data may still exist in the buffer.

Perform the following configuration in user view.

Table 742 Storage device operation

Operation	Command
Format the storage device	format <i>filesystem</i>
Restore the space of the storage device	fixdisk <i>device</i>
Delete the CF card	umount <i>device</i>

Setting the Prompt Mode of the File System

The following command can be used for setting the prompt mode of the current file system.

Perform the following configuration in system view.

Table 743 File system operation

Operation	Command
Set the file system prompt mode.	file prompt { alert quiet }

69

DEVICE MANAGEMENT

Device Management Overview

With the device management function, the switch can display the current running state and event debugging information about the slots, thereby implementing the maintenance and management of the state and communication of the physical devices. In addition, there is a command available for rebooting the system, when some function failure occurs.

Device Management Configuration

The main device management tasks are to check the status of the modules, CPU, and the memory usage of the switch.

The following sections describe the configuration tasks for device management:

- “Rebooting the Switch”
- “Enabling the Timing Reboot Function”
- “Specifying the Bootstrap Programs for the Switch”
- “Upgrading BootROM”
- “Setting Slot Temperature Limit”
- “Updating Service Processing Modules”

Rebooting the Switch

It would be necessary for users to reboot the switch when failure occurs.

Perform the following configuration in user view.

Table 744 Reboot the switch

Operation	Command
Root the switch	reboot [slot slot-no]

Enabling the Timing Reboot Function

After you enable the timing reboot function on the switch, the switch will be rebooted on the specified time.

Perform the following configuration in user view, and **display schedule reboot** command can be performed in any view.

Table 745 Enable the Timing Reboot Function

Operation	Command
Enable the timing reboot function of the switch, and set specified time and date	schedule reboot at hh:mm [yyyy/mm/dd]
Enable the timing reboot function of the switch, and set waiting time	schedule reboot delay { hhh:mm mmm }

Table 745 Enable the Timing Reboot Function

Operation	Command
Cancel the parameter configuration of timing reboot function of the switch	undo schedule reboot
Check the parameter configuration of the reboot terminal service of the current switch	display schedule reboot



The precision of switch timer is 1 minute. The switch will reboot in one minute when time comes to the specified rebooting point.

Specifying the Bootstrap Programs for the Switch

You can specify two bootstrap programs for both active and standby SRPCs of the switch, with one used as the primary program and the other as the backup program. You can use the following command to specify the bootstrap programs for the switch:

Table 746 Specify a bootstrap program for the switch

Operation	Command	Remarks
Specify the bootstrap program for the switch	boot boot-loader { primary backup } file-url [slot slot-number]	Execute this command in user view.

If the switch fails to boot up through the specified bootstrap program, it retries to boot up by using a program in the flash memory or the CF card. If it fails again, the switch fails to start.

The switch select one application program as bootstrap program from Flash or CF card according to the different values of flag BootDev. The detail is as follows:

- There are two primary bootstrap programs: one is in the Flash card (assume it is A); the other is in the CF card (assume it is B).
- There are two backup programs too: one is in the Flash card (assume it is C); the other is in the CF card (assume it is D).
- There is one flag BootDev.

You can view or modify the names of the bootstrap programs and enable equipment flag BootDev.

The detailed rules that the switch follows in selecting a bootstrap program are as follows in Table 3-4.

Table 747 The sequence of bootstrap program selection by the switch

BootDev Value of for boot from primary bootstrap program	BootDev value for boot from backup bootstrap program	Bootstrap program selection sequence
0	0	A, C, B, D
0	1	A, D, B, C
1	1	B, D, A, C
1	0	B, C, A, D



The 3Com Switch 8800 Family series switches (hereinafter referred to as Switch 8800 Family series) support master/slave fabric switchover. The two modules both have a program system. The program user can operate the programs on both modules. When you specify the bootstrap APP program for use by the slave module at the next startup, make sure that the URL of the program starts with "slot[No.]#[flash: | cf:]/", where [No.] is the slave module number, and [flash: | cf:] is the name of the equipment, which can be a flash card or CR card. For example, if the slave module is on slot 1, the URL of 8500.app program on the slave module is "slot1#flash:/8500.app".

Upgrading BootROM

You can use followed command to upgrade the BootROM with the BootROM program in the Flash Memory. This configuration task facilitates the remote upgrade. You can upload the BootROM program file from a remote end to the switch by FTP and then use this command to upgrade the BootROM.

Perform the following configuration in user view.

Table 748 Upgrade BootROM

Operation	Command
Upgrade BootROM	boot bootrom <i>file-url slot slot-num-list</i>

Setting Slot Temperature Limit

The switch system alarms when the temperature on a slot exceeds the preset limit.

Perform the following configuration in user view.

Table 749 Set slot temperature limit

Operation	Command
Set slot temperature limit	temperature-limit <i>slot-no down-value up-value</i>
Restore temperature limit to default value	undo temperature-limit <i>slot-no</i>

Updating Service Processing Modules

The size of the flash for a main control module in a Switch 8800 Family series routing switch is 16MB, while the size of current host software including the host application of the application module reaches over 15MB. If a compact flash (CF) card is not configured, the current flash cannot provide enough room to save loading files. Therefore for the Switch 8800 Family series routing switch with the main control module of a 16MB flash, the application module cannot be updated according to the original procedure. To update it, you need to execute the following command to download host software containing the application file of the application module host application to the system's synchronous dynamic random access memory (SDRAM).



If you configure a CF card or the flash room of a subsequent main control module expands to 64MB, you need not to change the method to update modules. Then when loading files you only need to choose the APP files containing the application file of service processing module to update common interface modules and service processing modules.

Perform the following configuration in system view.

Table 750 Update service processing modules

Operation	Command
Download the host software of service processing module to the system memory	update l3plus slot <i>slot-no</i> filename <i>file-name</i> ftpserver <i>server-name</i> username <i>user-name</i> password <i>password</i> [port <i>port-num</i>]

**CAUTION:**

- When you use the **update l3plus** command to update service processing modules, you must use the switch host APP file which includes the load program of L3PLUS service processing modules.
- The maximum size of L3PLUS update file loaded by the **update l3plus** command is 24 M.

Displaying and Debugging Device Management

After the above configuration, execute **display** command in any view to display the running of the device management configuration, and to verify the effect of the configuration.

Table 751 Display and Debug device management

Operation	Command
Display the module types and running states of each card.	display device [detail] [shelf <i>shelf-no</i>] [frame <i>frame-no</i>] [slot <i>slot-no</i>]
Display the application deployed on next startup	display boot-loader
Display the running state of the built-in fans.	display fan [<i>fan-id</i>]
Display the Used status of switch memory	display memory [slot <i>slot-no</i>]
Display the state of the power.	display power [<i>power-ID</i>]
Display CPU occupancy	display cpu [slot <i>slot-no</i>]

Device Management Configuration Example

Using the Switch as an FTP Client to Implement the Remote Upgrade (Switch 8807)

Network requirements

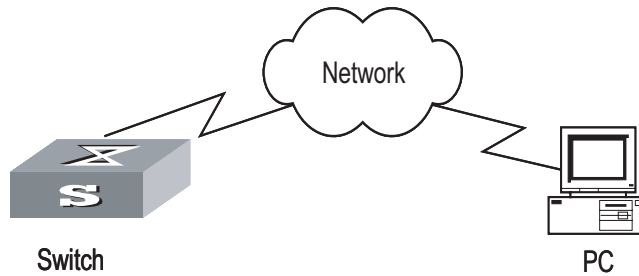
The user logs into the switch using Telnet, downloads the application from the FTP server to the flash memory of the switch, and implements remote upgrade using the right commands.

The switch serves as an FTP client and the remote PC as an FTP server. The configuration on the FTP server is as follows: an FTP user is configured with the name switch, the password hello and the read & write authority over the Switch root directory on the PC. The IP address of a VLAN interface on the switch is 1.1.1.1, and the IP address of the PC is 2.2.2.2. The switch and PC are reachable with each other.

The switch applications switch.app and boot.app are stored on the PC. Using FTP, these files can be downloaded from the remote FTP server to the switch.

Network diagram

Figure 185 Network diagram for FTP configuration



Configuration procedure

- 1 Configure FTP server parameters on the PC: a user named as switch, password hello, read & write authority over the Switch directory on the PC. No further details are provided here
- 2 Configure the switch

The switch has been configured with a Telnet user named as user, as 3-level user, with password hello, requiring username and password authentication.

Use the **telnet** command to log into the switch.

```
<SW8800>
```



CAUTION: If the Flash Memory of the switch is not enough, you need to first delete the existing programs in the flash memory and then download the new ones to the memory.

Enter the corresponding command in user view to establish FTP connection. Then enter correct username and password to log into the FTP server.

```
<SW8800> ftp 2.2.2.2
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):switch
331 Give me your password, please
Password:*****
230 Logged in successfully
[ftp]
```

Use the **get** command to download the switch.app and boot.app files from the FTP server to the flash directory on the FTP client.

```
[ftp] get switch.app
[ftp] get boot.app
```

Use the **quit** command to release FTP connection and return to user view.

```
[ftp] quit
<SW8800>
```

Upgrade the BootROM of main module 0.

```
<SW8800> boot bootrom boot.app slot 0
```

Use the **boot boot-loader** command to specify the downloaded program as the application at the next login and reboot the switch.

```
<SW8800>boot boot-loader primary flash:/switch.app slot 0
<SW8800>disp boot-loader
The primary app to boot of slot 0 at the next time is: flash:/switch.app
The backup app to boot of slot 0 at the next time is: flash:/switch.app
The app to boot of slot 0 at this time is: flash:/switch.app
<SW8800>
```

Using the Switch as an FTP Server to Implement the Remote Upgrade (Switch 8807)

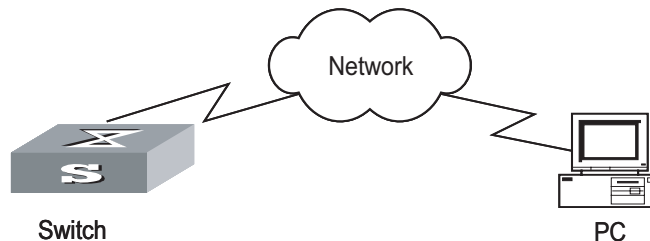
Network requirements

The switch serves as an FTP server and the PC as an FTP client. The configuration on the FTP server is as follows: an FTP user is configured with the name switch, the password hello and the read & write authority over the root directory of the switch. The IP address of a VLAN interface on the switch is 1.1.1.1, and the IP address of the PC is 2.2.2.2. The switch and PC are reachable with each other.

The switch application switch.app is stored on the PC. Using FTP, this file can be uploaded from the PC to the switch remotely, and the configuration file vrpcfg.txt on the switch can be downloaded to the PC as a backup.

Network diagram

Figure 186 Network diagram for FTP configuration



Configuration procedure

1 Configure the switch

Log into the switch through the console port locally or through telnet remotely (refer to the getting start module for details about the login modes).

```
<SW8800>
```

Enable FTP on the switch; configure a username, password and path.

```
[SW8800] ftp server enable
[SW8800] local-user switch
[3Com-luser-switch] service-type ftp ftp-directory flash:
[3Com-luser-switch] password simple hello
```

2 Run the FTP client program on the PC to set up an FTP connection with the switch. Then upload the switch program switch.app to the flash root directory on the switch and download the configuration file vrpcfg.txt from the switch. The FTP client program is not provided along with the switch, so, it is for you to purchase and install it.



CAUTION: *If the Flash Memory on the switch is not sufficient, delete the original application program in the flash before uploading the new one into the flash of the switch.*

- 1 After uploading, performs upgrading on the switch.

```
<SW8800>
```

You can use the **boot boot-loader** command to specify the new file as the application program on the next booting and reboot the switch to implement the upgrading of the application program.

```
<SW8800> boot boot-loader primary flash:/switch.app slot 0  
<SW8800> reboot
```


70

FTP&TFTP CONFIGURATION

FTP Configuration

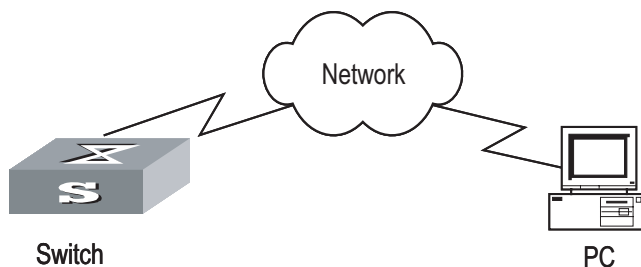
FTP Overview FTP (File Transfer Protocol) is a universal method for transmitting files on the Internet and IP networks. In this method, files are copied from one system to another. FTP supports definite file types (such as ASCII and Binary) and file structures (byte stream and record). Even now, FTP is still used widely, while most users transmit files by Email and Web.

FTP, a TCP/IP protocol on the application layer, is used for transmitting files between a remote server and a local host.

The switch provides the following FTP services:

- FTP server: You can run FTP client program to log in the server and access the files on it.
- FTP client: You can run the ftp X.X.X.X command (where, X.X.X.X represents the IP address of the remote FTP server) to set up a connection between the switch and a remote FTP server to access the files on the remote server.

Figure 187 FTP configuration



The configuration of the switch as FTP client.

Table 752 Configuration of the switch as FTP client

Device	Configuration	Default	Remarks
Switch	Log into the remote FTP server directly with the ftp command.	-	You need first get FTP user command and password, and then log into the remote FTP server. Then you can get the directory and file authority.
PC	Start FTP server and make such settings as username, password, and authority.	-	-

The configuration of the switching as FTP server.

Table 753 Configuration of the switch as FTP server

Device	Configuration	Default	Remarks
	Start FTP server.	FTP server is disabled	You can view the configuration information of FTP server with the display ftp-server command
Switch	Configure authentication and authorization for FTP server.	-	Configure username, password and authorized directory for FTP users
	Configure running parameters for FTP server.	-	Configure timeout time value for FTP server.
PC	Log into the switch from FTP client.	-	-



CAUTION: The prerequisite for normal FTP function is that the switch and PC are reachable.

Enabling/Disabling FTP Server

You can use the following commands to enable/disable the FTP server on the switch. Perform the following configuration in system view.

Table 754 Enable/disable FTP Server

Operation	Command
Enable the FTP server	ftp server enable
Disable the FTP server	undo ftp server

FTP server supports multiple users to access at the same time. A remote FTP client sends request to the FTP server. Then, the FTP server will carry out the corresponding operation and return the result to the client.

By default, FTP server is disabled.

Configuring the FTP Server Authentication and Authorization

The authorization information of FTP server includes the path to the desired directory for FTP users. The FTP server service is available only for the authenticated and authorized users. The authorization information of FTP server includes the top working directory provided for FTP clients. You can use the following commands to configure FTP server authentication and authorization.

Perform the following configuration in corresponding view.

Table 755 Configure the FTP Server Authentication and Authorization

Operation	Command
Create new local FTP user and enter local user view (in System view)	local-user { <i>username</i> multicast [domain <i>domain-name</i>] <i>ipaddress</i> password-display-mode { auto cipher-force } }

Table 755 Configure the FTP Server Authentication and Authorization

Operation	Command
Delete local FTP user (in system view)	undo local-user { <i>username</i> all [service-type { ftp lan-access telnet ppp ssh terminal }] multicast [domain <i>domain-name</i>] <i>ipaddress</i> password-display-mode }
Set the password display mode when the switch displays local user information	local-user password-display-mode { auto cipher-force }
Restore the password display mode when the switch displays local user information	undo local-user password-display-mode
Configure password for local user(local user view)	password { cipher simple } <i>password</i>
Configure service type for local user(local user view)	service-type { ftp [ftp-directory <i>directory</i>] lan-access ppp [call-number <i>call-number</i> callback-nocheck callback-number <i>callback-number</i>] ssh [level <i>level</i> telnet terminal] telnet [level <i>level</i> ssh terminal] terminal [level <i>level</i> ssh telnet] }
Cancel password for local user(local user view)	undo password
Cancel authorization information for FTP user(local user view)	undo service-type { ftp [ftp-directory <i>directory</i>] lan-access ppp [call-number <i>call-number</i> callback-nocheck callback-number <i>callback-number</i>] ssh [level <i>level</i> telnet terminal] telnet [level <i>level</i> ssh terminal] terminal [level <i>level</i> ssh telnet] }

Only the clients who have passed the authentication and authorization can access the FTP server.



CAUTION: When using the file manager or IE browser to perform the FTP operations, you are recommended to input the user name and password in the address column in the following format: *ftp://username:password@URL*. If you input the URL of the FTP site you want to connect directly, the login may fail because of the bugs in the file manager or in the IE browser.

Configuring the Running Parameters of FTP Server

You can use the following commands to configure the connection timeout of the FTP server. If the FTP server receives no service request from the FTP client for a period of time, it will cut the connection to it, thereby avoiding the illegal access from the unauthorized users. The period of time is FTP connection timeout.

Perform the following configuration in system view.

Table 756 Configuring FTP server connection timeout

Operation	Command
Configure FTP server connection timeouts	ftp timeout <i>minute</i>
Restoring the default FTP server connection timeouts	undo ftp timeout

By default, the FTP server connection timeout is 30 minutes.

Displaying and Debugging FTP Server

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

Table 757 Display and debug FTP Server

Operation	Command
Display FTP server	display ftp-server
Display the connected FTP users.	display ftp-user

The **display ftp-server** command can be used for displaying the configuration information about the current FTP server, including the maximum amount of users supported by FTP server and the FTP connection timeout. The **display ftp-user** command can be used for displaying the detail information about the connected FTP users.

Disconnecting an FTP User

Perform the following configuration in system view.

Table 758 Disconnect an FTP user

Operation	Command
Disconnect an FTP user.	ftp disconnect user-name

Introduction to FTP Client

As an additional function provided by the switch, FTP client is an application module and has no configuration functions. The switch connects the FTP clients and the remote server and inputs the command from the clients for corresponding operations (such as creating or deleting a directory).

FTP Client Configuration Example

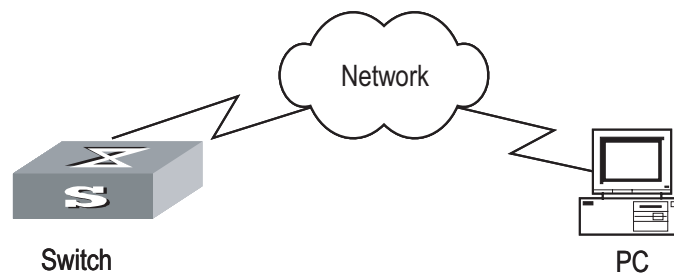
Network requirements

The switch serves as FTP client and the remote PC as FTP server. The configuration on FTP server: Configure an FTP user named as switch, with password hello and with read & write authority over the Switch root directory on the PC. The IP address of a VLAN interface on the switch is 1.1.1.1, and that of the PC is 2.2.2.2. The switch and PC are reachable.

The switch application switch.app is stored on the PC. Using FTP, the switch can download the switch.app from the remote FTP server and upload the vrpcfg.cfg to the FTP server under the switch directory for backup purpose.

Network diagram

Figure 188 Network diagram for FTP configuration



Configuration procedure

- 1 Configure FTP server parameters on the PC: a user named as switch, password hello, read and write authority over the Switch directory on the PC.
- 2 Configure the switch

Log into the switch through the Console port locally or Telnet remotely.

Then type in the right command in user view to establish FTP connection, then correct username and password to log into the FTP server.

```
<SW8800> ftp 2.2.2.2
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):switch
331 Give me your password, please
Password:*****
230 Logged in successfully
[ftp]
```



CAUTION: *If the Flash Memory of the switch is not enough, you need to first delete the existing programs in the Flash Memory and then upload the new ones.*

Enter the authorized directory of the FTP server.

```
[ftp] cd switch
```

Use the **put** command to upload the vrpcfg.cfg to the FTP server.

```
[ftp] put vrpcfg.cfg
```

Use the **get** command to download the switch.app from the FTP server to the Flash directory on the FTP server.

```
[ftp] get switch.app
```

Use the **quit** command to release FTP connection and return to user view.

```
[ftp] quit
<SW8800>
```

Use the **boot boot-loader** command to specify the downloaded program as the application at the next login and reboot the switch.

```
<SW8800> boot boot-loader switch.app
<SW8800> reboot
```

FTP Server Configuration Example

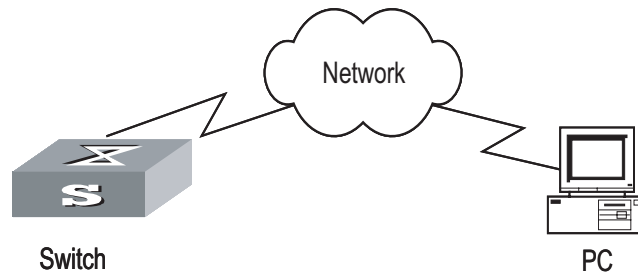
Network requirements

Switch serves as FTP server and the remote PC as FTP client. The configuration on FTP server: Configure an FTP user named as switch, with password hello and with read & write authority over the flash root directory on the PC. The IP address of a VLAN interface on the switch is 1.1.1.1, and that of the PC is 2.2.2.2. The switch and PC are reachable.

The switch application switch.app is stored on the PC. Using FTP, the PC can upload the switch.app from the remote FTP server and download the vrpcfg.cfg from the FTP server for backup purpose.

Network diagram

Figure 189 Network diagram for FTP configuration



Configuration procedure

1 Configure the switch

Log into the switch through the console port locally or Telnet remotely, and start FTP function and set username, password and file directory.

```
[SW8800] ftp server enable
[SW8800] local-user switch
[3Com-luser-switch] service-type ftp ftp-directory flash:
[3Com-luser-switch] password simple hello
```

2 Run FTP client on the PC and establish FTP connection. Upload the switch.app to the switch under the Flash directory and download the vrpcfg.cfg from the switch. FTP client is not shipped with the switch, so you need to buy it separately.



CAUTION: If the Flash Memory of the switch is not enough, you need to first delete the existing programs in the Flash Memory and then upload the new ones.

3 When the uploading is completed, initiate file upgrade on the switch.

Use the **boot boot-loader** command to specify the downloaded program as the application at the next login and reboot the switch.

```
<SW8800> boot boot-loader switch.app
<SW8800> reboot
```

TFTP Configuration

TFTP Overview

Trivial File Transfer Protocol (TFTP) is a simple file transmission protocol. It is initially designed for the booting of free-disk systems (work stations or X terminals in general). Compared with FTP, another file transmission protocol, TFTP has no complicated interactive access interface or authentication control, and therefore it can be used when there is no complicated interaction between the clients and server. TFTP is implemented on the basis of UDP.

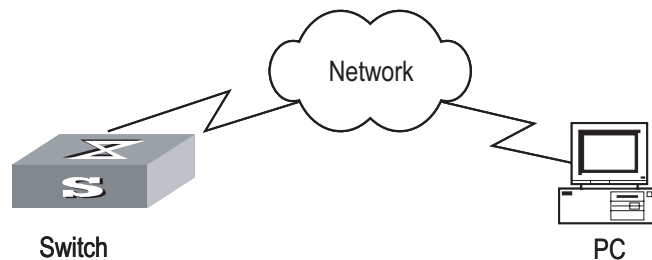
TFTP transmission is originated from the client end. To download a file, the client sends a request to the TFTP server and then receives data from it and sends

acknowledgement to it. To upload a file, the client sends a request to the TFTP server and then transmits data to it and receives the acknowledgement from it. TFTP transmits files in two modes, binary mode for program files and ASCII mode for text files.

The administrator needs to configure the IP addresses of TFTP client and server before configuring TFTP, and makes sure that the route between the client and server is reachable.

The switch can only function as a TFTP client.

Figure 190 TFTP configuration



The configuration of the switch as TFTP client.

Table 759 Configuration of the switch as TFTP client

Device	Configuration	Default	Remarks
Switch	Configure IP address for the VLAN interface of the switch, in the same network segment as that of TFTP server.	-	TFTP is right for the case where no complicated interactions are required between the client and server. Make sure that the route is reachable between the switch and the TFTP server.
	Use the tftp command to log into the remote TFTP server for file uploading and downloading.	-	-
PC	Start TFTP server and set authorized TFTP directory.	-	-

Downloading Files by Means of TFTP

To download a file, the client sends a request to the TFTP server and then receives data from it and sends acknowledgement to it. You can use the following commands to download files by means of TFTP.

Perform the following configuration in user view.

Table 760 Download files by means of TFTP

Operation	Command
Download files by means of TFTP	tftp tftp-server get source-file [dest-file]

In the command, *tftp-server* indicates the IP address or host name of TFTP server; *source-file* indicates the file information to be downloaded from TFTP server; *dest-file* indicates the name of the file downloaded on switch.

Uploading Files by Means of TFTP

To upload a file, the client sends a request to the TFTP server and then transmits data to it and receives the acknowledgement from it. You can use the following commands to upload files.

Perform the following configuration in user view.

Table 761 Upload files by means of TFTP

Operation	Command
Upload files by means of TFTP	tftp tftp-server put source-file [dest-file]

In the command, *source-file* indicates the file to be uploaded to server; *dest-file* indicates the saved-as name of the file on TFTP server; *tftp-server* indicates the IP address or host name of TFTP server.

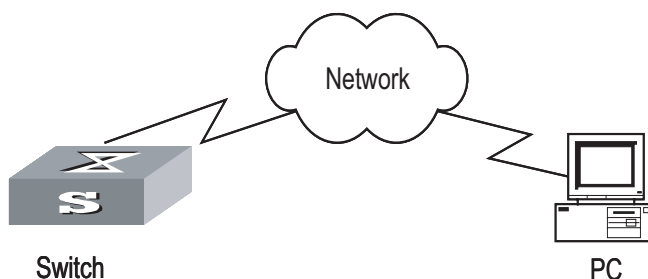
TFTP Client Configuration Example**Network requirements**

The switch serves as TFTP client and the remote PC as TFTP server. Authorized TFTP directory is set on the TFTP server. The IP address of a VLAN interface on the switch is 1.1.1.1, and that of the PC is 1.1.1.2.

The switch application switch.app is stored on the PC. Using TFTP, the switch can download the switch.app from the remote TFTP server and upload the vrpcfg.cfg to the TFTP server under the switch directory for backup purpose.

Network diagram

Figure 191 Network diagram for TFTP configuration

**Configuration procedure**

- 1 Start TFTP server on the PC and set authorized TFTP directory.
- 2 Configure the switch

Log into the switch (through local console or remote Telnet, refer to the Getting Started for login information), and then enter the system view.

```
<SW8800> system-view
[SW8800]
```



CAUTION: If the Flash Memory of the switch is not enough, you need to first delete the existing programs in the Flash Memory and then upload the new ones.

Configure IP address 1.1.1.1 for the VLAN interface, ensure the port connecting the PC is also in this VALN (VLAN 1 in this example).


```
[SW8800] interface vlan 1
[3Com-vlan-interface1] ip address 1.1.1.1 255.255.255.0
[3Com-vlan-interface1] quit
```

Enter system view and download the switch.app from the TFTP server to the Flash Memory of the switch.

```
<SW8800> tftp 1.1.1.2 get switch.app switch.app
```

Upload the vrpcfg.cfg to the TFTP server.

```
<SW8800> tftp 1.1.1.2 put vrpcfg.cfg vrpcfg.cfg
```

Use the **boot boot-loader** command to specify the downloaded program as the application at the next login and reboot the switch.

```
<SW8800> boot boot-loader switch.app
<SW8800> reboot
```

Information Center Function

Introduction to Information Center

The information center is an indispensable part of the switch. It serves as an information center of the system software modules. The logging system is responsible for most of the information outputs, and it also makes detailed classification to filter the information efficiently. Coupled with the debugging program, the information center provides powerful support for the network administrators and the R&D personnel to monitor the operating status of networks and diagnose network failures.

When the log information is output to terminal or log buffer, the following parts will be included:

```
% <priority> Timestamp Sysname Module name/Severity/Digest: Content
```

For example:

```
%Jun 7 05:22:03 2003 3Com IFNET/6/UPDOWN:Line protocol on interface  
Ethernet2/1/2, changed state to UP
```

When the log information is output to information center, the first part will be "<Priority>".

For example:

```
% <189>Jun 7 05:22:03 2003 3Com IFNET/6/UPDOWN:Line protocol on interface  
Ethernet0/0/0, changed state to UP
```

The description of the components of log information is as follows:

1 %

In practical output, some of the information is started with the % character, which means a logging is necessary.

2 Priority

The priority is computed according to following formula: $\text{facility} * 8 + \text{severity} - 1$. The default value for the facility is 23. The range of severity is 1~8, and the severity will be introduced in separate section.

Priority is only effective when information is send to log host. There is no character between priority and timestamp.

3 Timestamp

If the logging information is send to the log host, the default format of timestamp is date

The date format of timestamp is " Mmm dd hh:mm:ss yyyy".

Mmm " is month field, such as: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

dd" is day field, if the day is little than 10th, one blank should be added, such as " 7".

hh:mm:ss" is time field, "hh" is from 00 to 23, "mm" and "ss" are from 00 to 59.

yyyy" is year field.

4 Sysname

The sysname is the host name, the default value is "3Com".

User can change the host name through **sysname** command.

Notice: There is a blank between sysname and module name.

5 Module name

The module name is the name of module which create this logging information, the following sheet list some examples:

Table 762 The module name field

Module name	Description
8021X	802.1X module
ACL	Access control list module
ADBM	MAC address management module
ARP	Address resolution protocol module
BGP	Border gateway protocol module
CFM	Configuration file management module
CMD	Command module
default	Default settings for all the modules
DEV	Device management module
DHCP	Dynamic host configuration protocol module
DIAGCLI	Diagnosis module
DNS	Domain name server module
DRVMPLS	Multiprotocol label switching drive module
DRVL2	Layer 2 drive module
DRVL3	Layer 3 drive module
DRVL3MC	Layer 3 multicast module
MPLS	MPLS drive module
DRVQACL	QACL drive module

Table 762 The module name field

Module name	Description
DRVVPLS	Virtual private LAN service drive module
ETH	Ethernet module
FTPS	FTP server module
HA	High availability module
HABP	3Com authentication bypass protocol module
HWCM	3Com configuration management MIB module
IFNET	Interface management module
IGSP	IGMP snooping module
IP	Internet protocol module
ISIS	Intermediate system-to-intermediate system intra-domain routing protocol module
L2INF	L2 interface management module
L2V	L2 VPN module
LACL	LAN switch ACL module
LDP	label distribution protocol module
LINKAGG	LINKAGG module
LQOS	LAN switch QoS module
LS	Local server module
LSPAGENT	Label switched path agent module
LSPM	Label switch path management module
MIX	Dual system management module
MMC	MMC module
MODEM	Modem module
MPLSFW	MPLS forward module
MPM	Multicast port management module
MSDP	Multicast source discovery protocol module
MSTP	Multiple spanning tree protocol module
NTP	Network time protocol module
OSPF	Open shortest path first module
PHY	Physical sublayer & physical layer module
PPP	Point to point protocol module
PSSINIT	PSSINIT module
RDS	RADIUS module
RM	Routing management module
RMON	Remote monitor module
RSA	RSA (Rivest, Shamir and Adleman) encryption module
RTPRO	Routing protocol module
SHELL	User interface module
SNMP	Simple network management protocol module
SOCKET	Socket module
SSH	Secure shell module
SYSM	System manage veneer module

Table 762 The module name field

Module name	Description
SYSMIB	System MIB module
TAC	Terminal access controller module
TELNET	Telnet module
USERLOG	User calling logging module
VFS	Virtual file system module
VLAN	Virtual local area network module
VOS	Virtual operate system module
VRRP	VRRP (virtual router redundancy protocol) module
VTY	VTY (virtual type terminal) module

Notice: There is a slash ('/') between module name and severity.

6 Severity

Switch information falls into three categories: log information, debugging information and trap information. The information center classifies every kind of information into 8 severity or urgent levels. The log filtering rule is that the system prohibits outputting the information whose severity level is greater than the set threshold. The more urgent the logging packet is, the smaller its severity level is. The level represented by "emergencies" is 1, and that represented by "debugging" is 8. Therefore, when the threshold of the severity level is "debugging", the system will output all the information.

Definition of severity in logging information is as followed.

Table 763 Information center-defined severity

Severity	Value	Description
emergencies	1	The extremely emergent errors
alerts	2	The errors that need to be corrected immediately.
critical	3	Critical errors
errors	4	The errors that need to be concerned but not critical
warnings	5	Warning, there might exist some kinds of errors.
notifications	6	The information should be concerned.
informational	7	Common prompting information
debugging	8	Debugging information

Notice: There is a slash between severity and digest.

7 Digest

The digest is abbreviation, it represent the abstract of contents.

Notice: There is a colon between digest and content. The digest can be up to 32 characters long.

Information Center Configuration

Switch supports 7 output directions of information.

The system assigns a channel in each output direction by default. See the table below.

Table 764 Numbers and names of the channels for log output

Output direction	Channel number	Default channel name
Console	0	console
Monitor	1	monitor
Information center loghost	2	loghost
Trap buffer	3	trapbuf
Logging buffer	4	logbuf
snmp	5	snmpagent
Log file	6	logfile



The settings in the 7 directions are independent from each other. The settings will take effect only after enabling the information center.

The information center of the switch has the following features:

- Support to output log in 7 directions, i.e., Console, monitor to Telnet terminal, logbuffer, loghost, trapbuffer, and SNMP log file.
- The log is divided into 8 levels according to the significance and it can be filtered based on the levels.
- The information can be classified in terms of the source modules and the information can be filtered in accordance with the modules.
- The output language can be selected between Chinese and English.

1 Sending the configuration information to the loghost

Table 765 Send the configuration information to the loghost

Device	Configuration	Default value	Configuration description
	Enable information center	By default, information center is enabled	Other configurations are valid only if the information center is enabled
Switch	Set the information output direction to the loghost	-	The configuration about the loghost on the switch and that on loghost must be the same; otherwise the information cannot be sent to the loghost correctly
	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the switch of the corresponding module before defining output debugging information

Table 765 Send the configuration information to the loghost

Device	Configuration	Default value	Configuration description
Loghost	Refer to configuration cases for related log host configuration	-	-

2 Sending the configuration information to the console terminal

Table 766 Send the configuration information to the console terminal.

Device	Configuration	Default value	Configuration description
	Enable information center	By default, information center is enabled.	Other configurations are valid only if the information center is enabled
	Set the information output direction to the Console	-	-
Switch	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the switch of the corresponding module before defining output debugging information
	Enable terminal display function	-	You can view debugging information after enabling terminal display function

3 Sending the configuration information to the monitor terminal

Table 767 Send the configuration information to the monitor terminal

Device	Configuration	Default value	Configuration description
	Enable information center	By default, information center is enabled	Other configurations are valid only if the information center is enabled
	Set the information output direction to the monitor	-	-
Switch	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the switch of the corresponding module before defining output debugging information
	Enable the terminal display function and this function for the corresponding information	-	For Telnet terminal and dumb terminal, to view the information, you must enable the current terminal display function using the terminal monitor command

4 Sending the configuration information to the log buffer

Table 768 Send the configuration information to the log buffer

Device	Configuration	Default value	Configuration description
	Enable information center	By default, information center is enabled	Other configurations are valid only if the information center is enabled
	Set the information output direction to the logbuffer	-	You can configure the size of the log buffer at the same time.
Switch	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the switch of the corresponding module before defining output debugging information

5 Sending the configuration information to the trap buffer

Table 769 Send the configuration information to the trap buffer

Device	Configuration	Default value	Configuration description
	Enable information center	By default, information center is enabled	Other configurations are valid only if the information center is enabled
	Set the information output direction to the trapbuffer	-	You can configure the size of the trap buffer at the same time
Switch			You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the switch of the corresponding module before defining output debugging information
	Set information source	-	

6 Sending the configuration information to SNMP

Table 770 Send the configuration information to SNMP

Device	Configuration	Default value	Configuration description
	Enable information center	By default, information center is enabled	Other configurations are valid only if the information center is enabled
	Set the information output direction to SNMP	-	-
Switch			You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the switch of the corresponding module before defining output debugging information
	Set information source	-	
	Configure SNMP features	-	Refer to Chapter "SNMP"
Network management workstation	The same as the SNMP configuration of the switch	-	-

Sending the Configuration Information to the Loghost

To send configuration information to the loghost, follow the steps below:

1 Enabling information center

Perform the following configuration in system view.

Table 771 Enable/disable information center

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



Information center is enabled by default. After information center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2 Configuring to output information to the loghost

Perform the following configuration in system view.

Table 772 Configure to output information to the loghost

Operation	Command
Output information to the loghost	info-center loghost { source <i>interface-type interface-number</i> <i>host-ip-addr</i> [channel { <i>channel-number</i> <i>channel-name</i> }] facility <i>local-number</i> language { chinese english }]* }
Cancel the configuration of outputting information to loghost	undo info-center loghost <i>host-ip-addr</i>

Note that the IP address of log host must be correct.



*Ensure to enter the correct IP address using the **info-center loghost** command to configure loghost IP address. If you enter a loopback address, the system prompts of invalid address appears.*

3 Configuring information source on the switch

By this configuration, you can define the information that sent to console terminal is generated by which modules, information type, information level, and so on.

Perform the following configuration in system view.

Table 773 Define information source

Operation	Command
Define information source	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> }* log { level <i>severity</i> state <i>state</i> }* trap { level <i>severity</i> state <i>state</i> }*]*

Table 773 Define information source

Operation	Command
Cancel the configuration of information source	undo info-center source { <i>modu-name</i> default all } channel { <i>channel-number</i> <i>channel-name</i> }

modu-name specifies the module name; **default** represents all the modules; **all** represents all the information filter configuration in channel *channel-number* except default; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to the loghost, *channel-number* or *channel-name* must be set to the channel that corresponds to loghost direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.



*If you want to view the debugging information of some modules on the switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging switch of those modules.*

4 Configuring the loghost

The configuration on the loghost must be the same with that on the switch. For related configuration, see the configuration examples in the later part.

Sending the Configuration Information to Console terminal

To send configuration information to console terminal, follow the steps below:

1 Enabling information center

Perform the following configuration in system view.

Table 774 Enable/disable information center

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



Information center is enabled by default. After information center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2 Configuring to output information to console terminal

Perform the following configuration in system view.

Table 775 Configure to output information to console terminal

Operation	Command
Output information to Console	info-center console channel { <i>channel-number</i> <i>channel-name</i> }
Cancel the configuration of outputting information to Console	undo info-center console channel

3 Configuring information source on the switch

By this configuration, you can define the information that sent to console terminal is generated by which modules, information type, information level, and so on.

Perform the following configuration in system view:

Table 776 Define information source

Operation	Command
Define information source	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> }* log { level <i>severity</i> state <i>state</i> }* trap { level <i>severity</i> state <i>state</i> }*]*
Cancel the configuration of information source	undo info-center source { <i>modu-name</i> default all } channel { <i>channel-number</i> <i>channel-name</i> }

modu-name specifies the module name; **default** represents all the modules; **all** represents all the information filter configuration in channel *channel-number* except default; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to the console terminal, *channel-number* or *channel-name* must be set to the channel that corresponds to Console direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.



*If you want to view the debugging information of some modules on the switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging switch of those modules.*

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

This configuration will affect the timestamp of the displayed information.

Perform the following configuration in system view:

Table 777 Configure the output format of time-stamp

Operation	Command
Configure the output format of the time-stamp	info-center timestamp { log trap debugging } { boot date none }
Output time-stamp is disabled	undo info-center timestamp { log trap debugging }

4 Enable terminal display function

To view the output information at the console terminal, you must first enable the corresponding log, debugging and trap information functions at the switch.

For example, if you have set the log information as the information sent to the console terminal, now you need to use the **terminal logging** command to enable the terminal display function of log information on the switch, then you can view the information at the console terminal.

Perform the following configuration in user view:

Table 778 Enable terminal display function

Operation	Command
Enable terminal display function of debugging information	terminal debugging
Disable terminal display function of debugging information	undo terminal debugging
Enable terminal display function of log information	terminal logging
Disable terminal display function of log information	undo terminal logging
Enable terminal display function of trap information	terminal trapping
Disable terminal display function of trap information	undo terminal trapping

By default, the terminal display function of debugging information is disabled.

Sending the Configuration Information to Telnet Terminal or Dumb Terminal

To send configuration information to Telnet terminal or dumb terminal, follow the steps below:

1 Enabling information center

Perform the following configuration in system view.

Table 779 Enable/disable Information center

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



Information center is enabled by default. After information center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2 Configuring to output information to Telnet terminal or dumb terminal

Perform the following configuration in system view.

Table 780 Configure to output information to Telnet terminal or dumb terminal

Operation	Command
Output information to Telnet terminal or dumb terminal	info-center monitor channel { <i>channel-number</i> <i>channel-name</i> }
Cancel the configuration of outputting information to Telnet terminal or dumb terminal	undo info-center monitor channel

3 Configuring information source on the switch

By this configuration, you can define the information that sent to Telnet terminal or dumb terminal is generated by which modules, information type, information level, and so on.

Perform the following configuration in system view:

Table 781 Define information source

Operation	Command
Define information source	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> }* log { level <i>severity</i> state <i>state</i> }* trap { level <i>severity</i> state <i>state</i> }*]*
Cancel the configuration of information source	undo info-center source { <i>modu-name</i> default all } channel { <i>channel-number</i> <i>channel-name</i> }

modu-name specifies the module name; **default** represents all the modules; **all** represents all the information filter configuration in channel *channel-number* except default; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to Telnet terminal or dumb terminal, *channel-number* or *channel-name* must be set to the channel that corresponds to monitor direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.



When there are more than one Telnet users or monitor users at the same time, some configuration parameters should be shared among the users, such as

module-based filtering settings and severity threshold. When a user modifies these settings, it will be reflected on other clients.



If you want to view the debugging information of some modules on the switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging switch of those modules.

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

This configuration will affect the timestamp of the displayed information.

Perform the following configuration in system view:

Table 782 Configure the output format of time-stamp

Operation	Command
Configure the output format of the time-stamp	info-center timestamp { log trap debugging } { boot date none }
Output time-stamp is disabled	undo info-center timestamp { log trap debugging }

4 Enabling terminal display function

To view the output information at the Telnet terminal or dumb terminal, you must first enable the terminal display function, and then the corresponding terminal display function of log information on the switch.

For example, if you have specified the log information as the information sent to the Telnet terminal or dumb terminal, now you need to use the terminal monitor command to enable the terminal display function and the **terminal logging** command to enable the terminal display function of log information on the switch, then you can view the information at the Telnet terminal or dumb terminal.

Perform the following configuration in user view:

Table 783 Enable terminal display function

Operation	Command
Enable terminal display function of log, debugging and trap information	terminal monitor
Disable terminal display function of the above information	undo terminal monitor
Enable terminal display function of debugging information	terminal debugging
Disable terminal display function of debugging information	undo terminal debugging
Enable terminal display function of log information	terminal logging
Disable terminal display function of log information	undo terminal logging

Table 783 Enable terminal display function

Operation	Command
Enable terminal display function of trap information	terminal trapping
Disable terminal display function of trap information	undo terminal trapping

Sending the Configuration Information to the Log Buffer

To send configuration information to the log buffer, follow the steps below:

1 Enabling information center

Perform the following configuration in system view.

Table 784 Enable/disable information center

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



Information center is enabled by default. After information center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2 Configuring to output information to the log buffer

Perform the following configuration in system view.

Table 785 Configure to output information to log buffer

Operation	Command
Output information to log buffer	info-center logbuffer [channel { <i>channel-number</i> <i>channel-name</i> }] size buffersize]*
Cancel the configuration of outputting information to log buffer	undo info-center logbuffer [channel size]

By default, the switch outputs information to the log buffer in the CPU. The size of the log buffer is 512, that is, the log buffer can hold up to 512 messages.

3 Configuring information source on the switch

By this configuration, you can define the information that sent to log buffer is generated by which modules, information type, information level, and so on.

Perform the following configuration in system view:

Table 786 Define information source

Operation	Command
Define information source	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> }* log { level <i>severity</i> state <i>state</i> }* trap { level <i>severity</i> state <i>state</i> }*]*
Cancel the configuration of information source	undo info-center source { <i>modu-name</i> default all } channel { <i>channel-number</i> <i>channel-name</i> }

modu-name specifies the module name; **default** represents all the modules; **all** represents all the information filter configuration in channel *channel-number* except default; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to log buffer, *channel-number* or *channel-name* must be set to the channel that corresponds to logbuffer direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.



If you want to view the debugging information of some modules on the switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging switch of those modules.

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following configuration in system view:

Table 787 Configure the output format of time-stamp

Operation	Command
Configure the output format of the time-stamp	info-center timestamp { log trap debugging } { boot date none }
Output time-stamp is disabled	undo info-center timestamp { log trap debugging }

Sending the Configuration Information to the Trap Buffer

To send configuration information to the trap buffer, follow the steps below:

1 Enabling information center

Perform the following configuration in system view.

Table 788 Enable/disable information center

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



Information center is enabled by default. After information center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2 Configuring to output information to the trap buffer

Perform the following configuration in system view.

Table 789 Configure to output information to trap buffer

Operation	Command
Output information to trap buffer	info-center trapbuffer [size <i>buffersize</i> channel { <i>channel-number</i> <i>channel-name</i> }]*
Cancel the configuration of outputting information to trap buffer	undo info-center trapbuffer [channel size]

By default, the switch outputs information to the trap buffer in the CPU. The size of the trap buffer is 256, that is, the trap buffer can hold up to 256 messages.

3 Configuring information source on the switch

By this configuration, you can define the information that sent to trap buffer is generated by which modules, information type, information level, and so on.

Perform the following configuration in system view:

Table 790 Define information source

Operation	Command
Define information source	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> }* log { level <i>severity</i> state <i>state</i> }* trap { level <i>severity</i> state <i>state</i> }*]*
Cancel the configuration of information source	undo info-center source { <i>modu-name</i> default all } channel { <i>channel-number</i> <i>channel-name</i> }

modu-name specifies the module name; **default** represents all the modules; **all** represents all the information filter configuration in channel *channel-number* except default; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to trap buffer, *channel-number* or *channel-name* must be set to the channel that corresponds to trapbuffer direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.



*If you want to view the debugging information of some modules on the switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging switch of those modules.*

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

This configuration will affect the timestamp of the displayed information.

Perform the following configuration in system view:

Table 791 Configure the output format of time-stamp

Operation	Command
Configure the output format of the time-stamp	info-center timestamp { log trap debugging } { boot date none }
Output time-stamp is disabled	undo info-center timestamp { log trap debugging }

Sending the Configuration Information to SNMP Network Management

To send configuration information to SNMP NM, follow the steps below:

1 Enabling information center

Perform the following configuration in system view.

Table 792 Enable/disable information center

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



Information center is enabled by default. After information center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2 Configuring to output information to SNMP NM

Perform the following configuration in system view.

Table 793 Configure to output information to SNMP NM

Operation	Command
Output information to SNMP NM	info-center snmp channel { channel-number channel-name }

Table 793 Configure to output information to SNMP NM

Operation	Command
Cancel the configuration of outputting information to SNMP NM	undo info-center snmp channel

3 Configuring information source on the switch

By this configuration, you can define the information that sent to SNMP NM is generated by which modules, information type, information level, and so on.

Perform the following configuration in system view:

Table 794 Define information source

Operation	Command
Define information source	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [debug { level <i>severity</i> state <i>state</i> }* log { level <i>severity</i> state <i>state</i> }* trap { level <i>severity</i> state <i>state</i> }*]*
Cancel the configuration of information source	undo info-center source { <i>modu-name</i> default all } channel { <i>channel-number</i> <i>channel-name</i> }

modu-name specifies the module name; **default** represents all the modules; **all** represents all the information filter configuration in channel *channel-number* except default **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to SNMP NM, *channel-number* or *channel-name* must be set to the channel that corresponds to SNMP direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.



*If you want to view the debugging information of some modules on the switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging switch of those modules.*

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

This configuration will affect the timestamp of the displayed information.

Perform the following configuration in system view:

Table 795 Configure the output format of time-stamp

Operation	Command
Configure the output format of the time-stamp	info-center timestamp { log trap debugging } { boot date none }
Output time-stamp is disabled	undo info-center timestamp { log trap debugging }

4 Configuring of SNMP and network management workstation on the switch

You have to configure SNMP on the switch and the remote workstation to ensure that the information is correctly sent to SNMP NM. Then you can get correct information from network management workstation. SNMP configuration on switch refers to Chapter "SNMP" of the *SNMP&RMON Command Manual*.

Displaying and Debugging Information Center

After the above configuration, execute the **display** command in any view to view the running status of the information center. You also can authenticate the effect of the configuration by viewing displayed information. Execute the **reset** command in user view to clear statistics of information center.

Perform the following configuration in user view. The **display** command still can be performed in any view.

Table 796 Display and debug information center

Operation	Command
Display the content of information channel	display channel [<i>channel-number</i> <i>channel-name</i>]
Display configuration of system log and memory buffer	display info-center
Display the attribute of logbuffer and the information recorded in logbuffer	display logbuffer [summary] [size <i>sizenum</i> [reverse] level { <i>levelNum</i> emergencies alerts critical errors warnings notifications informational debugging }] * [[{ begin include exclude } <i>text</i>]
Display the summary information recorded in logbuffer	display logbuffer summary [level <i>severity</i>]
Display the attribute of trapbuffer and the information recorded in trapbuffer	display trapbuffer [summary] [level [<i>levelNum</i> emergencies alerts critical debugging errors informational notifications warnings]] [size <i>sizenum</i>]
Clear information in memory buffer	reset logbuffer
Clear information in trap buffer	reset trapbuffer

Configuration Examples of Sending Log to the Unix Loghost

Network requirements

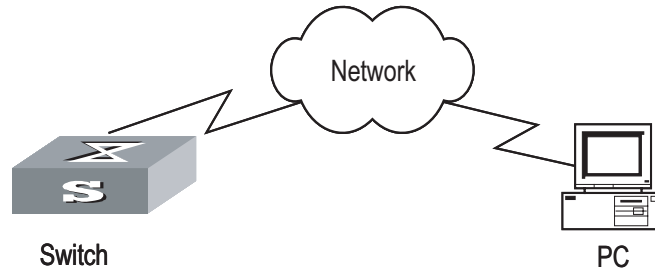
The network requirements are as follows:

- Sending the log information of the switch to UNIX loghost
- The IP address of the loghost is 202.38.1.10
- The information with the severity level above informational will be sent to the loghost
- The output language is English

- The modules that allowed to output information are ARP and IP

Network diagram

Figure 192 Network diagram



Configuration steps

1 Configuration on the switch

Enable information center

```
[SW8800] info-center enable
```

Set the host with the IP address of 202.38.1.10 as the loghost; set the severity level threshold value as informational, set the output language to English; set that the modules which are allowed to output information are ARP and IP.

```
[SW8800] info-center loghost 202.38.1.10 facility local4 language english
[SW8800] info-center source arp channel loghost log level informational
[SW8800] info-center source ip channel loghost log level informational
```

2 Configuration on the loghost

This configuration is performed on the loghost. The following example is performed on SunOS 4.0 and the operation on Unix operation system produced by other manufactures is generally the same to the operation on SunOS 4.0.

Step 1: Perform the following command as the super user (root).

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

Step 2: Edit file /etc/syslog.conf as the super user (root), add the following selector/actor pairs.

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



Note the following points when editing /etc/syslog.conf:

- The note must occupy a line and start with the character #.
- There must be a tab other than a space as the separator in selector/actor pairs.
- No redundant space after file name.
- The device name and the acceptant log information level specified in /etc/syslog.conf must be consistent with information center loghost and

information center loghost a.b.c.d facility configured on the switch. Otherwise, the log information probably cannot be output to the loghost correctly.

Step 3: After the establishment of information (log file) and the revision of /etc/syslog.conf, you should send a HUP signal to syslogd (system daemon), through the following command, to make syslogd reread its configuration file /etc/syslog.conf.

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

After the above operation, the switch system can record information in related log files.



To configure facility, severity, filter and the file syslog.conf synthetically, you can get classification in great detail and filter the information.

Configuration examples of sending log to Linux loghost

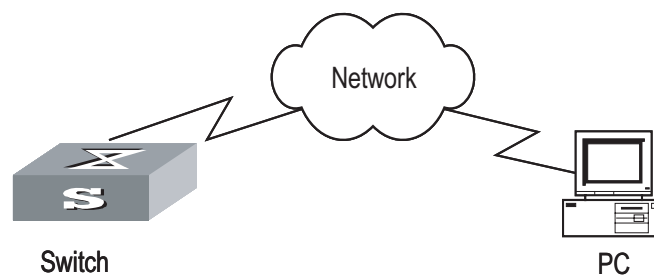
Network requirements

The Network requirements are as follows:

- Sending the log information of the switch to LINUX loghost
- The IP address of the loghost is 202.38.1.10
- The information with the severity level above informational will be sent to the loghost
- The output language is English
- All modules are allowed to output information

Network diagram

Figure 193 Network diagram



Configuration procedure

1 Configuration on the switch

Enable information center

```
[SW8800] info-center enable
```

Set the host with the IP address of 202.38.1.10 as the loghost; set the severity level threshold value as informational, set the output language to English; set all the modules are allowed output information.


```
[SW8800] info-center loghost 202.38.1.10 facility local7 language english
[SW8800] info-center source default channel loghost log level informational
```

2 Configuration on the loghost

This configuration is performed on the loghost.

Step 1: Perform the following command as the super user (root).

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

Step 2: Edit file /etc/syslog.conf as the super user (root), add the following selector/actor pairs.

```
# 3Com configuration messages
local7.info /var/log/3Com/information
```



Note the following points when editing /etc/syslog.conf:

- The note must occupy a line and start with the character #.
- There must be a tab other than a space as the separator in selector/actor pairs.
- No redundant space after file name.
- The device name and the acceptant log information level specified in /etc/syslog.conf must be consistent with information center loghost and information center loghost a.b.c.d facility configured on the switch. Otherwise, the log information probably cannot be output to the loghost correctly.

Step 3: After the establishment of information (log file) and the revision of /etc/syslog.conf, you should view the number of syslogd (system daemon) through the following command, kill syslogd daemon and reuse -r option the start syslogd in daemon.

```
# ps -ae | grep syslogd
147
# kill -9 147
# syslogd -r &
```



For LINUX loghost, you must ensure that syslogd daemon is started by -r option.

After the above operation, the switch system can record information in related log files.



To configure facility, severity, filter and the file syslog.conf synthetically, you can get classification in great detail and filter the information.

Configuration Examples of Sending Log to the Console Terminal

Network requirements

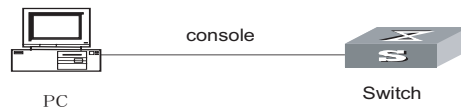
The network requirements are as follows:

- Sending the log information of the switch to console terminal
- The information with the severity level above informational will be sent to the console terminal
- The output language is English

The modules that allowed to output information are ARP and IP

Network diagram

Figure 194 Network diagram



Configuration procedure

1 Configuration on the switch

Enable information center.

```
[SW8800] info-center enable
```

Configure console terminal log output; allow modules ARP and IP to output information; the severity level is restricted within the range of emergencies to informational.

```
[SW8800] info-center console channel console
```

```
[SW8800] info-center source arp channel console log level informational
```

```
[SW8800] info-center source ip channel console log level informational
```

Enable terminal display function.

```
<SW8800> terminal logging
```

72

SYSTEM MAINTENANCE AND DEBUGGING

Basic System Configuration

The basic system configuration and management include:

- Switch name setting
- System clock setting
- Time zone setting
- Summer time setting

Setting a Name for a Switch

Perform the following configuration in system view.

Table 797 Set a name for a switch

Operation	Command
Set a switch name	sysname <i>sysname</i>
Restore the switch name to the default	undo sysname

Setting the System Clock

Perform the following configuration in user view.

Table 798 Set the system clock

Operation	Command
Set the system clock	clock datetime <i>HH:MM:SS YYYYMMDD</i>

Setting the Time Zone

You can configure the name of the local time zone and the time difference between the local time and the Universal Time Coordinated (UTC) time.

Perform the following configuration in user view.

Table 799 Set the time zone

Operation	Command
Set the local time	clock timezone <i>zone-name</i> { add minus } <i>HH:MM:SS</i>
Restore to the default UTC time zone	undo clock timezone

By default, the UTC time zone is adopted.

Setting the Summer Time

You can set the name, start and end time of the summer time.

Perform the following configuration in user view.

Table 800 Set the summer time

Operation	Command
Set the name and range of the summer time	clock summer-time <i>zone-name</i> { one-off repeating } <i>start-time start-date end-time end-date offset-time</i>
Remove the setting of the summer time	undo clock summer-time

By default, the summer time is not set.

Displaying the Status and Information of the System

The switch provides the **display** command for displaying the system status and statistics information.

For the **display** commands related to each protocols and different ports, refer to the relevant chapters. The following **display** commands are used for displaying the system status and the statistics information.

Perform the following configuration in any view.

Table 801 The display commands of the system

Operation	Command
Display the system clock	display clock
Display the system version	display version
Display the status of the debugging	display debugging [interface { <i>interface-type interface-number</i> } [<i>module-name</i>]
Display the information about the optical module connected with a in-position optical port on current frame	display fiber-module or display fiber-module [<i>interface-type interface-number</i>]

System Debugging

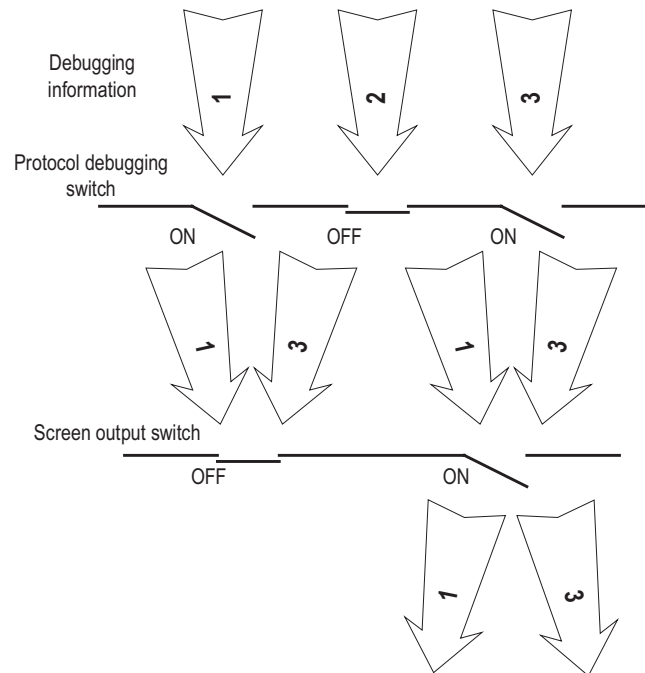
Enabling/Disabling the Terminal Debugging

The switch provides various ways for debugging most of the supported protocols and functions, which can help you diagnose and locate the errors.

The following ON/OFF switches can control the outputs of the debugging information:

- Protocol debugging ON/OFF switch controls the debugging output of a protocol.
- Terminal debugging ON/OFF switch controls the debugging output on a specified user screen.

The figure below illustrates the relationship between two ON/OFF switches.

Figure 195 Debugging output

You can use the following commands to control the above-mentioned debugging. Perform the following operations in user view.

Table 802 Enable/Disable the debugging

Operation	Command
Enable the protocol debugging	debugging { all timeout <i>interval</i> <i>module-name</i> [<i>debugging-option</i>] }
Disable the protocol debugging	undo debugging { all <i>module-name</i> [<i>debugging-option</i>] }
Enable the terminal debugging	terminal debugging
Disable the terminal debugging	undo terminal debugging

For more about the usage and format of the debugging commands, refer to the relevant chapters.



*Since the debugging output will affect the system operating efficiency, do not enable the debugging without necessity, especially use the **debugging all** command with caution. When the debugging is over, disable all the debugging.*

Displaying Diagnostic Information

When the switch does not run well, you can collect all sorts of information about the switch to locate the source of fault. Each module has its corresponding display command which displays the operating information of related module for fault locating and analyzing. You can use the **display diagnostic-information** command.

Perform the following operations in any view.

Table 803 Display diagnostic information

Operation	Command
Display diagnostic information	display diagnostic-information



When using the **display diagnostic-information** command to keep track of the switch, you should execute the command at least twice so that you can compare the information for locating problems.

Testing Tools for Network Connection

ping The **ping** command can be used to check the network connectivity and host reachability.

Perform the following configuration in any view.

Table 804 Execute the ping command

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

The output of the command includes:

- The response to each ping message. If no response packet is received when the timer expires, "Request time out" information appears. Otherwise, the data bytes, the packet sequence number, TTL, and the round-trip time of the response packet will be displayed.
- The final statistics, including the number of sent packets, the number of received packets, the packet loss ratio, the round-trip time in its minimum value, mean value and maximum value.

quick-ping enable Use the **quick-ping enable** command to enable the ping distribution function.

Use the **undo quick-ping enable** command to disable the ping distribution function.

Perform the following configuration in system view.

Table 805 Enable/disable the PING distribution function

Operation	Command
Enable the PING distribution function	quick-ping enable
Disable the PING distribution function	undo quick-ping enable

By default, the PING distribution function is enabled.

tracert The **tracert** is used for testing the gateways passed by the packets from the source host to the destination one. It is mainly used for checking if the network is connected and analyzing where the fault occurs in the network.

The execution process of the **tracert** command is described as follows: Send a packet with TTL value as 1 and the first hop sends back an ICMP error message indicating that the packet cannot be sent, for the TTL is timeout. Re-send the packet with TTL value as 2 and the second hop returns the TTL timeout message. The process is carried over and over until the packet reaches the destination. The purpose to carry out the process is to record the source address of each ICMP TTL timeout message, so as to provide the route of an IP packet to the destination.

Perform the following configuration in any view.

Table 806 The tracert command

Operation	Command
Trace route	tracert [-a <i>source-IP</i> -f <i>first-TTL</i> -m <i>max-TTL</i> -p <i>port</i> -q <i>num-packet</i> -vpn-instance <i>vpn-instance-name</i> -w <i>timeout</i>] <i>string</i>

73

PROTOCOL PORT SECURITY CONFIGURATION

Introduction to Protocol Port Security

The protocol port security function is short for TCP, UDP protocol port close check function. If a protocol is not enabled, this function can drop the packet whose destination IP is the virtual interface IP of the switch, so that it reduces the unnecessary communications between the modules and the CPU operation of the fabric, and enhances the anti-interference ability of the switch to the packet.

Setting the State of Protocol Port

Please perform the following configuration in system view.

Table 807 Set the status of protocol port

Operation	Command
Enable the protocol port security function	ip portsafe enable
Disable the protocol port security function	undo ip portsafe enable

By default, the protocol port security function is enabled.

At present, the following protocols are being checked:

Table 808 State of the protocol port

Protocol	Port	Default State
IGMP/IGSP	PROTOCOL:2	Close
OSPF	PROTOCOL:89	Close
PIM	PROTOCOL:123	Close
SSH	TCP:22	Close
TELNET	TCP:23	Close
HTTP	TCP:80	Open
BGP	TCP:179	Close
MPLS LDP	TCP:646	Close
DHCP	UDP:67,68	Close
NTP	UDP:123	Close
SNMP-AGENT	UDP:161	Close
RIP	UDP:520	Close
MPLS LDP	UDP:646	Close
RADIUS CLIENT	UDP:1812	Close
RADIUS LOCAL SERVER	UDP:1645,1646	Open
PORTAL SERVER	UDP:2000	Close

Set the State of HTTP Protocol port

Perform the following configurations in system view.

Table 809 Set the status of HTTP protocol port

Operation	Command
Shutdown the port of HTTP protocol	ip http shutdown
Open the port of HTTP protocol	undo ip http shutdown

By default, the port 80 of HTTP protocol is enabled.

74

PACKET STATISTICS CONFIGURATION

Introduction to Egress Packet Statistics

A card provides two sets of counters for monitoring egress packet statistics of the card. The monitored objects include ports, VLANs, ports+VLANs, and cards. In addition to these four types of objects, a traffic class (TC) or a drop precedence (DP) can also be monitored. When monitoring a card, the counters can monitor all TCs and all DPs. Egress packet statistics involves the number of unicast packets, the number of multicast packets, the number of broadcast packets, the number of bridge-filtered packets and the number of dropped packets in congestion. In packet statistic, only the number of packets, rather than the number of bytes, is counted.



A card provides only two sets of counters, Counter0 and Counter1, which are independent of each other.

Configuring Egress Packet Statistics Counters**Table 810** Configure egress packet statistics counters

Operation	Command	Remarks
Enter system view	system-view	-
Configure the monitored objects of the egress packet statistics counters	set egress { counter0 counter1 } slot <i>slot-num</i> [interface <i>interface-type interface-number</i>] [vlan <i>vlan-id</i>] [tc <i>traffic-class</i>] [dp <i>drop-precedence</i>]	Required By default, the egress packet statistics counters of a card monitor all ports, all VLANs, all TCs, and all DPs By default, egress packet statistics is disabled for cards
Query counter information	display egress { counter0 counter1 } slot <i>slot-num</i> [clear]	The display command can be used in any view

Note that:

- You cannot configure ports as the objects to be monitored by the egress packet statistics counters on GV48D, GT24D, GP24D, XP4B and XP4CA cards.
- After successful configuration, it is necessary to reset the counters to start counting again.
- If the monitored objects are ports, you can use the **display current-configuration | include egress** command to view the port configuration.

75

ETHERNET PORT LOOPBACK DETECTION

Ethernet Port Loopback Detection Function

Use the following configuration tasks can enable the port loopback detection function, configure the VLAN enabled with the loopback detection function (you can configure up to 800 such VLANs) and set the interval for external loopback detection on ports to check whether there exists a loop on each port or not. If a loop is found on a port, the switch will give out a trap alarm and determine whether performing Shutdown on this loop or not according to your configuration.

Configuring the Loopback Detection Function

Table 811 Configure the loopback detection function

Operation	Command	Remarks
Ether system view	system-view	-
Enable the global loopback detection function	loopback-detection enable	Required
Enable the loopback detection function in a VLAN	loopback-detection enable vlan { <i>vlanlist</i> all }	Required; (need to enable the global loopback detection function)
Set the time interval for external loopback detection on a port	loopback-detection interval-time <i>time</i>	Optional; (need to enable the global loopback detection function)
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-num</i>	-
Enable the control function of port loopback detection	loopback-detection control	Optional; (need to enable the global loopback detection function)
Disable the port loopback detection function	loopback-detection disable	Optional; (need to enable the global loopback detection function)
Display the port loopback detection information	display loopback-detection	Display it in any view

Displaying and Maintaining the Loopback Detection Function

Execute the **display** command in any view to display the configuration information of the loopback detection function and the detection results.

Table 812 Display and maintain the loopback detection function

Operation	Command
Display loopback detection information	display loopback-detection

76

QINQ CONFIGURATION

QinQ Overview

Introduction to QinQ

QinQ refers to the technology that enables packets to be transmitted across the operators' backbone networks with VLAN tags of private networks nested in those of public networks. In public networks, packets of this type are transmitted by their outer VLAN tags (that is, the VLAN tags of public networks). And those of private networks, which are nested in the VLAN tags of public networks, remain intact.

Figure 196 describes the structure of the packets with single VLAN tags.

Figure 196 Structure of packets with private network VLAN tags

DA (6B)	SA (6B)	ETYPE(8100) (2B)	User VLAN TAG (2B)	ETYPE (2B)	DATA (0-1500B)	FCS (4B)
------------	------------	---------------------	-----------------------	---------------	-------------------	-------------

Figure 197 describes the structure of the packets with nested VLAN tags.

Figure 197 Structure of packets with nested VLAN tags

DA (6B)	SA (6B)	ETYPE(8100) (2B)	Nested VLAN TAG (2B)	ETYPE (2B)	User VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)
------------	------------	---------------------	-------------------------	---------------	-----------------------	---------------	-------------------	-------------

Compared with MPLS-based L2VPN, QinQ has the following features:

- Layer 2 VPN tunnels that are simpler.
- QinQ can be implemented without the support of signaling protocols. You can enable QinQ by static configuring.

As QinQ is implemented through trunk port defined in 802.1Q, all devices along tunnels with QinQ employed must be 802.1Q-enabled. Therefore, QinQ is suitable for small-sized metropolitan area networks (MANs) or intranets with Layer 3 switches operate as the core layer devices.

QinQ provides you with the following benefits:

- Saves public network VLAN IDs.
- You can have VLAN IDs of your own, which do not conflict with public network VLAN IDs.
- Provide simple Layer 2 VPN solutions for small-sized MANs or intranets.

Implementation of QinQ QinQ can be implemented on Switch 8800 Family series switches in the following ways:

1 Enabling VLAN VPN on ports

With VLAN VPN enabled, a received packet is tagged with the default VLAN tag of the port no matter whether or not the packet carries a VLAN tag. Otherwise, the packet is transmitted with the default VLAN tag carried.

2 Configuring traffic classification-based nested VLANs

You can implement QinQ in a more flexible way by configuring traffic classification-based nested VLANs. You can specify to perform the following operations on packets that match specified ACL rules:

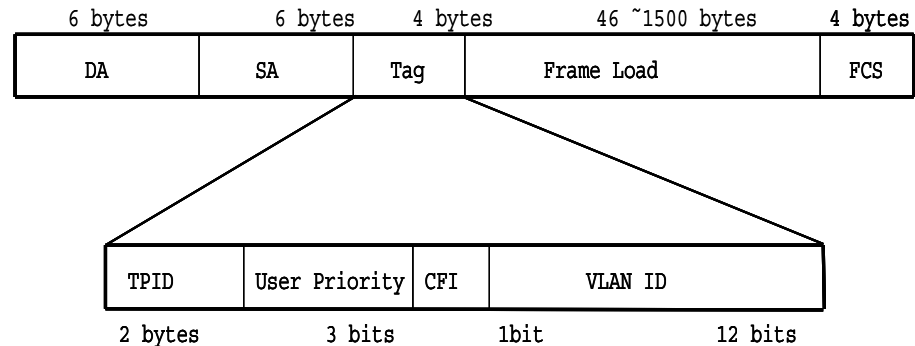
- Setting the outer VLAN tags
- Modifying the outer VLAN tags

Adjusting TPID Values of QinQ Packets

Tag protocol identifier (TPID) is a portion of the VLAN tag field. IEEE 802.1Q specifies the value of TPID to be 0x8100.

The structure of the Tag field of an Ethernet frame defined by IEEE 802.1Q is as follows:

Figure 198 The structure of the Tag field of an Ethernet frame



By default, a Switch 8800 Family series switch uses 0x8100 as the value of the TPID field, which is defined by IEEE 802.1Q. But Switch 8800 Family series switches can also adjust the TPID values of QinQ packets. This ensures Switch 8800 Family series switches are compatible with devices coming from other vendors even through the later use other TPID values (such as 0x9100 or 0x9200) in the outer tags of QinQ packets.

To modify the TPID values of packets, you need to set the ports connecting to the public networks to be VLAN-VPN uplink ports, whose TPID value can be configured by users. After you configure a TPID value for a VLAN-VPN uplink port, the switch substitutes the new TPID values for those VLAN-VPN uplink ports in the outer tags carried by received packets before transmitting the packet through the VLAN-VPN uplink ports to enable these packets to be accepted by devices of other vendors.

VLAN VPN Configuration

Configuration Prerequisites

- GARP VLAN registration protocol (GVRP), spanning tree protocol (STP), and 802.1x protocol are disabled on the ports.
- IGMP Snooping is disabled in the VLAN to which the ports belong.
- IGMP is disabled in the VLAN to which the port belongs.
- This port is not a VLAN-VPN uplink port.

Configuration procedure

Table 813 Configure VLAN VPN for a port

Configuration step	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface { <i>interface-type</i> <i>interface-number</i> <i>interface-name</i> }	-
Enable VLAN VPN	vlan-vpn enable	By default, VLAN VPN is disabled on a port. The port for which you enable VLAN VPN must be an Access port.
Display VLAN VPN configuration information about all ports in the system	display port vlan-vpn	Information about the current TPID value, VLAN-VPN ports, VLAN-VPN uplink ports is displayed.



CAUTION:

- VLAN VPN cannot be enabled if the port has any of the protocol among GVRP, STP, and 802.1x enabled.
- VLAN VPN cannot be enabled on a port if the VLAN which the port belongs to has IGMP Snooping enabled or its VLAN interface has IGMP enabled. Similarly, if a port is VLAN VPN-enabled, you cannot enable IGMP Snooping in the VLAN to which the port belongs or enable IGMP on the VLAN interface of the VLAN.
- If you have enabled VLAN VPN for the ports in the VLAN, the VLAN cannot be removed.
- After you enable the QinQ function, the configured ACL may fail to function.

VLAN VPN Configuration

Configuration Prerequisites

None

Configuration Procedure

Table 814 Configure VLAN VPN for PVC

Configuration step	Command	Description
Enter system view	system-view	-

Table 814 Configure VLAN VPN for PVC

Configuration step	Command	Description
Enter PVC view	pvc { name <i>pvc-name</i> [<i>vpi/vci</i>] <i>vpi/vci</i> }	-
Enable VLAN VPN for PVC	vlan-vpn enable	By default, VLAN VPN is disabled by default.

Traffic Classification-Based Nested VLAN Configuration

Configuration prerequisites

- ACLs and corresponding rules to be applied already exist.
- The VLANs to be specified by the *nested-vlanid* argument already exist.

Configuration procedure

Table 815 Configure traffic classification-based nest vlan

Configuration step	Command	Description
Enter system view	system-view	-
Enter Ethernet port view or port group view	interface { <i>interface-type</i> <i>interface-number</i> <i>interface-name</i> } or port-group <i>index</i>	-
Deliver a Layer 3 traffic classification rule	traffic-redirect inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] nested-vlan <i>nested-vlanid</i>	
Set outer VLAN tags for the packets matching the ACL rules	Deliver both Layer 2 and Layer 3 traffic classification rules	Make sure the VLAN which the <i>nested-vlanid</i> argument specifies exists to prevent otherwise the packets from being discarded.
Deliver a Layer 2 traffic classification rule	traffic-redirect inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] nested-vlan <i>nested-vlanid</i>	
	Deliver a Layer 2 traffic classification rule	
	traffic-redirect inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] nested-vlan <i>nested-vlanid</i>	

Table 815 Configure traffic classification-based nest vlan

Configuration step	Command	Description
Deliver a Layer 3 traffic classification rule	traffic-redirect inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] modified-vlan <i>modified-vlanid</i>	
Modify outer VLAN tags for the packets matching the ACL flow rules	traffic-redirect inbound ip-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i>] modified-vlan <i>modified-vlanid</i>	This command modifies the outer VLAN tag of the packets.
Deliver a Layer 2 traffic classification rule	traffic-redirect inbound link-group { <i>acl-number</i> <i>acl-name</i> } [rule <i>rule</i> [system-index <i>index</i>]] modified-vlan <i>modified-vlanid</i>	



CAUTION: At present, the **traffic-redirect** { *nested-vlan* | *modified-vlan* } command is only supported on 3C17533 24-port 1000 Base-X modules.

Traffic Classification-Based Nested VLAN Configuration Example

Network requirements

- As shown in Figure 199, two types of services run on the Switch 8814: common internet access and on-demand multicast video. Traffic classification-based nested VLAN encapsulates different tags at the exterior layer to distinguish the two services based on the packet tag sent by the digital subscriber line access multiplexer telnet (DSLAM).
- VLAN 100 to VLAN 512 can be used by internet access users at home. For the packets in this VLAN range, Switch 8814 needs to encapsulate another external tag of VLAN 1000, and then sends the packets to BRAS.

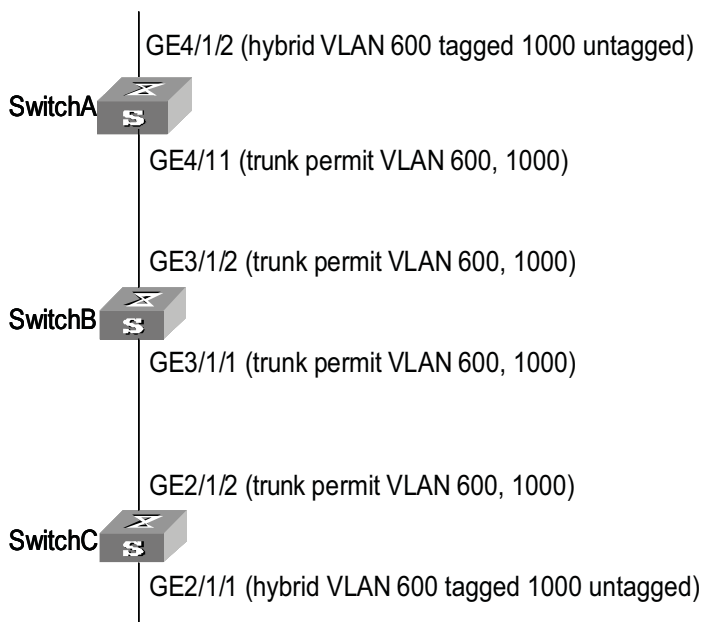
VLAN 600 is a multicast VLAN. When receiving a packet with the tag of VLAN 600, Switch 8814 does not process the packet.



Assume that 3C17533 24-port 1000 Base-X modules are installed in the slot 2 of Switch A and Switch C. And a card with any type of GE port is installed in slot 3 of Switch B.

Network diagram

Figure 199 QinQ network diagram



Configuration procedure

Enable IGMP-snooping in VLAN 600.

```

<Switch_A> system-view
[Switch_A] vlan 600
[Switch_A-vlan600] igmp-snooping enable
[Switch_A-vlan600] quit
  
```

Configure the downlink port GigabitEthernet 4/1/2 to a hybrid port. Configure VLAN 1000 to be untagged and VLAN 600 to be tagged.

```

[Switch_A] interface GigabitEthernet4/1/2
[Switch_A-GigabitEthernet4/1/2] port link-type hybrid
[Switch_A-GigabitEthernet4/1/2] port hybrid vlan 600 tagged
[Switch_A-GigabitEthernet4/1/2] port hybrid vlan 1000 untagged
[Switch_A-GigabitEthernet4/1/2] quit
  
```

Configure the flow template.

```

[Switch_A] flow-templte user-defined slot 4 s-tag-vlan
[Switch_A-GigabitEthernet4/1/2] flow-templte user-defined
[Switch_A-GigabitEthernet4/1/2] quit
  
```

Configure QinQ so that when the packets of VLAN 100 to 512 leave the uplink port GigabitEthernet 4/1/1, they need to be tagged with the exterior tag of VLAN 100.

```

[Switch_A] acl number 4000
[Switch_A-acl-link-4000] rule 0 permit s-tag-vlan 100 to 512 nested-vlan 1000
[Switch_A-GigabitEthernet4/1/2] traffic-redirect inbound link-group 4000 rule 0
nested-vlan 1000
[Switch_A-GigabitEthernet4/1/2] vlan filter disable
[Switch_A-GigabitEthernet4/1/2] quit
  
```

Configure the uplink port GigabitEthernet 4/1/1 to a trunk port and allow the packets of VLAN 1000 and VLAN 600 to pass the uplink port.

```
[Switch_A] interface GigabitEthernet4/1/1
[Switch_A-GigabitEthernet4/1/1] port link-type trunk
[Switch_A-GigabitEthernet4/1/1] port trunk permit vlan 600 1000
```

Adjusting TPID Values for QinQ Packets

Configuration Prerequisites

As VLAN-VPN uplink ports often works with the VLAN VPN ports, make sure that:

- GVRP, STP or 802.1x is not enabled on the port.
- VLAN VPN is not enabled on the port.

Configuration Tasks

Table 816 Adjust TPID values for QinQ packets

Configuration step	Command	Description
Enter system view	system-view	-
Set a TPID value for the port	vlan-vpn tpid <i>value</i>	The <i>value</i> argument ranges from 1 to 0xFFFF and defaults to 0x8100. Do not set the TPID value to a value that causes conflicts, such as that of known protocol type.
Enter Ethernet port view	interface { <i>interface-type</i> <i>interface-number</i> <i>interface-name</i> }	-
Set the port to be a VLAN-VPN uplink port.	vlan-vpn uplink enable	By default, a port is not a VLAN-VPN uplink port.
Display VLAN VPN configuration information about all ports in the system	display port vlan-vpn	Information about the current TPID value, VLAN-VPN ports and VLAN-VPN uplink ports is display.



CAUTION:

- At present, 3C17526 card does not support the **vlan-vpn uplink enable** command.
- The **vlan-vpn uplink enable** and the **vlan-vpn enable** command are mutual exclusive. That is, if you execute the **vlan-vpn enable** command on a port, you will fail to execute the **vlan-vpn uplink enable** command on the same port; if you execute the **vlan-vpn uplink enable** command on a port, you will fail to execute the **vlan-vpn enable** command on the same port.

TPID Value Configuration Example

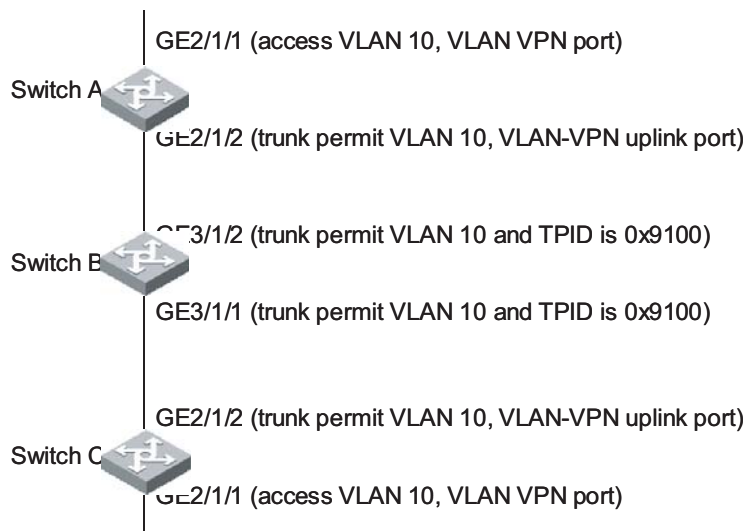
Network requirements

- Switch A and Switch C are Switch 8800 Family series switches. Switch B is a switch produced by other vendor. It uses TPID value of 0x9100.
- Two networks are connected to the GigabitEthernet2/1/1 ports of Switch A and Switch C respectively.

- Switch B only permits packets of VLAN 10.
- It is desired that packets of VLANs other than VLAN 10 can be exchanged between the networks connected to Switch A and Switch C.

Network diagram

Figure 200 Network diagram for adjusting TPID values



Configuration Procedure

- 1 Configure Switch A and Switch C. As the configuration performed on Switch A and Switch C is the same, configuration on Switch C is omitted.

Set the TPID value of the VLAN-VPN uplink port to 0x9100.

```
<SwitchA>system-view
System View: return to User View with Ctrl+Z.
[SwitchA]vlan-vpn tpid 9100
[SwitchA]vlan 10
[SwitchA-vlan10]quit
```

Configure the GigabitEthernet2/1/2 port to be a VLAN-VPN uplink port and add it to VLAN 10 (a trunk port).

```
[SwitchA]interface GigabitEthernet2/1/2
[SwitchA-GigabitEthernet2/1/2]port link-type trunk
[SwitchA-GigabitEthernet2/1/2]port trunk permit vlan 10
[SwitchA-GigabitEthernet2/1/2]vlan-vpn uplink enable
```

Configure the GigabitEthernet2/1/1 port to be a VLAN VPN port and add it to VLAN 10 (an access port).

```
[SwitchA]interface GigabitEthernet2/1/1
[SwitchA-GigabitEthernet2/1/1]port access vlan 10
[SwitchA-GigabitEthernet2/1/1]vlan-vpn enable
[SwitchA-GigabitEthernet2/1/1]quit
```

- 2 Configure Switch B

Because Switch B is produced by other vendor, related commands may differ from those available to Switch 8800 Family switches. So only the operation is listed, as shown below:

- Configure GigabitEthernet3/1/1 and GigabitEthernet3/1/3 ports of Switch B to be trunk ports.
- Add the two ports to VLAN 10.



The following describes how a packet is forwarded from Switch A to Switch C.

- As the GigabitEthernet2/1/1 port of Switch A is a VLAN VPN port, when a packet reaches GigabitEthernet2/1/1 port of Switch A, it is tagged with the default VLAN tag (VLAN 10, the outer tag) and is then forwarded to GigabitEthernet2/1/2 port.
- Because GigabitEthernet2/1/2 port is a VLAN-VPN uplink port with a TPID of 0x9100, Switch A changes the TPID value in the outer VLAN Tag of the packet to 0x9100, and forwards the packet to the public network.
- The packet reaches GigabitEthernet3/1/2 port of Switch B. Switch B sends the packet to its GigabitEthernet3/1/1 port by forwarding the packet in VLAN 10.
- The packet is forward from GigabitEthernet3/1/1 port of Switch B to the network on the other side and enters GigabitEthernet2/1/2 port of Switch C, Switch C sends the packet to its GigabitEthernet2/1/1 port by forwarding the packet in VLAN 10. As GigabitEthernet2/1/1 port is an access port, Switch C strip off the outer VLAN tag of the packet and restores the original packet.

It is the same case when a packet travel from Switch C to Switch A.

Verification

The configuration is successful if packets sourced from the networks connected to Switch A can reach those connected to Switch C, or packets sourced from the networks connected to Switch C can reach those connected to Switch A.

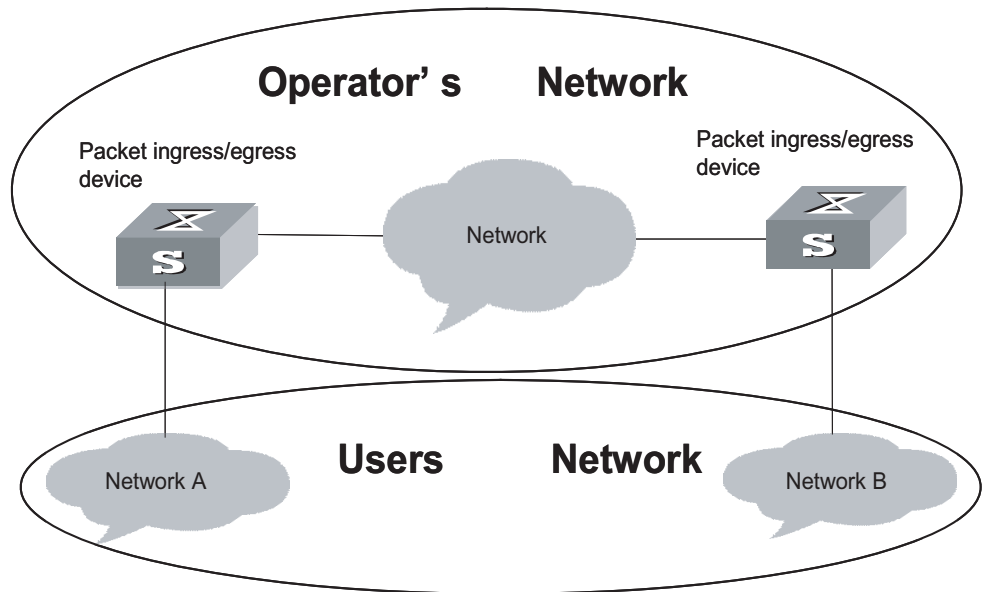
VLAN-VPN Tunnel Configuration

Introduction to VLAN-VPN Tunnel

The function of VLAN-VPN tunnel is that user networks in different regions can transmit BPDU packets transparently through VLAN VPN designated in the operator's network.

Figure 201 shows the hierarchy diagram of VLAN-VPN tunnel: operator's network and user network. The operator's network involves packet input and output devices. The user network includes network A and network B. Through the configuration on the devices at both ends of the operator's network, the destination MAC address of the BPDU packet is replaced with a MAC address in a special format at one end, and the MAC address is converted back to the original destination MAC address at the other end. In this way the packet is transmitted transparently over the operator's network.

Figure 201 Diagram of the VLAN-VPN tunnel network hierarchy



Configuring VLAN-VPN Perform the following configuration to configure VLAN-VPN tunnel.

Table 817 Configure VLAN-VPN tunnel

Operation	Command	Description
Enter system view	system-view	-
Enable VLAN-VPN tunnel	vlan-vpn tunnel	Required
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable VLAN VPN of the port	vlan-vpn enable	Required By default, VLAN VPN of the port is disabled.



VLAN VPN is not compatible with STP, DOT1X, GVRP, and NTDP.

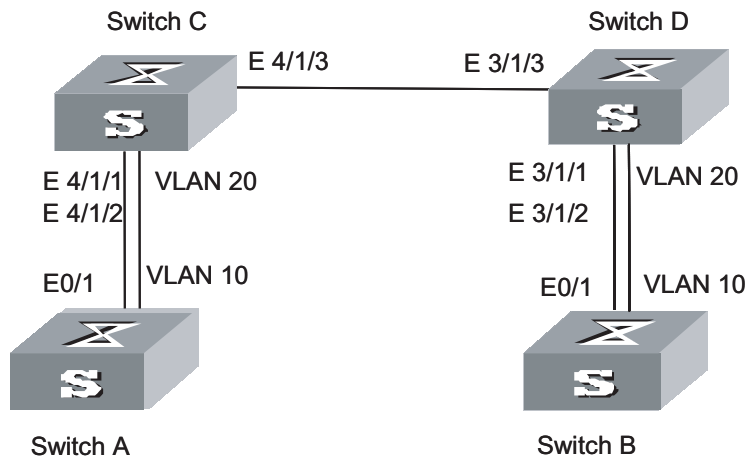
VLAN-VPN Tunnel Configuration Example

Network requirements

- Switch 8800 Family series switches, namely Switch C and D in the network diagram, serve as devices used to access the operator's network.
- Switch 8800 series switches, namely Switch A and B in the network diagram, serve as devices used to access the user network.
- Interconnect switch C and switch D through trunk ports. Enable VLAN-VPN tunnel to transmit packets transparently between the user network and the operator's network.

Network diagram

Figure 202 Configure VLAN-VPN tunnel



Configuration procedure

1 Configure switch A.

Enable RSTP.

```
[Switch_A] stp enable
```

Set the port to a trunk port and allow the packets of VLAN 10 to pass the port.

```
[Switch_A] vlan 10
[Switch_A-Ethernet0/1] port link-type trunk
[Switch_A-Ethernet0/1] port trunk permit vlan 10
```

2 Configure switch B.

Enable RSTP.

```
[Switch_B] stp enable
```

Set the port to a trunk port and allow the packets of VLAN 10 to pass the port.

```
[Switch_B] vlan 10
[Switch_B-Ethernet0/1] port link-type trunk
[Switch_B-Ethernet0/1] port trunk permit vlan 10
```

3 Configure switch C.

Enable MSTP.

```
[Switch_C] stp enable
```

Enable VLAN-VPN tunnel.

```
[Switch_C] vlan-vpn tunnel
```

Add Ethernet4/1/1 to VLAN 20.

```
[Switch_C] vlan 20
[Switch_C-Vlan20] port Ethernet4/1/1
[Switch_C-Vlan20] quit
```

Disable the STP protocol and enable VLAN-VPN on Ethernet4/1/1.

```
[Switch_C] interface Ethernet4/1/1
[Switch_C-Ethernet4/1/1] stp disable
[Switch_C-Ethernet4/1/1] vlan-vpn enable
[Switch_C-Ethernet4/1/1] quit
```

Add Ethernet4/1/2 to VLAN 20.

```
[Switch_C] vlan 20
[Switch_C-Vlan20] port Ethernet4/1/3
[Switch_C-Vlan20] quit
```

Disable the STP protocol and enable VLAN-VPN on Ethernet4/1/2.

```
[Switch_C] interface Ethernet4/1/2
[Switch_C-Ethernet4/1/2] stp disable
[Switch_C-Ethernet4/1/2] vlan-vpn enable
[Switch_C-Ethernet4/1/2] quit
```

Set Ethernet4/1/3 to a trunk port and add this port to all the VLANs.

```
[Switch_C] interface Ethernet4/1/3
[Switch_C-Ethernet4/1/3] port link-type trunk
[Switch_C-Ethernet4/1/3] port trunk permit vlan all
```

4 Configure switch D.

Enable MSTP.

```
[Switch_D] stp enable
```

Enable VLAN-VPN tunnel.

```
[SW8800] vlan-vpn tunnel
```

Add Ethernet3/1/1 to VLAN 20.

```
[Switch_D] vlan 20
[Switch_D-Vlan20] port Ethernet3/1/1
[Switch_D-Vlan20] quit
```

Disable the STP protocol and enable VLAN-VPN on Ethernet3/1/1.

```
[Switch_D] interface Ethernet3/1/1
[Switch_D-Ethernet3/1/1] stp disable
[Switch_D-Ethernet3/1/1] vlan-vpn enable
[Switch_D-Ethernet3/1/1] quit
```

Add Ethernet3/1/2 to VLAN 20.

```
[Switch_D] vlan 20
[Switch_D-Vlan20] port Ethernet3/1/2
[Switch_D-Vlan20] quit
```

Disable the STP protocol and enable VLAN-VPN on Ethernet3/1/3.

```
[Switch_D] interface Ethernet3/1/2
[Switch_D-Ethernet3/1/2] stp disable
[Switch_D-Ethernet3/1/2] vlan-vpn enable
[Switch_D-Ethernet3/1/2] quit
```

Set Ethernet3/1/3 to a trunk port and add this port to all the VLANs.

```
[Switch_D] interface Ethernet3/1/3
[Switch_D-Ethernet3/1/3] port link-type trunk
[Switch_D-Ethernet3/1/3] port trunk permit vlan all
```



CAUTION:

- STP must be enabled on VLAN-VPN tunnel-enabled devices; otherwise BPDUs in the user network cannot be transmitted transparently.
- VLAN-VPN-enabled ports must be configured to Access ports. The link type of the intermediate operator's network must be configured to the Trunk link.
- You cannot configure VLAN-VPN tunnel on the ports where DOT1X, GVRP, STP, or NTDP is enabled.

Introduction to NQA

NQA, which is an enhancement of the ping function, is used to test the performance of various protocols operating in the network. The ping function can only use the ICMP protocol to test the round trip travel time of data packets between the local endpoint and the specified destination endpoint by command lines. While the NQA not only can finish the above functions, but also can probe whether the DLSW, DHCP, FTP, HTTP, and SNMP servers are on or off, and test the response time of various services. Besides, the NQA also realizes the MIB operation through which you can perform various tests conveniently.

The ICMP function test of NQA has the following features:

The NQA function is similar with the ping function. But the NQA has more parameters and can execute multiple tests simultaneously and automatically.

The NQA function configures various parameters needed by the test through the network management tool or the command line. Then you can enable the test, and view the test result. After the test, use the **display nqa** command to display the test result.



The ICMP function of NQA and the corresponding MIB operation of the ICMP are realized on the Switch 8800 Family switch. Other functions, like DLSW, DHCP, FTP, HTTP and SNMP are not realized on the Switch 8800 Family switch at present.

NQA Configuration

The ICMP function test of the NQA includes the following configuration:

- Enable the NQA client function.
- Configure the maximum number of the test tasks that can be performed simultaneously.
- Set the NQA test group.
- Set various test parameters.
- Enable the test.
- Display the test result.

Configuration Prerequisites

The ICMP function of the NQA needs no special prerequisite; however, note the following two points during the configuration:

- Enabling the NQA client function is the prerequisite of all tests.
- To execute the test, you must set the NQA test group, configure the parameters, and then enable the test.

Introduction to NQA Configuration Tasks

Table 818 Introduction to the configuration tasks of the ICMP test in NQA

Operation	Command	Remarks
Enter system view	system-view	-
Enable the client function of the NQA	nqa-agent enable	Required; By default, NQA client is disabled.
Configure the maximum number of the test tasks performed simultaneously	nqa-agent max-requests <i>max-number</i>	Optional; The default maximum number of the test tasks performed simultaneously is 5.
Set the NQA test group, enter NQA test group view	nqa administrator-name <i>test-tag</i>	Required; By default, the system creates no test group. When a test group is set, the system automatically enter the NQA test group view.
Set the test type	test-type <i>type</i>	At present, ICMP type is the only choice By default, the test type is ICMP type.
Set the destination address to be tested	destination-ip <i>ip-address</i>	Required; By default, no destination address is set.
Set the description information of the test group	description <i>text</i>	Optional; By default, there is no description information of the test group.
Set the timeout time for the test operation	timeout <i>time</i>	Optional; By default, the timeout time for the test operation is 3 seconds
Set the number of probe packets to be sent	count <i>times</i>	Optional; By default, one probe packet is sent.
Set the life time for NQA ICMP test packet, that is, the maximum number of hops that a test packet can pass in the network	ttl <i>number</i>	Optional; By default, the maximum number of hops that a test packet can pass is 20
Set the TOS value in the NQA test packet header	tos value	Optional; By default, the TOS value in the NQA test packet header is 0, that is , no special service is specified
Set the filler data size of the test packet	datasize <i>size</i>	Optional; By default, the filler data size of the test packet is 56 bytes (including no protocol header)
Set the filler data of the test packet	datafill <i>text</i>	Optional; By default, no filler data in the test packet is empty.

Table 818 Introduction to the configuration tasks of the ICMP test in NQA

Operation	Command	Remarks
Set the name of the VPN instance	vpn-instance <i>name</i>	Optional; By default, no name of the VPN instance is set
Set the source IP address of this test	source-ip <i>ip-address</i>	Optional; By default, no source IP address is configured. The system uses the IP address of the source interface as the source IP address.
Set the source interface	source-interface { <i>interface-name</i> <i>interface-type</i> <i>interface-number</i> }	Optional; By default, no source interface is configured
Assume the connection mode between the destination address and the equipment enabling the test as direct connection mode	sendpacket passroute	Optional; By default, no such assumption
Set the number of the test results that can be stored in the history record	history-records <i>number</i>	Optional; By default, 50 test results can be stored in the history record.
Set the condition (probe) of sending Trap information to the network management system	send-trap { all { probefailure testcomplete testfailure } * }	Optional; By default, no Trap information is sent to the network management system.
Set the times of constant probe fails after which the Trap information is sent to the network management system	probe-failtimes <i>times</i>	Optional; By default, the system sends the Trap information to the network management system after one probe fail.
Set the Trap information filter condition (test)	test-failtimes <i>times</i>	Optional;By default, NQA sends the Tap information to the network management system after one NQA test fails.
Set the automatic test interval	frequency <i>interval</i>	Optional; The default interval time is 0, that is, no automatic test is performed; Configure the <i>interval</i> >0, then the system performs one automatic test every configured <i>interval</i> time
Enable the test	test-enable	Required; (ignore this configuration if you choose the frequency <i>interval</i> command to enable the automatic test); generally, use this command to enable tests.
Display the test result	display nqa { results history } [<i>administrator-name test-tag</i>]	The display command can be executed in any view.

**CAUTION:**

- When the system is testing, parameters that are configured in the NQA test group view cannot be changed except the simple description of the operations and the condition of sending the Trap information to the network management system.
- You can use the **undo test-enable** command to stop the test at any time. And you can stop the test by means of disabling the NQA client or deleting the test group.
- If you assume the connection mode as direct mode but set a TTL value at the same time, this TTL value does not take effect.
- It is not allowed to configure the source IP and the destination IP both to 0 or F. Other values are all allowed to configure. Source address can only be the Layer 3 interface configured with IP address.
- When you test for the first time, the first probe packet loses if there is no information of the destination address in the switch and the configured packet size is over the maximum size of a single packet.
- All of the parameters and test results can be displayed or set by MIB with the network management tool.

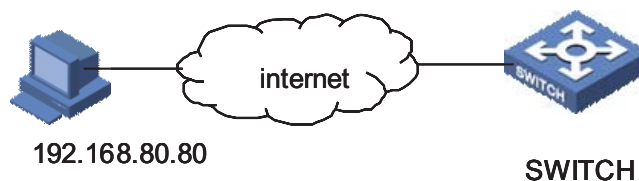
NQA Configuration Example

Network requirements

- Configure the simple NQA test. The type is ICMP.
- The destination address is 192.168.80.80. It is the address of a PC and accessible to the switch which performs the NQA test.

Network diagram

Figure 203 Network diagram for NQA configuration



Configuration procedure.

1 Enable the NQA client

Enable the NQA client.

```

<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
  
```

2 Set the NQA test group

Create an NQA test group. Its name is administrator and its test tag is icmp.

```

[SW8800] nqa administrator icmp
  
```

3 Set the parameters of the test group

Enter test group view.


```

<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa administrator icmp

# Configure the test type as icmp.

[SW8800-nqa-administrator-icmp] test-type icmp

# Configure the destination IP to 192.168.80.80.

[SW8800-nqa-administrator-icmp] destination-ip 192.168.80.80

# Configure the test times to 5.

[SW8800-nqa-administrator-icmp] count 5
4 Execute the test

# Execute one test.

[SW8800-nqa-administrator-icmp] test-enable
5 Display the test results

# Display the results of this test in this test group.

<SW8800> display nqa results administrator icmp
nqa entry(admin administrator, tag icmp) test results:
  Destination ip address:192.168.80.80
  Vpn-instance: NULL
  Send operation times: 5                Receive response times: 5
  Min/Max/Average Round Trip Time: 21/33/25
  Square-Sum of Round Trip Time: 3557
  Last complete test time: 2005-12-8 11:22:33.4
Extended result:
  Packet lost in test: 0%
  Disconnect operation number:0         Operation timeout number:0
  System busy operation number:0       Connection fail number:0
  Operation sequence errors:0          Drop operation number:0
  Other operation errors:0

```

Displaying and Maintaining NQA

Use the **display** command to display the operation status after the above configurations. Verify the configuration effect through the displayed information.

Table 819 Display and maintain NQA

Operation	Command
Display the configuration information	display current-configuration or display this in NQA test group view
Display the test results	display nqa { results history } [administrator-name test-tag]

Introduction to Password Control Configuration

Switch 8800 Family series switches provide the password control function. Before a user can log in to the switch, a system login password must be configured. After a password is configured, the user must enter the password each time he or she wants to log in to the switch. The user can successfully log in to the switch and proceed with operations only if he or she passes the authentication. If the password authentication fails, the user will not be able to log in to the switch.

The user can either use the default password configuration, or perform his or her own password control configuration. When conducting password control, the user must follow the steps below:

1 Configuring system login password

If password authentication is required for a user to log in to the system, the system will protect the password, instead of displaying the input password in the command line. The password must not be displayed in plain text either in the system configuration file or on the terminal: the password must be encrypted before being stored.

When a user inputs the password, "*****", rather than the plain text of the user's password, will appear on the terminal. When configuring a password, the user needs to input the password twice for confirmation. During password configuration, the password appears as "*****" in the command line, and it appears in the form of encrypted text in the configuration file.

2 Enabling password control

After password configuration, the user can conduct password control, which includes the following aspects:

- Enabling password aging
- Enabling limitation of minimum password length
- Enabling history password recording

When a login password expires, the system will require the user to input a new password and will save the old password automatically. By recording the history passwords, the system can prevent the user from using a single password or repeated passwords when modifying a password, thus to enhance the security.

The system stores the history password records in a private file in the flash memory. This file is not accessible to any user. In addition, the system automatically backs up the history password records and blacklist records, specifically as follows:

- When adding or deleting a history password record, the system requests the standby card to perform backup.
- When purging all history records or the history records of a certain user, the system requests the standby card to perform backup.
- When adding a user to or deleting a user from the blacklist, the system requests the standby card to perform backup.
- The flash memory on the active card and that on the standby keeps the same copies of history password records and blacklist records.

3 Configuring system password parameters

After password confirmation, the administrator can modify the password at the next login. Password parameters include:

- Password aging time
- Alert time before the password expires
- Minimum password length
- Maximum the number of attempts of entering a password and the processing mode for failed login attempts
- Maximum number of history password records
- Timeout time for user authentication

4 Configuring super password parameters

User levels are configured by the administrator during user configuration. The command **super** is used to change user levels. For example, a user of level 3 is allowed to log in to the system. After logging in, if the user wants to change his or her user level, the user needs to use the command **super** and pass the **super** password authentication. Password control, namely password aging and minimum password length limitation, must be enabled for this password.

5 Deleting history password records

After the history password record of a user is deleted, the configuration of a new password will not be restricted by the previously configured history password records. The system allows the deletion of the history password records of all users or a specific user.

Password Control Configuration

Configuration Prerequisites

A PC is connected with an Switch 8800 Family switch, and both devices work normally.

Configuration Tasks

The basic configuration tasks of password control are as follows:

- Configuring system login password
- Enabling password control

- Configuring system password parameters
- Configuring super password parameters
- Deleting history password records

After the configuration, you can carry out **display password-control** in any view to view the password control information for all users, including the enabled/disabled state of password aging, the aging time, the enabled/disabled state of the minimum password length limitation and the configured minimum password length, the enabled/disabled state of history password recording, the alert time before password expiration, the timeout time for password authentication, the maximum number of password input attempts, the maximum number of history password records, the processing mode after failed password input attempts, the time when the password history was last cleared, and so on.

If a user fails to provide the correct password after the allowed number *login-times*, the system adds the user to the blacklist. To view the names and the IP addresses of such users, carry out **display password-control blacklist** in any view.

Table 820 Basic configuration tasks of password control

Operation	Command	Description
Enter system view	<code>system-view</code>	-
Enter local user view	<code>local-user username</code>	-
Configure system login password	<code>password [simple cipher] password</code>	Input the password twice as prompted by the system, ensuring the same password is inputted at both time
Exit the current view and return to the system view	<code>quit</code>	
Enable password control	<code>password-control { aging length history } enable</code>	By default, password control is disabled
Configure system password parameters	<code>password-control { aging aging-time length length login-attempt login-times history max-record-num alert-before-expire alert-time authentication-timeout authentication-timeout exceed { lock unlock locktime time } }</code>	Refer to the detailed description in the following paragraphs about the configuration of system password parameters The commands password-control aging aging-time and password-control length length can also be used in the local user mode
Configure super password parameters	<code>password-control super { aging aging-time length length }</code>	By default, the aging time of the super password is 90 days, and the minimum length of the super password is 10 characters.
Delete history password records of one or all users	<code>reset password-control history-record [username username]</code>	-
Delete history records of super password	<code>reset password-control history-record super [level level-value]</code>	-

Table 820 Basic configuration tasks of password control

Operation	Command	Description
Display password control information for all users	display password-control	Display can be carried out in any view
Display super password control information	display password-control super	display can be carried out in any view

To cancel an operation, use the **undo** form of the corresponding command.

**CAUTION:**

- If the history password recording function is not enabled, the password clearing command **reset password-control history-record** can also clear the history password records of a specific user or all users.
- If the password control function is not enabled, the password aging parameters can be configured, but will not take effect.

The following paragraphs will describe the configuration of password parameters;

Configuring the aging time of system password

After the password aging function is enabled, when a user goes through authentication to log in, the system reads the creation time of the user's password and compares the password creation time with the password aging time of the user. There can be the following three cases:

- 1 If the password has not expired but is within the alert time range, the system will remind the user of the remaining days before the password will expire, and ask the user whether he or she wants to change the password. The prompt message is as follows:

```
Current user's password will age out in 2 day(s) ,Would you like to
enter a new one ? [Y/N]
```

- If the user chooses to change the password, after the password is successfully changed, the system will record the new password and record the time when the new password is set, and will allow the user to log in.
 - If the user chooses not to change the password or fails to change the password, the user can still log in normally before the password expires.
- 2 If the user password has expired, the system will notify the user about the expiration of the password, as follows:

```
your password has expired ,please enter a new password :
password: *****
confirm :*****
```

Namely, the user must enter a new password. After entering a new password, the user needs to confirm it by entering it again. If the password is not appropriate, or if the second input is different from the first input, the system will ask the user to enter a password again; otherwise the user cannot log in successfully.

- 3 If the user's password has not expired and the gap between the aging time and the expiration time is not in the range of alert time, the user can normally log in.

After the user successfully changes his or her password, the current password is saved into the file in the flash memory.

The password for **super** commands is processed in a similar way. However, no pre-expiration alert is given when the super password is to expire; the user is only notified whether the password has expired or not.

For an FTP user, no pre-expiration alert is given either when the password is to expire. The user is only notified about password errors but cannot change the password. Only the administrator can change the password.

Table 821 Configuring system password aging time

Operation	Command	Description
Enter system view	system-view	-
Configure password aging time	password-control aging <i>aging-time</i>	The value range of password aging time is 1 to 365 days. By default, the password aging time is 90 days. This command can also be carried out in user view

The configuration command for password aging time can be used either in the system view or in the user view. In the system view, this command is used to configure global parameters; in the user view, this command is used to configure the parameters for the user. When user parameters conflict with system parameters, the parameters configured in the user view will prevail.

Configuring alert time before password expires

Within the set period of time before the user password expires, the system will automatically give the following reminder information: `Current user's password will age out in 2 day (s) ,Would you like to enter a new one ? [Y/N]`, to remind the user of the remaining number of days in which the password will expire, and ask the user whether to change the password.

Table 822 Configuring alert time before password expiration

Operation	Command	Description
Enter system view	system-view	-
Configure alert time before password expires	password-control alert-before-expire <i>alert-time</i>	The range of pre-expiration alert time is 1 to 30 days. By default, the alert time is 7 days.

Configuring minimum length of password

There is a limitation for the minimum length of user-configured passwords. When a user configures a password, the system checks the password length. If the length of the password entered by the user is inappropriate, the system will give a prompt message to the user and ask the user to enter a new password.

If the password entered by the user is shorter than the set minimum length, the system will refuse this password, and will give the following prompt message: `Password is too short. Please enter minimum length password.`

The password for **super** commands is processed in the same way.

Table 823 Configuring minimum password length

Operation	Command	Description
Enter system view	system-view	-
Configure the minimum password length	password-control length <i>length</i>	The value range of the minimum password length is 4 to 32 characters. The default value is 10 characters. This command can also be carried out in user view

The configuration of minimum password length involves two situations: the global configuration command can be used in the system view to configure the minimum length of all user passwords, and the minimum password length can be configured for a certain user in the user view. Similar to the password aging time configuration, when the two types of parameters conflict, the parameters configured in the user view will prevail.

Configuring the maximum number of attempts of entering a password and the processing mode for failed login attempts

There is a limitation of the number of entering a password. When the number of attempts exceeds the configured maximum number of attempts, the system will have three options:

- The system will add the user to the blacklist and lock the user for a period of time by putting the user name + IP address and the lock time into the blacklist. Each time when the user logs in, the system will search in the blacklist. If the user name and IP address appear in the blacklist, the system will directly prohibit the user from going into password authentication. After a preset period of time, the system will remove the user from the blacklist and re-activate the user. The lock time is specified by the system administrator. The value range is 3 to 360 minutes, and the default value is 120 minutes.
- The system will permanently lock the user. In this case, the user can log in again only if he or she is removed from the blacklist and unlocked by the administrator manually. The blacklist can contain a maximum of 1024 entries.
- The system will allow the user to log in again instead of locking him or her.

Once the system administrator manually removes locked users from the blacklist, these users are unlocked and can log in to the switch again.

Table 824 Configuring the maximum number of attempts and the processing mode for failed login attempts

Operation	Command	Description
Enter system view	system-view	-
Configure the maximum number of attempts of entering a password	password-control login-attempt <i>login-times</i>	The value range of the maximum attempts of entering a password is 2 to 10; the default value is 3
Configure the processing mode for failed login attempts	password-control login-attempt <i>attempt-time exceed { lock unlock locktime time }</i>	By default, the system will lock the user and allow him/her to log in again a period of time later

Table 824 Configuring the maximum number of attempts and the processing mode for failed login attempts

Operation	Command	Description
View information of users added to the blacklist	display password-control blacklist	display can be carried out in any view If the command is carried out without <i>username</i> , all users will be removed from the blacklist
Remove a user or users from the blacklist	reset password-control blacklist [username username]	If the command is carried out with <i>username</i> , the specified user will be removed from the blacklist

Configuring the maximum number of history password records

When a password used to log in to the system expires, the system will ask the user to enter a new password and will automatically save the password. You can configure the maximum number of history records allowable for each user. The purpose is to prevent users from using a single password or repeated passwords, thus enhancing the security.

Table 825 Configuring the maximum number of history password records

Operation	Command	Description
Enter system view	system-view	-
Configure the maximum number of history password records	password-control history max-record-num	The value range of maximum number of history password records is 2 to 10, and the default value is 4



CAUTION:

- When a new password is added but the number of the recorded history passwords has reached the configured maximum number, the system replaces the oldest record with the new one.
- When you configure the maximum number of history password records, if the number of history password records is larger than the configured value, the system will give a prompt and allow you to make configuration for the user.
- When changing a password, do not use any recorded history password; otherwise, the system will give the following prompt: `The system failed to assign password. It has been used previously.` In this case, the change to the password will not take effect, and you need to configure another password.

Configuring the timeout time for password authentication

An authentication process for a user starts when the server obtains the user name and ends when the password authentication is completed for the user.

If the password authentication is not completed before the authentication times out, the authentication fails, and the system will terminate the user connection and record the log information; if the password authentication is completed before the authentication times out, the user will log in to the switch normally.

Table 826 Configuring the timeout time for password authentication

Operation	Command	Description
Enter system view	system-view	-
Configure password timeout time	password-control authentication-timeout authentication-timeout	The value range of password authentication timeout time is 30 to 120 seconds, and the default value is 60 seconds

System Logging Function

The system can automatically log related information in case of the following events:

- When a user logs in successfully, the system will log the user name, IP address, and VTY number
- When a user is prohibited by the ACL rule, the system will log the user's IP address
- When a user fails in authentication, the system will log the user name, IP address, VTY number, and failure cause
- When a user changes his or her password that has expired, the system will log the password change event

The administrator can query the login information of users based on these log records.

Password Control Configuration Example

Network requirements

A PC is connected with an Switch 8800 Family switch. You can either use the default configuration or configure the password control parameters as required.

Network diagram

Figure 204 Network diagram for password control configuration



Configuration procedure

Configure the system login password:

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] local-user test
[3Com-luser-test] password
Password:*****
confirm:*****
Updating the password file, please wait ...
```

Change the system login password to 0123456789:

```
[3Com-luser-test] password
Password:*****
```

```

Confirm :*****
Updating the password-file ,please wait...

# Enable password aging:

[SW8800] password-control aging enable
Password aging enabled for all users. Default: 90 days.

# Enable limitation of the minimum password length:

[SW8800] password-control length enable
Password minimum length enabled for all users. Default: 10 characters.

# Enable history password recording:

[SW8800] password-control history enable
Password history enabled for all users. Default: 10 history records

# Set the aging time of super passwords to 10 days:

[SW8800] password-control super aging 10

# Display the password control information of all users:

[SW8800] display password-control
Global password settings for all users:
Password aging:                Enabled(90 days)
Password length:               Enabled(10 Characters)
Password history:              Enabled(Max history records:4)
Password alert-before-expire : 7 days
Password authentication-timeout : 60 seconds
Password attempt times :      3 times
Password attempt-failed action : Lock for 120 minutes

# Display the user names and the corresponding IP addresses added to the
blacklist because of password attempt failure:

[SW8800] display password-control blacklist
USERNAME                        IP
The number of users in blacklist is :0
# Delete the history password records of all users:
<SW8800> reset password-control history-record
Are you sure to delete all the history record? [Y/N]

If you type "Y", the system will delete the history records of all users and gives the
following prompt:

Updating the password file, please wait...
All historical passwords have been cleared.

```


AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
AC	Access Code
ACK	ACKnowledgement
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AFI	Authority and Format Identifier
AH	Authentication Header
AM	Accounting Management
ANSI	American National Standard Institute
AP	Access Preamble
ARP	Address Resolution Protocol
AS	Access Server
ASBR	Autonomous System Border Router
ASCII	American Standard Code for Information Interchange
ASF	Alert Standard Forum
ASN	Abstract Syntax Notation
AU	Access Unit
AUG	Administrative Unit Group
AUX	Auxiliary (port)
BAS	Bit-rate Allocation Signal
BDR	Backup Designated Router
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
BSP	Board Support Package
BT	BitTorrent
BUS	Broadcast and Unknown Server
CA	Cell Allocation
Candidate-BSR	Candidate-BSR
Candidate-RP	Candidate-RP
CB	Cell Broadcast
CCC	Credit Card Calling
CD	Call Deflection
CE	Concurrent Engineering

CF	Call Forwarding services
CFM	Configuration File Management
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIST	Common and Internal Spanning Tree
CL	Configuration Librarian
CLNP	Connectionless Network Protocol
CON	Conference Calling
CoS	Class of Service
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
C-RP	Candidate-RP
CSNP	Complete SNP
DA	Destination Address
DB	Dummy Burst
DC	DC signaling
DCE	Data Circuit-terminal Equipment
DD	Data Date
DHCP	Dynamic Host Configuration Protocol
DMAC	Destination MAC
DNP	Development and Pilot
DNS	Domain Name Server
DoD	Downstream on Demand
DoS	Deny of Service
DP	Design Point
DR	Designated Router
DS	Data Stream
DSLAM	Digital Subscriber Line Access Multiplexer
DSP	Destination Signaling Point
DTE	Data Terminal Equipment
DU	DUration
DUT	device under test
DVMRP	Distance Vector Multicast Routing Protocol
EAP	Extensible Authentication Protocol
EAPoL	EAP over LANs
EBGP	External Border Gateway Protocol
EGP	Exterior Gateway Protocol
ES	Earliest Start Time
ESF	Extended Service Frame
ET	Exchange Terminal
FDDI	Fiber Distributed Data Interface
FE	Far End
FEC	Forward Error Control
FIB	Forward Indicator Bit

FIFO	First In First Out
FIN	Finance Management Dept.
FR	Frame Relay
FTP	File Transfer Protocol
FTPS	FTP Server
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GR	Graceful Restart
GRE	Generic Routing Encapsulation
HA	High Availability
HDLC	High-level Data Link Control
HTTP	Hyper Text Transport Protocol
IANA	Internet Assigned Number Authority
IBGP	Internal BGP
ICMP	Internet Control Message Protocol
ICP	Information Content Provider
ID	IDentification/IDentity
IDI	Initial Domain Identifier
IDP	Individual Development Plan
IE	Industrial Engineering
IETF	Internet Engineering Task Force
IF	Information Frame
IFM	IP Forward Module
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IGSP	Internet Group Management Protocol Snooping
ILM	Integrated Laser Modulator
IP	Intelligent Peripherals
IPX	Internet Packet Exchange
IS	Information Security Dept.
IS-IS	Intermediate System-to-Intermediate System
ISO	International Organization for Standardization
ISP	Interim inter-switch Signaling Protocol
IST	Immediate Service Termination (IST)
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
L2V	Layer 2 VPN
ACL	Switch ACL
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LAN	Local Area Network
LCP	Link Control Protocol

LDP	Label Distribution Protocol
LER	Label Edge Router
LIB	Indicator Light Immobility Board
QOS	Switch QoS
LR	Location Registration
LS	Latest Start Time
LSA	Link State Advertisement
LSAck	Low Speed Data
LSD	Low Speed Data
LSDB	Link State Database
LSP	Label Switch Path
LSPDU	Link State Protocol Data Unit
LSPM	Label Switch Path Management
LSR	Label Switch Router
LSU	Link State Update
MAC	Media Access Control
MAN	Metropolitan Area Network
MAP	Mobile Application Part
MBGP	Multiprotocol Border Gateway Protocol
MFC	Metalized Film Capacitor
MIB	Management Information Base
MM	Market Management (process)
MMC	Meet-Me Conference
MODEM	MODulator-DEMulator
MP	Multilink PPP
MPLS	Multiprotocol Label Switching
MPLSFW	Multi-protocol Label Switch Forward
MPM	Manufacturing Project Manager
MSDP	Multicast Source Discovery Protocol
MSOH	Multiplex Section Overhead
MST	Multiplex Section Termination
MSTI	Multi-Spanning Tree Instance
MSTP	Multi-Service Transmission Platform
MTBF	Mean Time Between Failure
MTU	Maximum Transmission Unit
NAM	National Area Message
NAPT	
NAS	Narrowband Access Server
NBMA	Non Broadcast Multi-Access
NET	NET Card
NetBIOS	Network Basic Input/Output System
NHLFE	Next Hop Label Forwarding Entry
NIC	Network Information Center
NLRI	Network Layer Reachability Information

NMS	Network Management Station
NPDU	Network Protocol Data Unit
NPE	Network Facing PE
NSAP	Network Service Access Point
NSM	Neighbour State Machine
NTP	Network Time Protocol
OAM	Operation Administration and Maintenance
OC-3	OC-3
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PAT	Pointing Acquisition Tracking
PCM	percentage of completion method
PD	Powered Device
PDU	Protocol Data Unit
PE	Provider Edge Router
PHP	Penultimate Hop Popping
PHY	Physical layer
PIM	Power Inspection Module
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PoE	Power Over Ethernet
POH	Path Overhead
Point-to-Point	Point-to-Point
PPP	Point-to-Point Protocol
PPTP	Point to Point Tunneling Protocol
PSE	Packet Switching Exchange
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Channel
PW	Pseudowire
QACL	QoS/ACL
QoS	Quality of Service
RADIUS	Remote Authentication Dial in User Service
RD	Router Distinguisher
RFC	Request For Change
RIP	Routing Information Protocol
RM	Remote Manager
RMON	Remote Monitoring
RP	Response Path
RPC	Raman Pump Amplifier Unit For C-band
RPF	Reverse Path Forwarding
RRP	Resilient Packet Ring
RS	Regenerator Section
RSA	Remote RSA Interface Board

RSOH	Regenerator Section Overhead
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource ReserVation Protocol
RT	rate
RTD	Radio Test Device
SA	Solution Architecture
SAFI	Subsequent Address Family Identifier
SBM	SGSN Basic Module
SDH	Synchronous Digital Hierarchy
SEL	Clock Selection Control Board
SET	Secure Electronic Transaction
SF	Sampling Frequency
SITE	site
SNMP	Simple Network Management Protocol
SOH	Section Overhead
SONET	Synchronous Optical NETwork
SP	Service Provider
SPE	4Ð6STM-1 Electrical Process Board
SPT	Special Tone Board
SS	Scheduled Start Date or Start-to-Start
SSH	Secure Shell
SSL	Secure Socket(s) Layer
SSM	Spread Spectrum Modulation
ST	Segment Type
STM-1	SDH Transport Module -1
STP	Shielded Twisted Pair
SYSTEM	System Manage veneer
TAC	Terminal Access Controller
TACACS	Terminal Access Controller Access Control System
TC	Target Completion Date
TCI	Terminal Interface Board
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOS	Type of Service
TPID	Tag Protocol Identifier
TU	Test Unit
TUG	Tributary Unit Group
UDP	User Datagram Protocol
UP	Unique Number
UPE	User Facing PE
URL	Uniform Resource Locators
VC	Video Codec
VCI	Virtual Channel Identifier

VDSL	Very High Speed DSL; Very High Rate DSL
VFS	Virtual File System
VLAN	Virtual LAN
VLL	Virtual Leased Lines
VOS	Virtual Operate System
VPDN	Virtual Private Data Network
VPI	Virtual Path Identifier
VPLS	Virtual Private Local Switch
VPN	Virtual Private Network
Comware	Versatile Routing Platform
VSI	Virtual Switch Interface
WAN	Wide Area Network
WINS	Windows Internet Naming Service
WRR	Weighted Round Robin
WWW	World Wide Web