H3C S3600 Series Ethernet Switches

Operation Manual

Hangzhou H3C Technologies Co., Ltd.

http://www.h3c.com

Manual Version: T2-08163G-20070724-C-1.04

Product Version: Release 1510

Copyright © 2006-2007, Hangzhou H3C Technologies Co., Ltd. and its licensors

All Rights Reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Hangzhou H3C Technologies Co., Ltd.

Trademarks

H3C, H3C, Aolynk, Aolynk, H^{3}Care, H3care, TOP G, TOPG, IRF, NetPilot, Neocean, NeoVTL, SecPro, SecPoint, SecEngine, SecPath, Comware, Secware, Storware, NQA, VVG, V^{2}G, V^{n}G, PSPT, XGbus, N-Bus, TiGem, InnoVision and HUASAN are trademarks of Hangzhou H3C Technologies Co., Ltd.

All other trademarks that may be mentioned in this manual are the property of their respective owners.

Notice

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

To obtain the latest information, please access:

http://www. h3c.com

Technical Support

customer_service@h3c.com

http://www. h3c.com

About This Manual

Related Documentation

In addition to this manual, each H3C S3600 Series Ethernet Switches-Release 1510 documentation set includes the following:

Manual	Description
H3C S3600 Series Ethernet Switches Command Manual-Release 1510	It is used for assisting the users in using various commands.
H3C S3600 Series Ethernet Switches Installation Manual	It provides information for the system installation.

Organization

H3C S3600 Series Ethernet Switches Operation Manual-Release 1510 is organized as follows:

Part	Contents
0 Product Overview	Introduces the characteristics and implementations of the Ethernet switch.
1 CLI	Introduces the command hierarchy, command view and CLI features of the Ethernet switch.
2 Login	Introduces the ways to log into an Ethernet switch.
3 Configuration File Management	Introduces the ways to manage configuration files.
4 VLAN	Introduces VLAN fundamental and the related configuration.
5 IP Address and Performance Configuration	Introduces IP address and IP performance fundamental and the related configuration.
6 Management VLAN	Introduces the management VLAN configuration.
7 Voice VLAN	Introduces voice VLAN fundamental and the related configuration.
8 GVRP	Introduces GVRP and the related configuration.

Part	Contents
9 Port Basic Configuration	Introduces basic port configuration.
10 Link Aggregation	Introduces link aggregation and the related configuration.
11 Port Isolation	Introduces port isolation and the related configuration.
12 Port Security-Port Binding	Introduces port security, port binding, and the related configuration.
13 DLDP	Introduces DLDP and the related configuration.
14 MAC Address Table	Introduces MAC address forwarding table and the related configuration.
15 Auto Detect	Introduces auto detect and the related configuration.
16 MSTP	Introduces STP and the related configuration.
17 Routing Protocol	Introduces the routing protocol-related configurations, including static route configuration, RIP configuration, OSPF configuration, IS-IS configuration, BGP configuration, and routing policy configuration.
18 Multicast	Introduces the configuration of GMRP, IGMP Snooping, IGMP, PIM-DM, PIM-SM, and MSDP.
19 802.1x	Introduces 802.1x and the related configuration.
20 AAA-RADIUS-HWTACACS-EAD	Introduces AAA, RADIUS, HWTACACS, EAD, and the related configurations.
21 VRRP	Introduces VRRP and the related configuration.
22 Centralized MAC Address Authentication	Introduces centralized MAC address authentication and the related configuration.
23 ARP	Introduces ARP and the related configuration.
24 DHCP	Introduces DHCP server, DHCP relay, DHCP-Snooping, and the related configurations.
25 ACL	Introduces ACL and the related configuration.
26 QoS-QoS Profile	Introduces QoS, QoS profile and the related configuration.

Part	Contents
27 Web Cache Redirection	Introduces Web cache redirection and the related configuration.
28 Mirroring	Introduces port mirroring and the related configuration.
29 IRF Fabric	Introduces IRF fabric-related configuration.
30 Cluster	Introduces the configuration to form clusters using HGMP V2.
31 PoE-PoE Profile	Introduces PoE, PoE profile and the related configuration.
32 UDP Helper	Introduces UDP Helper and the related configuration.
33 SNMP-RMON	Introduces the configuration to manage network devices through SNMP and RMON.
34 NTP	Introduces NTP and the related configuration.
35 SSH Terminal Service	Introduces SSH2.0 and the related configuration.
36 File System Management	Introduces basic configuration for file system management.
37 FTP and TFTP	Introduces basic configuration for FTP and TFTP, and the applications.
38 Information Center	Introduces the configuration to analyze and diagnose networks using the information center.
39 System Maintenance and Debugging	Introduces daily system maintenance and debugging.
40 VLAN-VPN	Introduces VLAN VPN and the related configuration.
41 HWPing	Introduces HWPing and the related configuration.
42 DNS	Introduces DNS and the related configuration.
43 Access Management	Introduces Access Management and the related configuration.
44 Appendix	Lists the acronyms used in this manual.

Conventions

The manual uses the following conventions:

I. Command conventions

Convention	Description
Boldface	The keywords of a command line are in **Boldface**.
italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. Many or none can be selected.
#	A line starting with the # sign is comments.

II. GUI conventions

Convention	Description
< >	Button names are inside angle brackets. For example, click <OK>.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

III. Symbols

Convention	Description
 Warning	Means reader be extremely careful. Improper operation may cause bodily injury.
 Caution	Means reader be careful. Improper operation may cause data loss or damage to equipment.
🕮 Note	Means a complementary description.

Table of Contents

Chapter 1 Obtaining the Documentation 1-1
1.1 CD-ROM 1-1
1.2 H3C Website 1-1
1.3 Software Release Notes 1-2
Chapter 2 Product Overview 2-1
2.1 Preface 2-1
2.2 Switch Models 2-1
2.3 Software Features 2-2
Chapter 3 Networking Applications 3-1
3.1 Broadband Ethernet Access for Residential Communities 3-1
3.2 Application for Connecting Branches or Small- to Medium-Sized Enterprises 3-1
3.3 Application in Large Enterprise and Campus Networks 3-2

Chapter 1 Obtaining the Documentation

H3C Technologies Co., Ltd. provides various ways for you to obtain documentation, through which you can obtain the product documentations and those concerning newly added new features. The documentations are available in one of the following ways:

- CD-ROMs shipped with the devices
- H3C website
- Software release notes

1.1 CD-ROM

H3C delivers a CD-ROM together with each device. The CD-ROM contains a complete product document set, including the operation manual, command manual, installation manual, and compatibility manual. After installing the reader program provided by the CD-ROM, you can search for the desired contents in a convenient way through the reader interface.

The contents in the manual are subject to update on an irregular basis due to product version upgrade or some other reasons. Therefore, the contents in the CD-ROM may not be the latest version. This manual serves the purpose of user guide only. Unless otherwise noted, all the information in the document set does not claim or imply any warranty. For the latest software documentation, go to the H3C website.

1.2 H3C Website

Perform the following steps to query and download the product documentation from the H3C website.

Table 1-1 Acquire product documentation from the H3C website

How to apply for an account	Access the homepage of H3C at http:// www.h3c.com and click on Registration at the top right. In the displayed page, provide your information and click on Submit to register.
How to get documentation	Approach 1: In the homepage of H3C at http:// www.h3c.com, select Technical Support & Document > Technical Documents from the navigation menu at the top. Then select a product for its documents. Approach 2: In the homepage of H3C at http:// www.h3c.com, select Support > Technical Documents. Then select a product for its documents.

1.3 Software Release Notes

With software upgrade, new software features may be added. You can acquire the information about the newly added software features through software release notes.

Chapter 2 Product Overview

2.1 Preface

H3C S3600 Series Ethernet switches are Ethernet equipment capable of multilayer switching. They come in two series: S3600-SI and S3600-EI. In addition to the basic service features, S3600 Series Ethernet switches support abundant Layer 3 features and enhanced extended functions.

- S3600-SI series switches support basic routing functions, DHCP, basic IRF functions and IGMP-Snooping.
- S3600-EI series switches support advanced routing functions, DHCP, enhanced IRF functions, and enhanced multicast functions (including PIM-DM and PIM-SM).

2.2 Switch Models

Table 2-1 lists the S3600 series Ethernet Switches models.

Table 2-1 Models in the S3600 series

Model	Power supply unit (PSU)	Number of service ports	Number of 100 Mbps ports	Number of 1,000 Mbps uplink ports	Console port
H3C S3600-28P-SI	AC-input	28	24 10/100 Mbps ports(electrical)	4 Gigabit (SFP) ports	1
H3C S3600-28P-PWR-SI	AC-/DC-input	28	24 10/100 Mbps ports(electrical)	4 Gigabit (SFP) ports	1
H3C S3600-28TP-SI	AC-input	28	24 10/100 Mbps (electrical)	2 Gigabit (SFP) ports 2 10/100/1,000 Mbps ports (electrical)	1
H3C S3600-52P-SI	AC-input	52	48 10/100 Mbps (electrical)	4 Gigabit (SFP) ports	1
H3C S3600-28P-EI	AC-/DC-input	28	24 10/100 Mbps ports (electrical)	4 Gigabit (SFP) ports	1

Model	Power supply unit (PSU)	Number of service ports	Number of 100 Mbps ports	Number of 1,000 Mbps uplink ports	Console port
H3C S3600-28F-EI	AC-/DC-input	28	24 100 Mbps (SFP) ports	2 Gigabit (SFP) ports 2 10/100/1,000 Mbps ports (electrical)	1
H3C S3600-28P-PWR-EI	AC-/DC-input	28	24 10/100 Mbps ports (electrical)	4 Gigabit (SFP) ports	1
H3C S3600-52P-EI	AC-/DC-input	52	48 10/100 Mbps ports (electrical)	4 Gigabit ports (SFP)	1
H3C S3600-52P-PWR-EI	AC-/DC-input	52	48 10/100 Mbps ports (electrical)	4 Gigabit (SFP) ports	1
H3C S3600-52P-PWR-SI	AC-/DC-input	52	48 10/100 Mbps ports (electrical)	4 Gigabit (SFP) ports	1

2.3 Software Features

S3600 Series Ethernet Switches have abundant software features and can meet the requirements of different applications. Table 2-2 summarizes the features provided by each module.

Table 2-2 Service features of the S3600 series

Part	Features
1 CLI	• CLI • Hierarchically grouped commands • CLI online help
2 Login	• Logging into a switch through the Console port • Logging into a switch through an Ethernet port by using Telnet or SSH • Logging into a switch through the Console port by using modem • Logging into a switch through Web or NMS
3 Configuration File Management	• Saving, restoring, and deleting the configuration file
4 VLAN	• IEEE 802.1Q-compliant VLAN • Port-based VLAN • Protocol-based VLAN

Part	Features
5 IP Address and Performance Configuration	• Configuring an IP address for a switch • Configuring the TCP attributes for a switch
6 Management VLAN	• Management VLAN configuration • Management VLAN interface configuration
7 Voice VLAN	• Voice VLAN
8 GVRP	• GARP VLAN registration protocol (GVRP)
9 Port Basic Configuration	• Three port states supported: Access, Trunk, and Hybrid • Setting broadcast storm suppression globally • Loopback detection supported • Cable test
10 Link Aggregation	• Link aggregation control protocol (LACP)
11 Port Isolation	• Port isolation group
12 Port Security-Port Binding	• Multiple security modes • MAC address-to-port binding
13 DLDP	• Device link detection protocol (DLDP)
14 MAC Address Table	• Manually configuring dynamic, static, and black hole MAC addresses • Configuring the aging time for MAC addresses • MAC address learning limit
15 Auto Detect	• Auto detect • Auto detect applications in static routing, VRRP, and VLAN interface backup
16 MSTP	• STP/RSTP/MSTP • VLAN-VPN TUNNEL • H3C-proprietary MSTP path cost standard
17 Routing Protocols.	• Static route • Routing information protocol (RIP) v1/v2 • Open shortest path first (OSPF) (S3600-EI series switches only) • Routing policy
18 Multicast	• Internet group management protocol snooping (IGMP Snooping) • Internet group management protocol (IGMP) (S3600-EI series switches only) • Protocol-independent multicast-dense mode (PIM-DM) (S3600-EI series switches only) • Protocol-independent multicast-sparse mode (PIM-SM) (S3600-EI series switches only)
19 802.1x	• 802.1X authentication • Guest VLAN • Huawei authentication bypass protocol (HABP)

Part	Features
20 AAA-RADIUS-HWTACACS-EAD	• Authentication, authorization, and accounting (AAA) • Remote authentication dial-In user service (RADIUS) • Huawei terminal access controller access control system (HWTACACS) • Endpoint admission defense (EAD)
21 VRRP	• Virtual router redundancy protocol (VRRP) (S3600-EI series switches only)
22 Centralized MAC Address Authentication	• Centralized MAC address authentication
23 ARP	• Gratuitous ARP • Manually configuring ARP entries
24 DHCP	• DHCP server (S3600-EI series switches only) • DHCP relay • DHCP Snooping • DHCP accounting • Using Option184 in DHCP server (S3600-EI series switches only) • Using Option82 in DHCP relay
25 ACL	• Basic ACLs • Advanced ACLs • Layer 2 ACLs • User-defined ACLs
26 QoS-QoS Profile	• Quality of Service (QoS) • QoS profile
27 Web Cache Redirection	• (Supported by S3600-EI series only)
28 Mirroring	• Traffic mirroring • Port mirroring • Remote port mirroring (S3600-EI series switches only)
29 IRF Fabric	• IRF Fabric • Stack port optional • Peer end detection for stack ports
30 Cluster	• Huawei group management protocol (HGMP) v2 • Neighbor discovery protocol (NDP) • Neighbor topology discovery protocol (NTDP)
31 PoE-PoE Profile	• Power over Ethernet (PoE) • PoE profile
32 UDP Helper	• Forwarding UDP broadcast packets by using UDP Helper
33 SNMP-RMON	• Simple network management protocol (SNMP) v3, compatible with SNMP v1/v2 • Remote monitoring (RMON)
34 NTP	• Network time protocol (NTP)

Part	Features
35 SSH Terminal Service	• Secure shell (SSH) • Secure FTP (SFTP)
36 File System Management	• File system management • Configuration file backup and restoration • FTP/TFTP lighting
37 FTP and TFTP	• Operating as an FTP server/FTP client • Operating as a TFTP client
38 Information Center	• System logs • Hierarchical alarms • Debugging information output
39 System Maintenance and Debugging	• Configuring system time • Language (Chinese/English) selecting • Displaying and configuring system device state
40 VLAN-VPN	• VLAN VPN (QinQ) • Configuring VLAN VPN interior-layer priority replication • Configuring TPID value
41 HWPing	• HWPing
42 DNS	• Domain Name System (DNS)
43 Access Management	• Configuring the access IP address pool based on the physical port

Chapter 3 Networking Applications

You can deploy S3600 series on many types of networks, such as enterprise networks and broadband access networks. Following are several typical networking applications.

3.1 Broadband Ethernet Access for Residential Communities

On the broadband access network of a residential community, an S3600 series switch is located in the center. It is downlinked to S2000 or S3026 series switches to reach the Ethernet users and uplinked to a core Layer 3 switch through a GE extension module to connect to the MAN backbone.

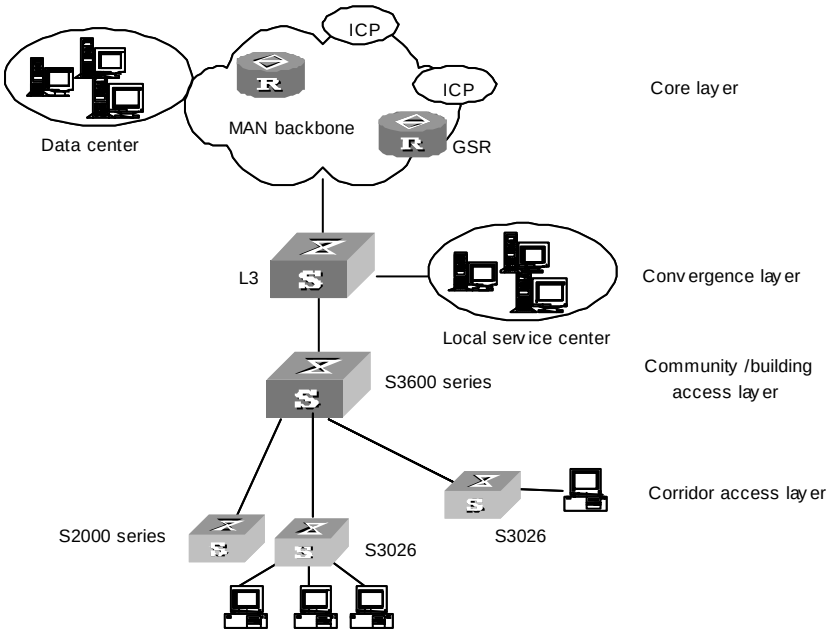


Figure 3-1 Network diagram for connecting community Ethernet to MAN using S3600 series Ethernet switches

3.2 Application for Connecting Branches or Small- to Medium-Sized Enterprises

For small-to medium-sized enterprises or branches of a large enterprise, S3600 series switches can server as the backbone switches on their networks and can be connected to the headquarters or other branches through routers. As the enterprise size increases, the network also can expand by subtending the S3600 series.

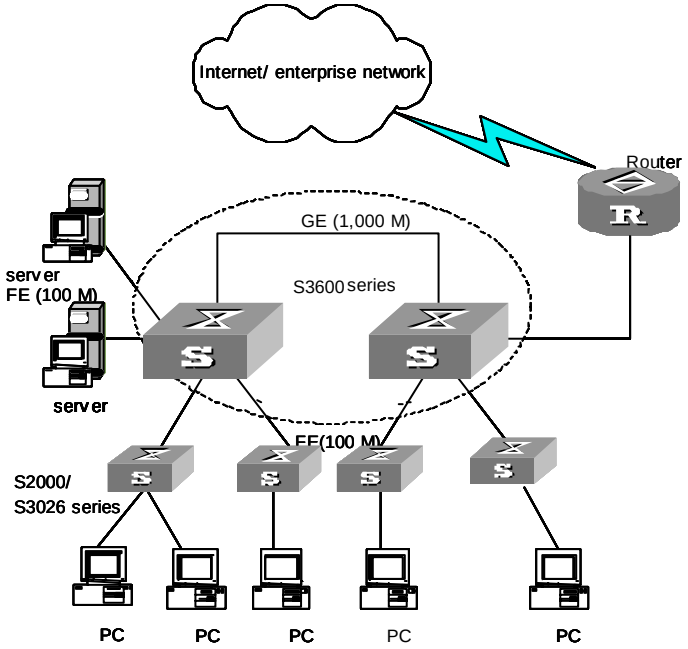


Figure 3-2 S3600 series switches application in branch network of midsize/large enterprise

3.3 Application in Large Enterprise and Campus Networks

In a large enterprise or campus network, the S3600 series switches can operate on the convergence layer. They are downlinked to layer 2 switches, S3000 Series for example; and uplinked to a layer 3 switch through GE expansion modules. These switches together provide a network-wide intranet solution that covers Gigabit-to-backbone and 100 Mbps-to-desktop.

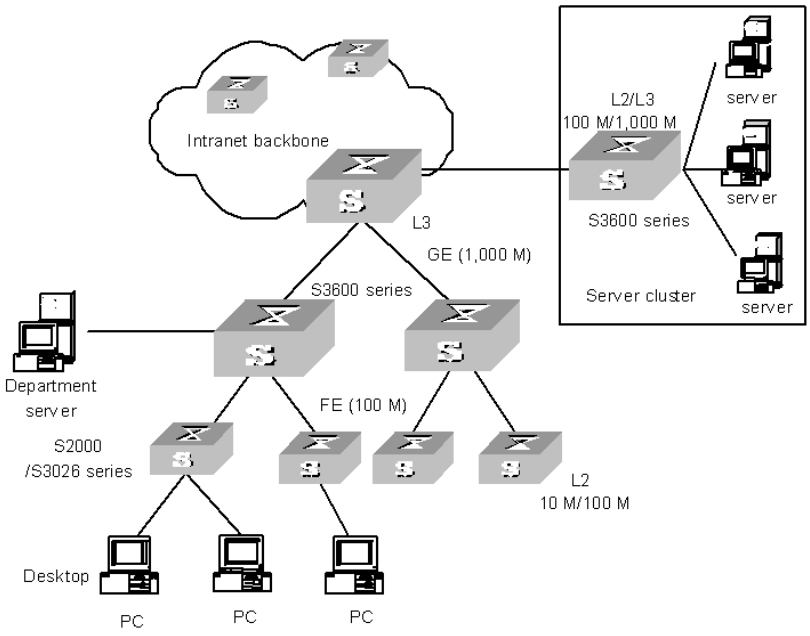


Figure 3-3 S3600 series application in large enterprise and campus network

Table of Contents

Chapter 1 CLI Configuration 1-1
1.1 Introduction to the CLI 1-1
1.2 Command Level/Command View 1-1
1.2.1 Switching between User Levels 1-2
1.2.2 Configuring a Level for a Specific Command in a Specific View 1-3
1.2.3 CLI Views 1-3
1.3 CLI Features 1-9
1.3.1 Online Help 1-9
1.3.2 Terminal Display 1-10
1.3.3 History Commands 1-10
1.3.4 Error Messages 1-11
1.3.5 Command Edit 1-12

Chapter 1 CLI Configuration

1.1 Introduction to the CLI

S3600 series Ethernet switches provide a command line interface (CLI) and commands for you to configure and manage your switches. The CLI is featured by the following:

- Commands are grouped by level. This prevents unauthorized users from configuring switches with relevant commands.
- You can gain online help at any time by entering a question mark "?".
- Common diagnostic utilities (such as Tracert and Ping) are available.
- A variety of debugging information is available.
- A function similar to Doskey is provided for you to execute a history command.
- You can execute a command by entering part of the command in the CLI as long as the keywords you enter do not conflict those of other commands.

1.2 Command Level/Command View

To prevent unauthorized accesses, commands are grouped by level.

Commands fall into four levels: visit, monitor, system, and manage.

- Visit level: Commands at this level are mainly used to diagnose network and switch the language mode on the user interface, and they cannot be saved in configuration files. Such commands include **ping**, **tracert**, and **language-mode**.
- Monitor level: Commands at this level are mainly used to maintain the system and diagnose service faults, and they cannot be saved in configuration files. Such commands include **display** and **debugging**.
- System level: Commands at this level are mainly used to configure services. Commands concerning routing and network layers are at this level. These commands can be used to provide network services directly.
- Manage level: Commands at this level are associated with the basic operation modules and support modules of the system. These commands provide supports for services. Commands concerning file system, FTP/TFTP/XModem downloading, user management, and level setting are at this level.

Users logging in to a switch also fall into four levels, which respectively correspond to the command levels. Users at a specific level can only use the commands at the same level or lower levels.

1.2.1 Switching between User Levels

You can switch from one user level to another by executing a related command and set a password for the switching as required after logging in to a switch.

I. Setting a password for user level switching

Table 1-1 lists the operations to set a password for user level switching.

Table 1-1 Set a password for user level switching

Operation	Command	Description
Enter system view	**system-view**	—
Set a password for switching from a lower user level to the user level specified by the *level* argument	**super password** [**level** *level*] { **simple** | **cipher** } *password*	Optional A password is necessary only when a user switches from a lower user level to a higher user level.

II. Switching between user levels

Table 1-2 lists the operation to switch between user levels.

Table 1-2 Switch between user levels

Operation	Command	Description
Switch from the current user level to the user level specified by the *level* argument	**super** [*level*]	Required Execute this command in user view. If you have set a password for user level switching by using the **super password** command and you want to switch from a lower user level to a higher user level, you need to enter the correct password. Otherwise, you will remain at the original user level.

Note:

- By default, you switch from the current user level to level 3.
- For the purpose of security, you cannot see the password you enter on the screen. You will remain at the original user level if you fail to enter the correct password after you have tried more than three times.

1.2.2 Configuring a Level for a Specific Command in a Specific View

You can configure a level for a specific command in a specific view. Commands fall into four levels: visit, monitor, system, and manage, which are identified as 0, 1, 2, and 3 respectively. The administrator can change the command level according to the requirements..

Table 1-3 lists the operations to configure a level for a specific command.

Table 1-3 Configure a level for a specific command in a specific view

Operation	Command	Description
Enter system view	**system-view**	—
Configure a level for a specific command in a specific view	**command-privilege level** *level* **view** *view command*	Required It is forbidden to change the command level at will. Doing so may bring inconvenience to maintenance and operation.

1.2.3 CLI Views

CLI views are designed for different configuration tasks. They are related but distinguished. You will enter user view once you log in to a switch successfully, where you can view operation status and statistics information. After executing the **system-view** command, you can enter system view, where you can go into other views by entering corresponding commands.

The following CLI views are provided:

- User view
- System view
- Ethernet interface view
- VLAN view
- VLAN interface view
- Loopback interface view
- Local user view
- User interface view
- FTP client view
- SFTP client view
- MST region view
- Cluster view
- Public key view
- Public key code view
- DHCP address pool view
- PIM view

- RIP view
- OSPF view
- OSPF area view
- Routing policy view
- Basic ACL view
- Advanced ACL view
- Layer 2 ACL view
- User-defined ACL view
- QoS profile view
- RADIUS scheme view
- ISP domain view
- HWPing view
- HWTACACS view
- MSDP view
- PoE profile view

Table 1-4 lists operations you can perform in these CLI views and details about commands used to enter these CLI views.

Table 1-4 Operations in CLI views

View	Available operation	Prompt	Enter method	Quit method
User view	Display operation status and statistical information	<H3C>	Enter user view once logging in to the switch.	Execute the **quit** command in user view to log out of the switch.
System view	Configure system parameters	[H3C]	Execute the **system-view** command in user view.	Execute the **quit** or **return** command to return to user view.
Ethernet interface view	Configure Ethernet interface parameters	[H3C-Ethernet1/0/1]	100M Ethernet interface view Execute the **interface ethernet** 1/0/1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
		[H3C-GigabitEthernet1/1/1]	Gigabit Ethernet interface view Execute the **interface gigabitethernet** 1/1/1 command in system view.	

View	Available operation	Prompt	Enter method	Quit method
VLAN view	Configure VLAN parameters	[H3C-vlan1]	Execute the **vlan** 1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
VLAN interface view	Configure IP interface parameters for VLANs and aggregated VLANs	[H3C-Vlan-interface1]	Execute the **interface vlan-interface** 1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Loopback interface view	Configure loopback interface parameters	[H3C-LoopBack0]	Execute the **interface loopback** 0 command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Local user view	Configure local user parameters	[H3C-luser-user1]	Execute the **local-user** user1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
User interface view	Configure user interface parameters	[H3C-ui0]	Execute the **user-interface** 0 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
FTP client view	Configure FTP client parameters	[ftp]	Execute the **ftp** command in user view.	Execute the **quit** command to return to user view.
SFTP client view	Configure SFTP client parameters	sftp-client>	Execute the **sftp** 10.1.1.1 command in system view.	Execute the **quit** command to return to user view.
MST region view	Configure MST region parameters	[H3C-mst-region]	Execute the **stp region-configuration** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.

View	Available operation	Prompt	Enter method	Quit method
Cluster view	Configure cluster parameters	[H3C-cluster]	Execute the **cluster** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Public key view	Configure RSA public keys for SSH users	[H3C-rsa-public-key]	Execute the **rsa peer-public-key** a003 command in system view.	Execute the **peer-public-key end** command to return to system view.
Public key code view	Edit RSA public key for SSH users	[H3C-rsa-key-code]	Execute the **public-key-code begin** command in public key code view	Execute the **public-key-code end** command to return to public key view
DHCP address pool view	Configure DHCP address pool parameters	[H3C-dhcp-pool-a123]	Execute the **dhcp server ip-pool** a123 command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
PIM view	Configure PIM parameters	[H3C-pim]	Execute the **pim** command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
RIP view	Configure RIP parameters	[H3C-rip]	Execute the **rip** command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
OSPF view	Configure OSPF protocol parameters	[H3C-ospf-1]	Execute the **ospf** command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.

View	Available operation	Prompt	Enter method	Quit method
OSPF area view	Configure OSPF area parameters	[H3C-ospf-1-area-0.0.0.1]	Execute the **area** 1 command in OSPF view	Execute the **quit** command to return to OSPF view. Execute the **return** command to return to user view.
Routing policy view	Configure routing policies	[H3C-route-policy]	Execute the **route-policy** policy1 **permit node** 10 command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Basic ACL view	Define sub-rules for a basic ACL (with ID ranging from 2000 to 2999)	[H3C-acl-basic-2000]	Execute the **acl number** 2000 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Advanced ACL view	Define sub-rules for an advanced ACL (with ID ranging from 3000 to 3999)	[H3C-acl-adv-3000]	Execute the **acl number** 3000 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Layer 2 ACL view	Define sub-rules for an layer 2 ACL (with ID ranging from 4000 to 4999)	[H3C-acl-ethernetframe-4000]	Execute the **acl number** 4000 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
User-defined ACL view	Define sub-rules for a user-defined ACL (with ID ranging from 5000 to 5999)	[H3C-acl-user-5000]	Execute the **acl number** 5000 command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
QoS profile view	Define QoS profile	[H3C-qos-profile-a123]	Execute the **qos-profile** a123 command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.

View	Available operation	Prompt	Enter method	Quit method
RADIUS scheme view	Configure RADIUS parameters	[H3C-radius-1]	Execute the **radius scheme** 1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
ISP domain view	Configure ISP domain parameters	[H3C-isp-aaa163.net]	Execute the **domain** aaa163.net command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
HWPing view	Configure HWPing parameters	[H3C-hwping-a123-a123]	Execute the **hwping** a123 a123 command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
HWTACACS view	Configure HWTACACS parameters	[H3C-hwtacacs-a123]	Execute the **hwtacacs scheme** a123 command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
MSDP view	Configure MSDP parameters	[H3C-msdp]	Execute the **msdp** command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
PoE profile view	Configure PoE profile parameters	[H3C-poe-profile-a123]	Execute the **poe-profile** a123 command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.

Note:

The <Ctrl + Z> keys function as the **return** command does.

1.3 CLI Features

1.3.1 Online Help

CLI provides two types of online help: complete online help and partial online help. You can obtain help information necessary for the switch configuration.

I. Complete online help

Enter a "?" character in any view on your terminal to display all the commands available in the view and their brief descriptions. The following takes user view as an example.

```
<H3C> ?
User view commands:
  backup          Backup current configuration
  boot            Set boot option
  cd              Change current directory
  clock           Specify the system clock
  cluster         Run cluster command
  copy            Copy from one file to another
  debugging       Enable system debugging functions
  delete          Delete a file
  dir             List files on a file system
  display         Display current system information
  <omitted>
```

Enter a command, a space, and a "?" character. If a keyword is in the “?” position of the command, all available keywords and their brief descriptions will be displayed on your terminal. The following takes the **clock** command as an example.

```
<H3C> clock ?
  datetime     Specify the time and date
  summer-time  Configure summer time
  timezone     Configure time zone
```

Enter a command, a space, and a "?" character. If an argument is in the “?” position of the command, all available arguments and their brief descriptions will be displayed on your terminal. The following takes the **interface vlan** command as an example.

```
[H3C] interface vlan-interface ?
  <1-4094>  VLAN interface number
[H3C] interface vlan-interface 1 ?
 <cr>
```

The <cr> string means that no argument is available in the “?” position. You can directly execute the command by pressing <Enter>.

II. Partial online help

Enter a character string followed by a "?" character on your terminal to display all the commands beginning with the string. For example:

```
<H3C> pi?
ping
```

Enter a command, a space, and a character string followed by a "?" character on your terminal to display all the keywords that belong to the command and begin with the string (if available). For example:

```
<H3C> display ver?
  version
```

Enter the first several characters of a keyword in a command and then press <Tab>, the complete keyword will be displayed on the terminal screen if the input characters uniquely identify a keyword; all the keywords that match the input characters will be displayed on the terminal screen if the input characters match more than one keyword.

You can use the **language-mode** command to display the help information in English.

1.3.2 Terminal Display

CLI provides the following display features:

- The prompt information and help information can be displayed in Chinese or English.
- Display suspension. That is, the display of output information can be paused when the screen is full and you can then perform one of the three operations listed in Table 1-5 as needed.

Table 1-5 Display-related operations

Operation	Function
Press <Ctrl+C>	Suspend the display and execution of a command.
Press the space key	Scroll the output information up by one page.
Press <Enter>	Scroll the output information up by one line.

1.3.3 History Commands

The CLI provides a function similar to Doskey to store the history commands automatically. You can recall and execute these history commands at any time. By default, the CLI can store 10 history commands for each user. Table 1-6 lists history command-related operations.

Table 1-6 Access history commands

Operation	Operation	Description
Display history commands	Execute the **display history-command** command	This command displays valid history commands.
Recall the previous history command	Press the up-arrow key or <Ctrl+P>	This operation recalls the previous history command (if available).
Recall the next history command	Pressing the down-arrow key or <Ctrl+N>	This operation recalls the next history command (if available).

Note:

- The Up and Down arrow keys can be used to recall history commands only in terminals running on Windows 3.x or Telnet running on Windows 3.x. You can press <Ctrl + P> or <Ctrl + N> in terminals running on Windows 9x to achieve the same purpose.
- If you enter and execute the same command for multiple times, the command is buffered when it is entered for the first time.

1.3.4 Error Messages

If the command you enter passes the syntax check, it will be successfully executed; otherwise an error message will appear. Table 1-7 lists the common error messages.

Table 1-7 Common error messages

Error message	Description
Unrecognized command	The command does not exist.
	The keyword does not exist.
	The parameter type is wrong.
	The parameter value is out of range.
Incomplete command	The command entered is incomplete.
Too many parameters	You have entered too many parameters.
Ambiguous command	The parameters entered are ambiguous.
Wrong parameter found at '^' position.	The parameter at the '^' position is incorrect.

1.3.5 Command Edit

The CLI provides basic command edit functions and supports multi-line editing. The maximum number of characters a command can contain is 254. Table 1-8 lists the CLI edit operations.

Table 1-8 Edit operations

Press…	To…
Common key	Insert the character the key represents at the cursor and move the cursor one character to the right if the edit buffer is not full.
Backspace key	Delete the character on the left of the cursor and move the cursor one character to the left.
Left arrow key or <Ctrl+B>	Move the cursor one character to the left.
Right arrow key or <Ctrl+F>	Move the cursor one character to the right.
Up arrow key or <Ctrl+P> Down arrow key or <Ctrl+N>	Display history commands.
Tab key	Utilize the partial online help. That is, when you enter an incomplete keyword and press the Tab key, if the input keyword uniquely identifies an existing keyword, the system substitutes the complete key word for the incomplete keyword; if the input keyword matches more than one keyword, all the keywords are displayed on the terminal screen, with each keyword on a line; if the input arguments matches no keyword, the system displays your original input on a new line without any change.

Table of Contents

Chapter 1 Logging into an Ethernet Switch 1-1
1.1 Logging into an Ethernet Switch 1-1
1.2 Introduction to the User Interface 1-1
1.2.1 Supported User Interfaces 1-1
1.2.2 User Interface Number 1-1
1.2.3 Common User Interface Configuration 1-2

Chapter 2 Logging in through the Console Port 2-1
2.1 Introduction 2-1
2.2 Logging in through the Console Port 2-1
2.3 Console Port Login Configuration 2-3
2.3.1 Common Configuration 2-3
2.3.2 Console Port Login Configurations for Different Authentication Modes 2-4
2.4 Console Port Login Configuration with Authentication Mode Being None 2-6
2.4.1 Configuration Procedure 2-6
2.4.2 Configuration Example 2-7
2.5 Console Port Login Configuration with Authentication Mode Being Password 2-9
2.5.1 Configuration Procedure 2-9
2.5.2 Configuration Example 2-11
2.6 Console Port Login Configuration with Authentication Mode Being Scheme 2-12
2.6.1 Configuration Procedure 2-12
2.6.2 Configuration Example 2-15

Chapter 3 Logging in through Telnet 3-1
3.1 Introduction 3-1
3.1.1 Common Configuration 3-1
3.1.2 Telnet Configurations for Different Authentication Modes 3-2
3.2 Telnet Configuration with Authentication Mode Being None 3-4
3.2.1 Configuration Procedure 3-4
3.2.2 Configuration Example 3-5
3.3 Telnet Configuration with Authentication Mode Being Password 3-7
3.3.1 Configuration Procedure 3-7
3.3.2 Configuration Example 3-8
3.4 Telnet Configuration with Authentication Mode Being Scheme 3-10
3.4.1 Configuration Procedure 3-10
3.4.2 Configuration Example 3-13
3.5 Telneting to a Switch 3-15
3.5.1 Telneting to a Switch from a Terminal 3-15
3.5.2 Telneting to another Switch from the Current Switch 3-17

Chapter 4 Logging in Using Modem 4-1
4.1 Introduction 4-1
4.2 Configuration on the Administrator Side 4-1
4.3 Configuration on the Switch Side 4-1
4.3.1 Modem Configuration 4-1
4.3.2 Switch Configuration 4-2
4.4 Modem Connection Establishment 4-3

Chapter 5 Logging in through Web-based Network Management System 5-1
5.1 Introduction 5-1
5.2 HTTP Connection Establishment 5-1
5.3 Web Server Shutdown/Startup 5-2

Chapter 6 Logging in through NMS 6-1
6.1 Introduction 6-1
6.2 Connection Establishment Using NMS 6-1

Chapter 7 Configuring Source IP Address for Telnet Service Packets 7-1
7.1 Configuring Source IP Address for Telnet Service Packets 7-1
7.2 Displaying Source IP Address Configuration 7-2

Chapter 8 User Control 8-1
8.1 Introduction 8-1
8.2 Controlling Telnet Users 8-1
8.2.1 Prerequisites 8-1
8.2.2 Controlling Telnet Users by Source IP Addresses 8-1
8.2.3 Controlling Telnet Users by Source and Destination IP Addresses 8-2
8.2.4 Controlling Telnet Users by Source MAC Addresses 8-3
8.2.5 Configuration Example 8-4
8.3 Controlling Network Management Users by Source IP Addresses 8-5
8.3.1 Prerequisites 8-5
8.3.2 Controlling Network Management Users by Source IP Addresses 8-5
8.3.3 Configuration Example 8-7
8.4 Controlling Web Users by Source IP Address 8-7
8.4.1 Prerequisites 8-8
8.4.2 Controlling Web Users by Source IP Addresses 8-8
8.4.3 Disconnecting a Web User by Force 8-8
8.4.4 Configuration Example 8-8

Chapter 1 Logging into an Ethernet Switch

1.1 Logging into an Ethernet Switch

You can log into an S3600 Ethernet switch in one of the following ways:

- Logging in locally through the Console port
- Telneting locally or remotely to an Ethernet port
- Telneting to the Console port using a modem
- Logging into the Web-based network management system
- Logging in through NMS (network management station)

1.2 Introduction to the User Interface

1.2.1 Supported User Interfaces

S3600 series Ethernet switches support two types of user interfaces: AUX and VTY.

Table 1-1 Description on user interface

User interface	Applicable user	Port used	Description
AUX	Users logging in through the Console port	Console port	Each switch can accommodate one AUX user.
VTY	Telnet users and SSH users	Ethernet port	Each switch can accommodate up to five VTY users.

Note:

The AUX port and the Console port of a H3C series Ethernet switch are the same port. You will be in the AUX user interface if you log in through this port.

1.2.2 User Interface Number

Two kinds of user interface index exist: absolute user interface index and relative user interface index.

1) The absolute user interface indexes are as follows:

- AUX user interface: 0
- VTY user interfaces: Numbered after AUX user interfaces and increases in the step of 1

2) A relative user interface index can be obtained by appending a number to the identifier of a user interface type. It is generated by user interface type. The relative user interface indexes are as follows:

- AUX user interface: AUX 0
- VTY user interfaces: VTY 0, VTY 1, VTY 2, and so on.

1.2.3 Common User Interface Configuration

Table 1-2 Common user interface configuration

Operation	Command	Description
Lock the current user interface	**lock**	Optional Execute this command in user view. A user interface is not locked by default.
Specify to send messages to all user interfaces/a specified user interface	**send** { **all** | *number* | *type number* }	Optional Execute this command in user view.
Disconnect a specified user interface	**free user-interface** [*type*] *number*	Optional Execute this command in user view.
Enter system view	**system-view**	—
Set the banner	**header** [**incoming** | **login** | **shell**] *text*	Optional
Set a system name for the switch	**sysname** *string*	Optional The system name defaults to “H3C”.
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	—
Set the command that is automatically executed when a user logs into the user interface	**auto-execute command** *text*	Optional By default, no command is automatically executed when a user logs into a user interface.

Operation	Command	Description
Display the information about the current user interface/all user interfaces	**display users** [**all**]	Optional You can execute the **display** command in any view.
Display the physical attributes and configuration of the current/a specified user interface	**display user-interface** [*type number* | *number*]	
Display the information about the current web users	**display web users**	

Caution:

- The **auto-execute command** command may cause you unable to perform common configuration in the user interface, so use it with caution.
- Before executing the **auto-execute command** command and save your configuration, make sure you can log into the switch in other modes and cancel the configuration.

Chapter 2 Logging in through the Console Port

2.1 Introduction

To log in through the Console port is the most common way to log into a switch. It is also the prerequisite to configure other login methods. Normally, you can log into an S3600 Ethernet switch through its Console port.

To log into an Ethernet switch through its Console port, the communication configuration of the user terminal must be in accordance with that of the Console port.

Table 2-1 lists the default settings of a Console port.

Table 2-1 The default settings of a Console port

Setting	Default
Baud rate	9,600 bps
Flow control	None
Check mode (Parity)	None
Stop bits	1
Data bits	8

After logging into a switch, you can perform configuration for AUX users. Refer to section 2.3 “Console Port Login Configuration” for more.

2.2 Logging in through the Console Port

Following are the procedures to connect to a switch through the Console port.

1) Connect the serial port of your PC/terminal to the Console port of the switch, as shown in Figure 2-1.

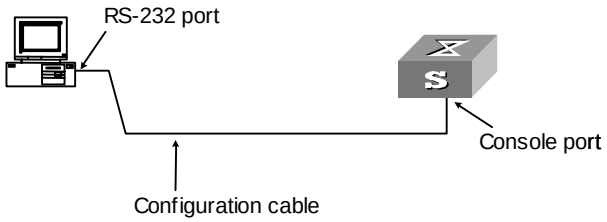


Figure 2-1 Diagram for setting the connection to the Console port

2) If you use a PC to connect to the Console port, launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 9X) and perform

the configuration shown in Figure 2-2 through Figure 2-4 for the connection to be created. Normally, the parameters of a terminal are configured as those listed in Table 2-1. And the type of the terminal is set to VT100.

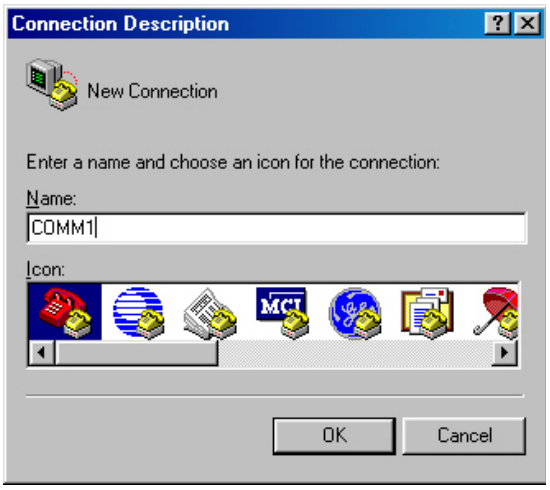


Figure 2-2 Create a connection



Figure 2-3 Specify the port used to establish the connection

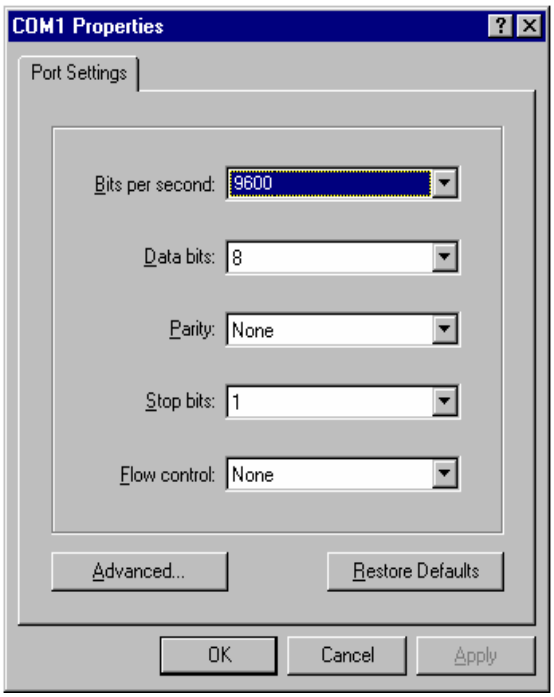


Figure 2-4 Set port parameters

3) Turn on the switch. You will be prompted to press the Enter key if the switch successfully completes POST (power-on self test). The prompt (such as <H3C>) appears after you press the Enter key.
4) You can then configure the switch or check the information about the switch by executing the corresponding commands. You can also acquire help by typing the ? character. The commands available on a switch are described in the command manuals.

2.3 Console Port Login Configuration

2.3.1 Common Configuration

Table 2-2 lists the common configuration of Console port login.

Table 2-2 Common configuration of Console port login

Configuration		Remarks
Console port configuration	Baud rate	Optional The default baud rate is 9,600 bps.
	Check mode	Optional By default, the check mode of the Console port is set to “none”, which means no check bit.
	Stop bits	Optional The default stop bits of a Console port is 1.
	Data bits	Optional The default data bits of a Console port is 8.
AUX user interface configuration	Configure the command level available to the users logging into the AUX user interface	Optional By default, commands of level 3 are available to the users logging into the AUX user interface.
Terminal configuration	Make terminal services available	Optional By default, terminal services are available in all user interfaces
	Set the maximum number of lines the screen can contain	Optional By default, the screen can contain up to 24 lines.
	Set history command buffer size	Optional By default, the history command buffer can contain up to 10 commands.
	Set the timeout time of a user interface	Optional The default timeout time is 10 minutes.

Caution:

Changing of Console port configuration terminates the connection to the Console port. To establish the connection again, you need to modify the configuration of the termination emulation utility running on your PC accordingly. Refer to section 2.2 “Logging in through the Console Port” for more.

2.3.2 Console Port Login Configurations for Different Authentication Modes

Table 2-3 lists Console port login configurations for different authentication modes.

Table 2-3 Console port login configurations for different authentication modes

Authentication mode	Console port login configuration		Remarks
None	Perform common configuration	Perform common configuration for Console port login	Optional Refer to section 2.3.1 “Common Configuration” for more.
Password	Configure the password	Configure the password for local authentication	Required
	Perform common configuration	Perform common configuration for Console port login	Optional Refer to section 2.3.1 “Common Configuration” for more.
Scheme	Specify to perform local authentication or RADIUS authentication	AAA configuration specifies whether to perform local authentication or RADIUS authentication	Optional Local authentication is performed by default. Refer to the AAA-RADIUS-HWTACACS-EAD module for more.
	Configure user name and password	Configure user names and passwords for local/RADIUS users	Required • The user name and password of a local user are configured on the switch. • The user name and password of a RADIUS user are configured on the RADIUS server. Refer to user manual of RADIUS server for more.
	Manage AUX users	Set service type for AUX users	Required
	Perform common configuration	Perform common configuration for Console port login	Optional Refer to section 2.3.1 “Common Configuration” for more.

Note:

Changes of the authentication mode of Console port login will not take effect unless you quit the command-line interface and then enter it again.

2.4 Console Port Login Configuration with Authentication Mode Being None

2.4.1 Configuration Procedure

Table 2-4 Console port login configuration with the authentication mode being none

Operation		Command	Description
Enter system view		**system-view**	—
Enter AUX user interface view		**user-interface aux** 0	—
Configure not to authenticate users		**authentication-mode none**	Required By default, users logging in through the Console port are not authenticated.
Configure the Console port	Set the baud rate	**speed** *speed-value*	Optional The default baud rate of an AUX port (also the Console port) is 9,600 bps.
	Set the check mode	**parity** { **even** | **none** | **odd** }	Optional By default, the check mode of a Console port is set to **none**, that is, no check bit.
	Set the stop bits	**stopbits** { **1** | **1.5** | **2** }	Optional The stop bits of a Console port is 1.
	Set the data bits	**databits** { **7** | **8** }	Optional The default data bits of a Console port is 8.
Configure the command level available to users logging into the user interface		**user privilege level** *level*	Optional By default, commands of level 3 are available to users logging into the AUX user interface.
Make terminal services available		**shell**	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain		**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.

Operation	Command	Description
Set the history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time for the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that if you configure not to authenticate the users, the command level available to users logging into a switch depends on both the **authentication-mode none** command and the **user privilege level** *level* command, as listed in the following table.

Table 2-5 Determine the command level (A)

Scenario			Command level
Authentication mode	**User type**	**Command**	
None (**authentication-mode none**)	Users logging in through Console port	The **user privilege level** *level* command not executed	Level 3
		The **user privilege level** *level* command already executed	Determined by the *level* argument

2.4.2 Configuration Example

I. Network requirements

Assume the switch is configured to allow you to login through Telnet, and your user level is set to the administrator level (level 3). After you telnet to the switch, you need to limit the console user at the following aspects.

- Do not authenticate users logging in through the Console port.
- Commands of level 2 are available to users logging into the AUX user interface.
- The baud rate of the Console port is 19,200 bps.

- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

II. Network diagram

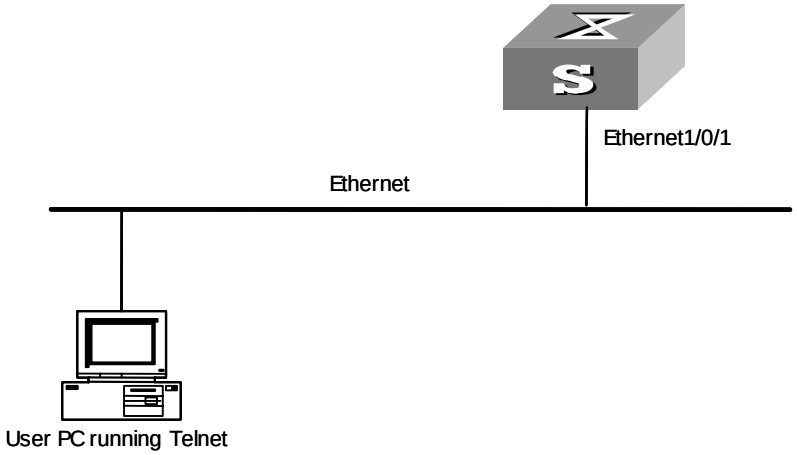


Figure 2-5 Network diagram for AUX user interface configuration (with the authentication mode being none)

III. Configuration procedure

Enter system view.

```
<H3C> system-view
```

Enter AUX user interface view.

```
[H3C] user-interface aux 0
```

Specify not to authenticate users logging in through the Console port.

```
[H3C-ui-aux0] authentication-mode none
```

Specify commands of level 2 are available to users logging into the AUX user interface.

```
[H3C-ui-aux0] user privilege level 2
```

Set the baud rate of the Console port to 19,200 bps.

```
[H3C-ui-aux0] speed 19200
```

Set the maximum number of lines the screen can contain to 30.

```
[H3C-ui-aux0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[H3C-ui-aux0] history-command max-size 20
```

Set the timeout time of the AUX user interface to 6 minutes.

```
[H3C-ui-aux0] idle-timeout 6
```

2.5 Console Port Login Configuration with Authentication Mode Being Password

2.5.1 Configuration Procedure

Table 2-6 Console port login configuration with the authentication mode being password

Operation		Command	Description
Enter system view		**system-view**	—
Enter AUX user interface view		**user-interface aux** 0	—
Configure to authenticate users using the local password		**authentication-mode password**	Required By default, users logging into a switch through the Console port are not authenticated; while those logging in through Modems or Telnet are authenticated.
Set the local password		**set authentication password** { **cipher** | **simple** } *password*	Required
Configure the Console port	Set the baud rate	**speed** *speed-value*	Optional The default baud rate of an AUX port (also the Console port) is 9,600 bps.
	Set the check mode	**parity** { **even** | **none** | **odd** }	Optional By default, the check mode of a Console port is set to **none**, that is, no check bit.
	Set the stop bits	**stopbits** { **1** | **1.5** | **2** }	Optional The default stop bits of a Console port is 1.
	Set the data bits	**databits** { **7** | **8** }	Optional The default data bits of a Console port is 8.
Configure the command level available to users logging into the user interface		**user privilege level** *level*	Optional By default, commands of level 3 are available to users logging into the AUX user interface.
Make terminal services available to the user interface		**shell**	Optional By default, terminal services are available in all user interfaces.

Operation	Command	Description
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.
Set history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time for the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that if you configure to authenticate the users in the password mode, the command level available to users logging into a switch depends on both the **authentication-mode password** and the **user privilege level** *level* command, as listed in the following table.

Table 2-7 Determine the command level (B)

Scenario			Command level
Authentication mode	**User type**	**Command**	
Local authentication (**authentication-mode password**)	Users logging in through Console port	The **user privilege level** *level* command is not executed	Level 3
		The **user privilege level** *level* command is already executed	Determined by the *level* argument

2.5.2 Configuration Example

I. Network requirements

Assume the switch is configured to allow you to login through Telnet, and your user level is set to the administrator level (level 3). After you telnet to the switch, you need to limit the console user at the following aspects.

- Authenticate users logging in through the Console port using the local password.
- Set the local password to 123456 (in plain text).
- The commands of level 2 are available to users logging into the AUX user interface.
- The baud rate of the Console port is 19,200 bps.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

II. Network diagram

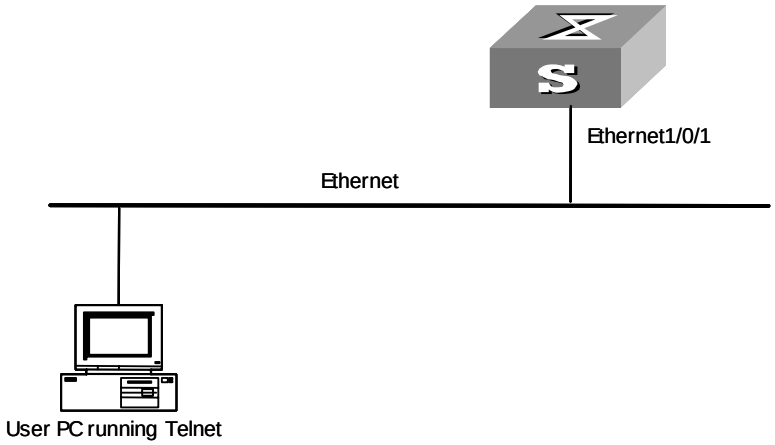


Figure 2-6 Network diagram for AUX user interface configuration (with the authentication mode being password)

III. Configuration procedure

Enter system view.

```
<H3C> system-view
```

Enter AUX user interface view.

```
[H3C] user-interface aux 0
```

Specify to authenticate users logging in through the Console port using the local password.

```
[H3C-ui-aux0] authentication-mode password
```

Set the local password to 123456 (in plain text).

```
[H3C-ui-aux0] set authentication password simple 123456
```

Specify commands of level 2 are available to users logging into the AUX user interface.

```
[H3C-ui-aux0] user privilege level 2
```

Set the baud rate of the Console port to 19,200 bps.

```
[H3C-ui-aux0] speed 19200
```

Set the maximum number of lines the screen can contain to 30.

```
[H3C-ui-aux0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[H3C-ui-aux0] history-command max-size 20
```

Set the timeout time of the AUX user interface to 6 minutes.

```
[H3C-ui-aux0] idle-timeout 6
```

2.6 Console Port Login Configuration with Authentication Mode Being Scheme

2.6.1 Configuration Procedure

Table 2-8 Console port login configuration with the authentication mode being scheme

Operation		Command	Description
Enter system view		**system-view**	—
Configure the authentication mode	Enter the default ISP domain view	**domain** d*omain-name*	Optional By default, the local AAA scheme is applied. If you specify to apply the local AAA scheme, you need to perform the configuration concerning local user as well. If you specify to apply an existing scheme by providing the *radius-scheme-name* argument, you need to perform the following configuration as well: • Perform AAA-RADIUS configuration on the switch. (Refer to the AAA-RADIUS-HWTACACS-EAD module for more.) • Configure the user name and password accordingly on the AAA server. (Refer to the user manual of AAA server.)
	Specify the AAA scheme to be applied to the domain	**scheme** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] }	
	Quit to system view	**quit**	

Operation		Command	Description
Create a local user (Enter local user view.)		**local-user** *user-name*	Required No local user exists by default.
Set the authentication password for the local user		**password** { **simple** | **cipher** } *password*	Required
Specify the service type for AUX users		**service-type terminal** [**level** *level*]	Required
Quit to system view		**quit**	—
Enter AUX user interface view		**user-interface aux** 0	—
Configure to authenticate users locally or remotely		**authentication-mode scheme** [**command-authorization**]	Required The specified AAA scheme determines whether to authenticate users locally or remotely. Users are authenticated locally by default.
Configure the Console port	Set the baud rate	**speed** *speed-value*	Optional The default baud rate of the AUX port (also the Console port) is 9,600 bps.
	Set the check mode	**parity** { **even** | **none** | **odd** }	Optional By default, the check mode of a Console port is set to **none**, that is, no check bit.
	Set the stop bits	**stopbits** { **1** | **1.5** | **2** }	Optional The default stop bits of a Console port is 1.
	Set the data bits	**databits** { **7** | **8** }	Optional The default data bits of a Console port is 8.
Configure the command level available to users logging into the user interface		**user privilege level** *level*	Optional By default, commands of level 3 are available to users logging into the AUX user interface.
Make terminal services available to the user interface		**shell**	Optional By default, terminal services are available in all user interfaces.

Operation	Command	Description
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.
Set history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time for the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that if you configure to authenticate the users in the scheme mode, the command level available to users logging into a switch depends on both the **authentication-mode scheme** [**command-authorization**] command and the **service-type terminal** [**level** *level*] command, as listed in Table 2-9.

Table 2-9 Determine the command level

Scenario			Command level
Authentication mode	**User type**	**Command**	
authentication-mode scheme [**command-authorization**]	Users logging into the Console port and passing AAA-RADIUS or local authentication	The **service-type terminal** command does not specify the available command level.	Level 0 The default command level of local users is level 0.
		The **service-type terminal** command specifies the available command level.	Determined by the command level specified by the **service-type terminal** command

2.6.2 Configuration Example

I. Network requirements

Assume the switch is configured to allow you to login through Telnet, and your user level is set to the administrator level (level 3). After you telnet to the switch, you need to limit the console user at the following aspects.

- Configure the name of the local user to be “guest”.
- Set the authentication password of the local user to 123456 (in plain text).
- Set the service type of the local user to Terminal.
- Configure to authenticate users logging in through the Console port in the scheme mode.
- The commands of level 2 are available to users logging into the AUX user interface.
- The baud rate of the Console port is 19,200 bps.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

II. Network diagram

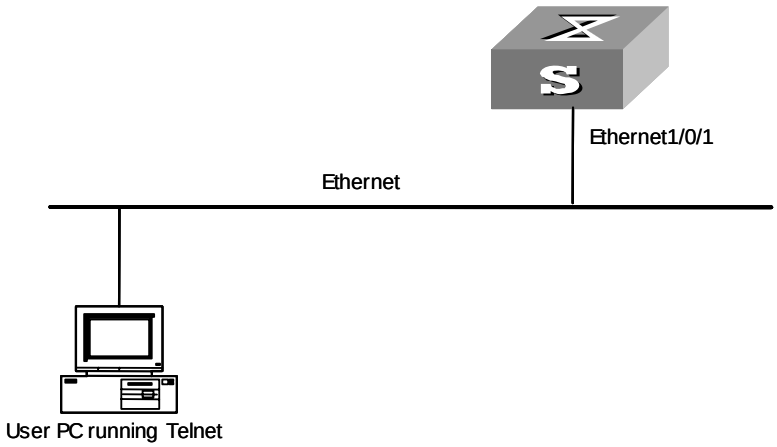


Figure 2-7 Network diagram for AUX user interface configuration (with the authentication mode being scheme)

III. Configuration procedure

Enter system view.

```
<H3C> system-view
```

Create a local user named guest and enter local user view.

```
[H3C] local-user guest
```

Set the authentication password to 123456 (in plain text).

```
[H3C-luser-guest] password simple 123456
```

Set the service type to Terminal, Specify commands of level 2 are available to users logging into the AUX user interface.

```
[H3C-luser-guest] service-type terminal level 2
[H3C-luser-guest] quit
```

Enter AUX user interface view.

```
[H3C] user-interface aux 0
```

Configure to authenticate users logging in through the Console port in the scheme mode.

```
[H3C-ui-aux0] authentication-mode scheme
```

Set the command level available to the users logging into the AUX user interface to 2.

```
[H3C-ui-aux0] user privilege level 2
```

Set the baud rate of the Console port to 19,200 bps.

```
[H3C-ui-aux0] speed 19200
```

Set the maximum number of lines the screen can contain to 30.

```
[H3C-ui-aux0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[H3C-ui-aux0] history-command max-size 20
```

Set the timeout time of the AUX user interface to 6 minutes.

```
[H3C-ui-aux0] idle-timeout 6
```

Chapter 3 Logging in through Telnet

3.1 Introduction

You can manage and maintain a switch remotely by Telneting to the switch. To achieve this, you need to configure both the switch and the Telnet terminal accordingly.

Table 3-1 Requirements for Telneting to a switch

Item	Requirement
Switch	The management VLAN of the switch is created and the route between the switch and the Telnet terminal is available. (Refer to the Management VLAN Configuration module for more.)
	The authentication mode and other settings are configured. Refer to Table 3-2 and Table 3-3.
Telnet terminal	Telnet is running.
	The IP address of the management VLAN of the switch is available.

3.1.1 Common Configuration

Table 3-2 lists the common Telnet configuration.

Table 3-2 Common Telnet configuration

Configuration		Description
VTY user interface configuration	Configure the command level available to users logging into the VTY user interface	Optional By default, commands of level 0 are available to users logging into a VTY user interface.
	Configure the protocols the user interface supports	Optional By default, Telnet and SSH protocol are supported.

Configuration		Description
VTY terminal configuration	Make terminal services available	Optional By default, terminal services are available in all user interfaces
	Set the maximum number of lines the screen can contain	Optional By default, the screen can contain up to 24 lines.
	Set history command buffer size	Optional By default, the history command buffer can contain up to 10 commands.
	Set the timeout time of a user interface	Optional The default timeout time is 10 minutes.

3.1.2 Telnet Configurations for Different Authentication Modes

Table 3-3 lists Telnet configurations for different authentication modes.

Table 3-3 Telnet configurations for different authentication modes

Authentication mode	Telnet configuration		Description
None	Perform common configuration	Perform common Telnet configuration	Optional Refer to Table 3-2.
Password	Configure the password	Configure the password for local authentication	Required
	Perform common configuration	Perform common Telnet configuration	Optional Refer to Table 3-2.

Authentication mode	Telnet configuration		Description
Scheme	Specify to perform local authentication or RADIUS authentication	AAA configuration specifies whether to perform local authentication or RADIUS authentication	Optional Local authentication is performed by default. Refer to the AAA-RADIUS-HWTACACS-EAD module for more.
	Configure user name and password	Configure user names and passwords for local/RADIUS users	Required • The user name and password of a local user are configured on the switch. • The user name and password of a remote user are configured on the DADIUS server. Refer to user manual of RADIUS server for more.
	Manage VTY users	Set service type for VTY users	Required
	Perform common configuration	Perform common Telnet configuration	Optional Refer to Table 3-2.

Note:

To improve security and avoid malicious attack to the unused SOCKETs, TCP 23 and TCP 22, ports for Telnet and SSH services respectively, will be enabled or disabled after corresponding configurations.

- If the authentication mode is **none**, TCP 23 will be enabled, and TCP 22 will be disabled.
- If the authentication mode is **password**, and the corresponding password has been set, TCP 23 will be enabled, and TCP 22 will be disabled.
- If the authentication mode is **scheme**, there are three scenarios: when the supported protocol is specified as **telnet**, TCP 23 will be enabled; when the supported protocol is specified as **ssh**, TCP 22 will be enabled; when the supported protocol is specified as **all**, both the TCP 23 and TCP 22 port will be enabled.

3.2 Telnet Configuration with Authentication Mode Being None

3.2.1 Configuration Procedure

Table 3-4 Telnet configuration with the authentication mode being none

Operation	Command	Description
Enter system view	**system-view**	—
Enter one or more VTY user interface views	**user-interface vty** *first-number* [*last-number*]	—
Configure not to authenticate users logging into VTY user interfaces	**authentication-mode none**	Required By default, VTY users are authenticated after logging in.
Configure the command level available to users logging into VTY user interface	**user privilege level** *level*	Optional By default, commands of level 0 are available to users logging into VTY user interfaces.
Configure the protocols to be supported by the VTY user interface	**protocol inbound** { **all** | **ssh** | **telnet** }	Optional By default, both Telnet protocol and SSH protocol are supported.
Make terminal services available	**shell**	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.
Set the history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.

Operation	Command	Description
Set the timeout time of the VTY user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that if you configure not to authenticate the users, the command level available to users logging into a switch depends on both the **authentication-mode none** command and the **user privilege level** *level* command, as listed in Table 3-5.

Table 3-5 Determine the command level when users logging into switches are not authenticated

Scenario			Command level
Authentication mode	**User type**	**Command**	
None (**authentication-mode none**)	VTY users	The **user privilege level** *level* command is not executed	Level 0
		The **user privilege level** *level* command is already executed	Determined by the *level* argument

3.2.2 Configuration Example

I. Network requirements

Assume the switch is configured to allow you to login through Console, and your user level is set to the administrator level (level 3). After you login through Console, you need to limit the telnet user into VTY 0 at the following aspects.

- Do not authenticate users logging into VTY 0.
- Commands of level 2 are available to users logging into VTY 0.
- Telnet protocol is supported.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

II. Network diagram

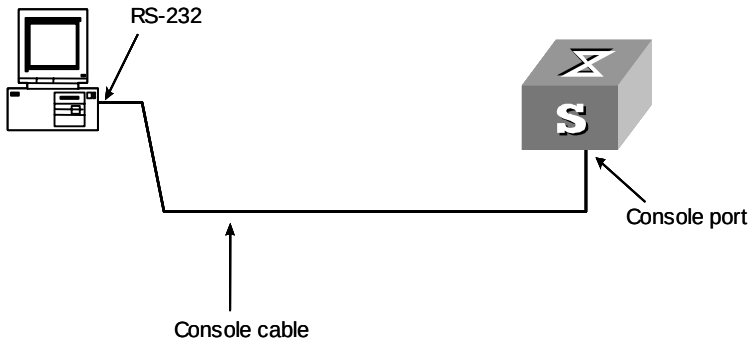


Figure 3-1 Network diagram for Telnet configuration (with the authentication mode being none)

III. Configuration procedure

Enter system view.

```
<H3C> system-view
```

Enter VTY 0 user interface view.

```
[H3C] user-interface vty 0
```

Configure not to authenticate Telnet users logging into VTY 0.

```
[H3C-ui-vty0] authentication-mode none
```

Specify commands of level 2 are available to users logging into VTY 0.

```
[H3C-ui-vty0] user privilege level 2
```

Configure Telnet protocol is supported.

```
[H3C-ui-vty0] protocol inbound telnet
```

Set the maximum number of lines the screen can contain to 30.

```
[H3C-ui-vty0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[H3C-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[H3C-ui-vty0] idle-timeout 6
```

3.3 Telnet Configuration with Authentication Mode Being Password

3.3.1 Configuration Procedure

Table 3-6 Telnet configuration with the authentication mode being password

Operation	Command	Description
Enter system view	**system-view**	—
Enter one or more VTY user interface views	**user-interface vty** *first-number* [*last-number*]	—
Configure to authenticate users logging into VTY user interfaces using the local password	**authentication-mode password**	Required
Set the local password	**set authentication password** { **cipher** | **simple** } *password*	Required
Configure the command level available to users logging into the user interface	**user privilege level** *level*	Optional By default, commands of level 0 are available to users logging into VTY user interface.
Configure the protocol to be supported by the user interface	**protocol inbound** { **all** | **ssh** | **telnet** }	Optional By default, both Telnet protocol and SSH protocol are supported.
Make terminal services available	**shell**	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.
Set the history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.

Operation	Command	Description
Set the timeout time of the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that if you configure to authenticate the users in the password mode, the command level available to users logging into a switch depends on both the **authentication-mode password** command and the **user privilege level** *level* command, as listed in Table 3-7.

Table 3-7 Determine the command level when users logging into switches are authenticated in the password mode

Scenario			Command level
Authentication mode	**User type**	**Command**	
Password (**authentication-mode password**)	VTY users	The **user privilege level** *level* command not executed	Level 0
		The **user privilege level** *level* command already executed	Determined by the *level* argument

3.3.2 Configuration Example

I. Network requirements

Assume the switch is configured to allow you to login through Console, and your user level is set to the administrator level (level 3). After you login through Console, you need to limit the telnet user into VTY 0 at the following aspects.

- Authenticate users logging into VTY 0 using the local password.
- Set the local password to 123456 (in plain text).
- Commands of level 2 are available to users logging into VTY 0.
- Telnet protocol is supported.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.

- The timeout time of VTY 0 is 6 minutes.

II. Network diagram

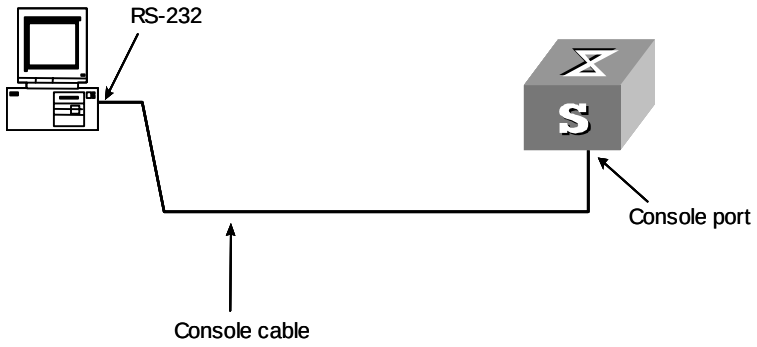


Figure 3-2 Network diagram for Telnet configuration (with the authentication mode being password)

III. Configuration procedure

Enter system view.

```
<H3C> system-view
```

Enter VTY 0 user interface view.

```
[H3C] user-interface vty 0
```

Configure to authenticate users logging into VTY 0 using the local password.

```
[H3C-ui-vty0] authentication-mode password
```

Set the local password to 123456 (in plain text).

```
[H3C-ui-vty0] set authentication password simple 123456
```

Specify commands of level 2 are available to users logging into VTY 0.

```
[H3C-ui-vty0] user privilege level 2
```

Configure Telnet protocol is supported.

```
[H3C-ui-vty0] protocol inbound telnet
```

Set the maximum number of lines the screen can contain to 30.

```
[H3C-ui-vty0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[H3C-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[H3C-ui-vty0] idle-timeout 6
```

3.4 Telnet Configuration with Authentication Mode Being Scheme

3.4.1 Configuration Procedure

Table 3-8 Telnet configuration with the authentication mode being scheme

<table>
<tr><th colspan="2">Operation</th><th>Command</th><th>Description</th></tr>
<tr><td colspan="2">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td rowspan="3">Configure the authentication scheme</td><td>Enter the default ISP domain view</td><td>domain domain-name</td><td rowspan="3">Optional
By default, the local AAA scheme is applied. If you specify to apply the local AAA scheme, you need to perform the configuration concerning local user as well.
If you specify to apply an existing scheme by providing the radius-scheme-name argument, you need to perform the following configuration as well:
• Perform AAA-RADIUS configuration on the switch. (Refer to the AAA-RADIUS-HWTACACS-EAD module for more.)
• Configure the user name and password accordingly on the AAA server. (Refer to the user manual of AAA server.)</td></tr>
<tr><td>Configure the AAA scheme to be applied to the domain</td><td>scheme { local | none | radius-scheme radius-scheme-name [local] | hwtacacs-scheme hwtacacs-scheme-name [local] }</td></tr>
<tr><td>Quit to system view</td><td>quit</td></tr>
<tr><td colspan="2">Create a local user and enter local user view</td><td>local-user user-name</td><td>No local user exists by default.</td></tr>
<tr><td colspan="2">Set the authentication password for the local user</td><td>password { simple | cipher } password</td><td>Required</td></tr>
<tr><td colspan="2">Specify the service type for VTY users</td><td>service-type telnet [level level]</td><td>Required</td></tr>
<tr><td colspan="2">Quit to system view</td><td>quit</td><td>—</td></tr>
<tr><td colspan="2">Enter one or more VTY user interface views</td><td>user-interface vty first-number [last-number]</td><td>—</td></tr>
</table>

Operation	Command	Description
Configure to authenticate users locally or remotely	**authentication-mode scheme** [**command-authorization**]	Required The specified AAA scheme determines whether to authenticate users locally or remotely. Users are authenticated locally by default.
Configure the command level available to users logging into the user interface	**user privilege level** *level*	Optional By default, commands of level 0 are available to users logging into the VTY user interfaces.
Configure the supported protocol	**protocol inbound** { **all** | **ssh** | **telnet** }	Optional Both Telnet protocol and SSH protocol are supported by default.
Make terminal services available	**shell**	Optional Terminal services are available in all use interfaces by default.
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.
Set history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time for the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that if you configure to authenticate the users in the scheme mode, the command level available to users logging into a switch depends on the **authentication-mode scheme** [**command-authorization**] command, the **user privilege level** *level* command, and the **service-type** { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** }* [**level** *level*] } command, as listed in Table 3-9.

Table 3-9 Determine the command level when users logging into switches are authenticated in the scheme mode

Scenario			Command level
Authentication mode	**User type**	**Command**	
authentication-mode scheme [**command-authorization**]	VTY users that are AAA-RADIUS authenticated or locally authenticated	The **user privilege level** *level* command is not executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is not executed, and the **service-type** command specifies the available command level.	Determined by the **service-type** command
		The **user privilege level** *level* command is executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is executed, and the **service-type** command specifies the available command level.	Determined by the **service-type** command
	VTY users that are authenticated in the RSA mode of SSH	The **user privilege level** *level* command is not executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is not executed, and the **service-type** command specifies the available command level.	
		The **user privilege level** *level* command is executed, and the **service-type** command does not specify the available command level.	Determined by the **user privilege level** *level* command

Scenario			Command level
Authentication mode	**User type**	**Command**	
		The **user privilege level** *level* command is executed, and the **service-type** command specifies the available command level.	
	VTY users that are authenticated in the password mode of SSH	The **user privilege level** *level* command is not executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is not executed, and the **service-type** command specifies the available command level.	Determined by the **service-type** command
		The **user privilege level** *level* command is executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is executed, and the **service-type** command specifies the available command level.	Determined by the **service-type** command

Note:

Refer to the corresponding modules in this manual for information about AAA, RADIUS, and SSH.

3.4.2 Configuration Example

I. Network requirements

Assume the switch is configured to allow you to login through Console, and your user level is set to the administrator level (level 3). After you login through Console, you need to limit the telnet user into VTY 0 at the following aspects.

- Configure the name of the local user to be “guest”.
- Set the authentication password of the local user to 123456 (in plain text).
- Set the service type of VTY users to Telnet.
- Configure to authenticate users logging into VTY 0 in scheme mode.
- The commands of level 2 are available to users logging into VTY 0.

- Only Telnet protocol is supported in VTY 0.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

II. Network diagram

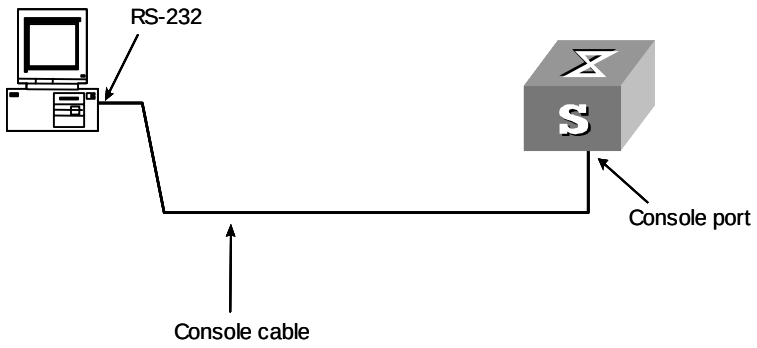


Figure 3-3 Network diagram for Telnet configuration (with the authentication mode being scheme)

III. Configuration procedure

Enter system view.

```
<H3C> system-view
```

Create a local user named “guest” and enter local user view.

```
[H3C] local-user guest
```

Set the authentication password of the local user to 123456 (in plain text).

```
[H3C-luser-guest] password simple 123456
```

Set the service type to Telnet, Specify commands of level 2 are available to users logging into VTY 0..

```
[H3C-luser-guest] service-type telnet level 2
[H3C-luser-guest] quit
```

Enter VTY 0 user interface view.

```
[H3C] user-interface vty 0
```

Configure to authenticate users logging into VTY 0 in the scheme mode.

```
[H3C-ui-vty0] authentication-mode scheme
```

Set the command level available to the users logging into the AUX user interface to 2.

```
[H3C-ui-aux0] user privilege level 2
```

Configure Telnet protocol is supported.

```
[H3C-ui-vty0] protocol inbound telnet
```

Set the maximum number of lines the screen can contain to 30.

```
[H3C-ui-vty0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[H3C-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[H3C-ui-vty0] idle-timeout 6
```

3.5 Telneting to a Switch

3.5.1 Telneting to a Switch from a Terminal

1) Assign an IP address to the interface of the management VLAN of a switch. This can be achieved by executing the **ip address** command in VLAN interface view after you log in through the Console port.

- Connect the serial port of your PC/terminal to the Console port of the switch, as shown in Figure 3-4

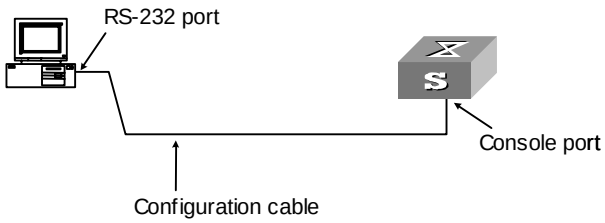


Figure 3-4 Diagram for establishing connection to a Console port

- Launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 9X) on the PC, with the baud rate set to 9,600 bps, data bits set to 8, parity check set to none, and flow control set to none.
- Turn on the switch and press Enter as prompted. The prompt (such as <H3C>) appears, as shown in the following figure.

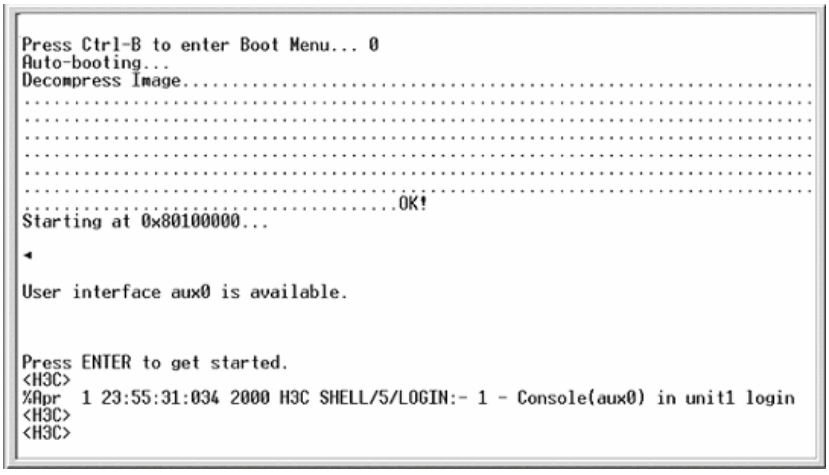


Figure 3-5 The terminal window

- Perform the following operations in the terminal window to assign an IP address to the management VLAN interface of the switch.

Enter system view

```
<H3C> system-view
```

Enter management VLAN interface view.

```
[H3C] interface Vlan-interface 1
```

Cancel original IP address of management VLAN.

```
[H3C-Vlan-interface1] undo ip address
```

Set the IP address of the management VLAN interface to 202.38.160.92, with the mask set to 255.255.255.0.

```
[H3C-Vlan-interface1] ip address 202.38.160.92 255.255.255.0
```

2) Perform Telnet-related configuration on the switch. Refer to section 3.2 "Telnet Configuration with Authentication Mode Being None", section 3.3 "Telnet Configuration with Authentication Mode Being Password", and section 3.4 "Telnet Configuration with Authentication Mode Being Scheme" for more.
3) Connect your PC/terminal and the Switch to an Ethernet, as shown in Figure 3-6. Make sure the port through which the switch is connected to the Ethernet belongs to the management VLAN and the route between your PC and the management VLAN interface is reachable.

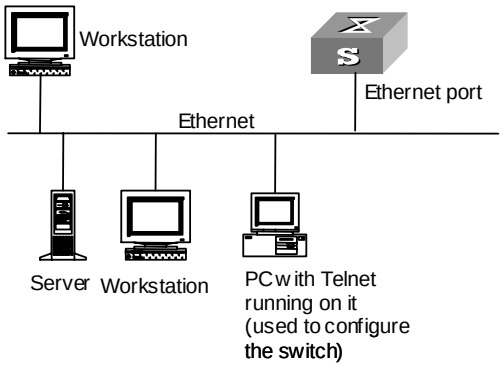


Figure 3-6 Network diagram for Telnet connection establishment

4) Launch Telnet on your PC, with the IP address of the management VLAN interface of the switch as the parameter, as shown in Figure 3-7.

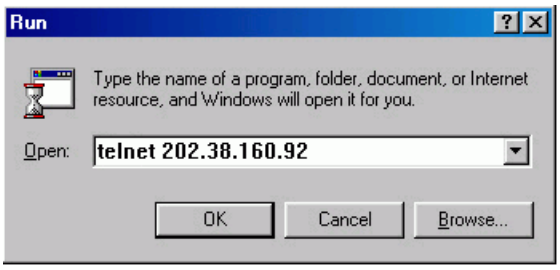


Figure 3-7 Launch Telnet

5) Enter the password when the Telnet window displays “Login authentication” and prompts for login password. The CLI prompt (such as <H3C>) appears if the password is correct. If all VTY user interfaces of the switch are in use, you will fail to establish the connection and receive the message that says “All user interfaces are used, please try later!”. A H3C series Ethernet switch can accommodate up to five Telnet connections at same time.
6) After successfully Telneting to a switch, you can configure the switch or display the information about the switch by executing corresponding commands. You can also type ? at any time for help. Refer to the following chapters for the information about the commands.

🕮 **Note:**

- A Telnet connection is terminated if you delete or modify the IP address of the VLAN interface in the Telnet session.
- By default, commands of level 0 are available to Telnet users authenticated by password. Refer to section 1.2 “Command Hierarchy/Command View” in CLI module for information about command hierarchy.

3.5.2 Telneting to another Switch from the Current Switch

You can Telnet to another switch from the current switch. In this case, the current switch operates as the client, and the other operates as the server. If the interconnected Ethernet ports of the two switches are in the same LAN segment, make sure the IP addresses of the two management VLAN interfaces to which the two Ethernet ports belong to are of the same network segment, or the route between the two VLAN interfaces is available.

As shown in Figure 3-8, after Telneting to a switch (labeled as Telnet client), you can Telnet to another switch (labeled as Telnet server) by executing the **telnet** command and then configure it.

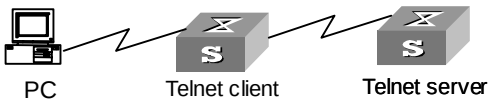


Figure 3-8 Network diagram for Telneting to another switch from the current switch

1) Perform Telnet-related configuration on the switch operating as the Telnet server. Refer to section 3.2 "Telnet Configuration with Authentication Mode Being None", section 3.3 "Telnet Configuration with Authentication Mode Being Password", and section 3.4 "Telnet Configuration with Authentication Mode Being Scheme" for more.
2) Telnet to the switch operating as the Telnet client.
3) Execute the following command on the switch operating as the Telnet client:

```
<H3C> telnet xxxx
```

Where xxxx is the IP address or the host name of the switch operating as the Telnet server. You can use the **ip host** to assign a host name to a switch.

4) Enter the password. If the password is correct, the CLI prompt (such as <H3C>) appears. If all VTY user interfaces of the switch are in use, you will fail to establish the connection and receive the message that says "All user interfaces are used, please try later!".
5) After successfully Telneting to the switch, you can configure the switch or display the information about the switch by executing corresponding commands. You can also type ? at any time for help. Refer to the following chapters for the information about the commands.

Chapter 4 Logging in Using Modem

4.1 Introduction

The administrator can log into the Console port of a remote switch using a modem through PSTN (public switched telephone network) if the remote switch is connected to the PSTN through a modem to configure and maintain the switch remotely. When a network operates improperly or is inaccessible, you can log into the switches in the network in this way to configure these switches, to query logs and warning messages, and to locate problems.

To log into a switch in this way, you need to configure the administrator side and the switch properly, as listed in the following table.

Table 4-1 Requirements for logging into a switch using a modem

Item	Requirement
Administrator side	The PC can communicate with the modem connected to it.
	The modem is properly connected to PSTN.
	The telephone number of the switch side is available.
Switch side	The modem is connected to the Console port of the switch properly.
	The modem is properly configured.
	The modem is properly connected to PSTN and a telephone set.
	The authentication mode and other related settings are configured on the switch. Refer to Table 2-3.

4.2 Configuration on the Administrator Side

The PC can communicate with the modem connected to it. The modem is properly connected to PSTN. And the telephone number of the switch side is available.

4.3 Configuration on the Switch Side

4.3.1 Modem Configuration

Perform the following configuration on the modem directly connected to the switch:

```
AT&F      ---------------------- Restore the factory settings
ATS0=1    ---------------------- Configure to answer automatically after the
first ring
AT&D      ---------------------- Ignore DTR signal
```

```
AT&K0     ---------------------- Disable flow control
AT&R1     ---------------------- Ignore RTS signal
AT&S0     ---------------------- Set DSR to high level by force
ATEQ1&W   ---------------------- Disable the modem from returning command
response and the result, save the changes
```

You can verify your configuration by executing the **AT&V** command.

Note:

- The above configuration is unnecessary to the modem on the administrator side.
- The configuration commands and the output of different modems may differ. Refer to the user manual of the modem when performing the above configuration.

4.3.2 Switch Configuration

Note:

After logging into a switch through its Console port by using a modem, you will enter the AUX user interface. The corresponding configuration on the switch is the same as those when logging into the switch locally through its Console port except that:

- When you log in through the Console port using a modem, the baud rate of the Console port is usually set to a value lower than the transmission speed of the modem. Otherwise, packets may get lost.
- Other settings of the Console port, such as the check mode, the stop bits, and the data bits, remain the default.

The configuration on the switch depends on the authentication mode the user is in. Refer to Table 2-3 for the information about authentication mode configuration.

I. Configuration on switch when the authentication mode is none

Refer to section 2.4 “Console Port Login Configuration with Authentication Mode Being None”.

II. Configuration on switch when the authentication mode is password

Refer to section 2.5 “Console Port Login Configuration with Authentication Mode Being Password”.

III. Configuration on switch when the authentication mode is scheme

Refer to section 2.6 “Console Port Login Configuration with Authentication Mode Being Scheme”.

4.4 Modem Connection Establishment

1) Before using Modem to log in the switch, perform corresponding configuration for different authentication modes on the switch. Refer to section 2.4 "Console Port Login Configuration with Authentication Mode Being None”, section 2.5 “Console Port Login Configuration with Authentication Mode Being Password”, and section 2.6 “Console Port Login Configuration with Authentication Mode Being Scheme” for more.

2) Perform the following configuration to the modem directly connected to the switch.

```
AT&F      ---------------------- Restore the factory settings
ATS0=1    ---------------------- Configure to answer automatically after the
first ring
AT&D      ---------------------- Ignore DTR signal
AT&K0     ---------------------- Disable flow control
AT&R1     ---------------------- Ignore RTS signal
AT&S0     ---------------------- Set DSR to high level by force
ATEQ1&W   ---------------------- Disable the modem from returning command
response and the result, save the changes
```

You can verify your configuration by executing the **AT&V** command.

🕮 **Note:**

- The configuration commands and the output of different modems may differ. Refer to the user manual of the modem when performing the above configuration.
- It is recommended that the baud rate of the AUX port (also the Console port) be set to a value lower than the transmission speed of the modem. Otherwise, packets may get lost.

---

3) Connect your PC, the modems, and the switch, as shown in the following figure.

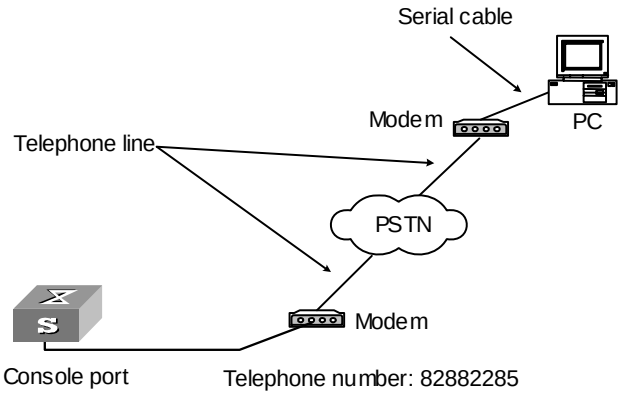


Figure 4-1 Establish the connection by using modems

4) Launch a terminal emulation utility on the PC and set the telephone number to call the modem directly connected to the switch, as shown in Figure 4-2 and Figure 4-3. Note that you need to set the telephone number to that of the modem directly connected to the switch.

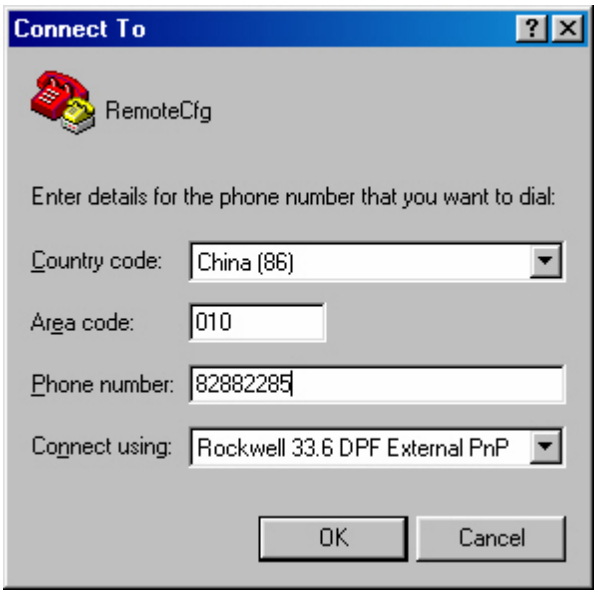


Figure 4-2 Set the telephone number

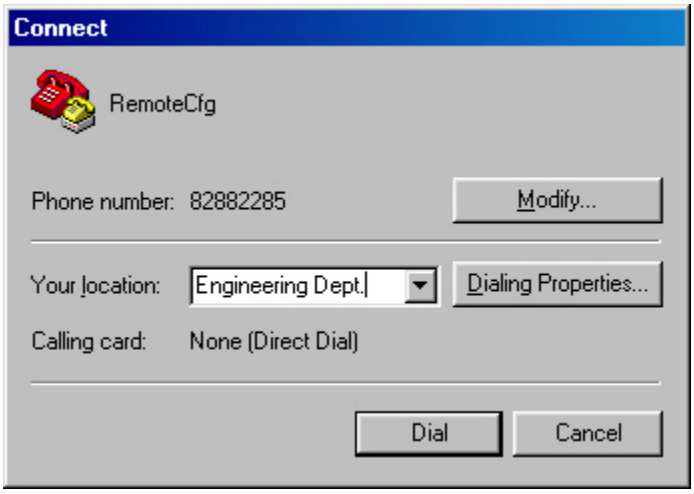


Figure 4-3 Call the modem

5) Provide the password when prompted. If the password is correct, the prompt (such as <H3C>) appears. You can then configure or manage the switch. You can also enter the character ? at anytime for help. Refer to the following chapters for information about the configuration commands.

Note:

If you perform no AUX user-related configuration on the switch, the commands of level 3 are available to modem users. Refer to the CLI module for information about command level.

Chapter 5 Logging in through Web-based Network Management System

5.1 Introduction

An S3600 Ethernet switch has a Web server built in. You can log into an S3600 Ethernet switch through a Web browser and manage and maintain the switch intuitively by interacting with the built-in Web server.

To log into an S3600 Ethernet switch through the built-in Web-based network management system, you need to perform the related configuration on both the switch and the PC operating as the network management terminal.

Table 5-1 Requirements for logging into a switch through the Web-based network management system

Item	Requirement
Switch	The management VLAN of the switch is configured. The route between the switch and the network management terminal is available. (Refer to the Management VLAN Configuration module for more.)
	The user name and password for logging into the Web-based network management system are configured.
PC operating as the network management terminal	IE is available.
	The IP address of the management VLAN interface of the switch is available.

5.2 HTTP Connection Establishment

1) Log into the switch through the Console port and assign an IP address to the management VLAN interface of the switch See section 3.5.1 "Telneting to a Switch from a Terminal" for more.
2) Through the Console port, configure the user name and the password for the Web-based network management system.

Configure the user name to be admin.

```
[H3C] local-user admin
```

Set the user level to level 3.

```
[H3C-luser-admin] service-type telnet level 3
```

Set the password to admin.

```
[H3C-luser-admin] password simple admin
```

3) Establish an HTTP connection between your PC and the switch, as shown in the following figure.

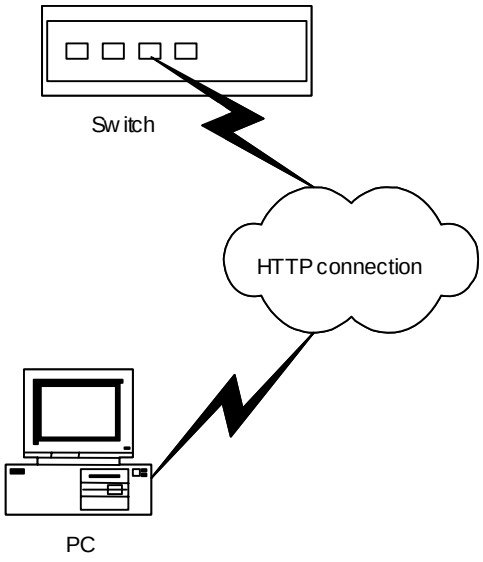


Figure 5-1 Establish an HTTP connection between your PC and the switch

4) Log into the switch through IE. Launch IE on the Web-based network management terminal (your PC) and enter the IP address of the management VLAN interface of the switch (here it is http://10.153.17.82) in the address bar. (Make sure the route between the Web-based network management terminal and the switch is available.)
5) When the login interface (as shown in Figure 5-2) appears, enter the user name and the password configured in step 2 and click <Login> to bring up the main page of the Web-based network management system.



Figure 5-2 The login page of the Web-based network management system

5.3 Web Server Shutdown/Startup

You can shut down or start up the Web server.

Table 5-2 Shut down/start up Web server

Operation	Command	Description
Shut down the Web server	**ip http shutdown**	Required Execute this command in system view.
Start the Web server	**undo ip http shutdown**	Required Execute this command in system view.

The Web server is started by default.

Note:

To improve security and avoid malicious attack to the unused SOCKETs, TCP 80 port for HTTP service will be enabled or disabled after corresponding configurations.
If you use the **undo ip http shutdown** command to enable the Web Server, TCP 80 will be enabled; if you use the **ip http shutdown** command to disabled the Web Server, TCP 80 will be disabled.

Caution:

After the Web files are upgraded, you need to specify a new Web file from the boot menu after the reboot. Otherwise, the Web Server function cannot be used normally.

Chapter 6 Logging in through NMS

6.1 Introduction

You can also log into a switch through an NMS (network management station), and then configure and manage the switch through the agent module on the switch.

- The agent here refers to the software running on network devices (switches) and as the server.
- SNMP (simple network management protocol) is applied between the NMS and the agent.

To log into a switch through an NMS, you need to perform related configuration on both the NMS and the switch.

Table 6-1 Requirements for logging into a switch through an NMS

Item	Requirement
Switch	The management VLAN of the switch is configured. The route between the NMS and the switch is available. (Refer to the Management VLAN Configuration module for more.)
	The basic SNMP functions are configured. (Refer to the SNMP-RMON module for more.)
NMS	The NMS is properly configured. (Refer to the user manual of your NMS for more.)

6.2 Connection Establishment Using NMS

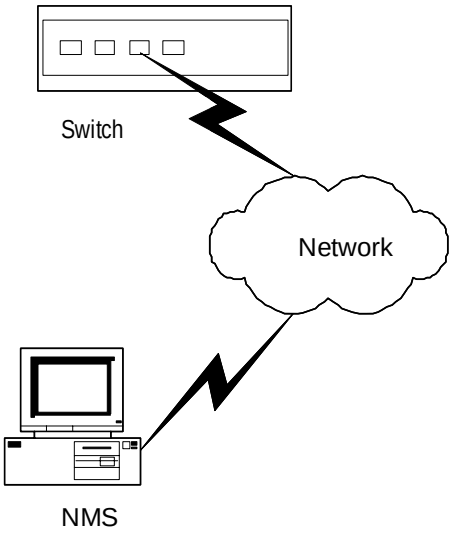


Figure 6-1 Network diagram for logging in through an NMS

Chapter 7 Configuring Source IP Address for Telnet Service Packets

You can configure source IP address or source interface for the Telnet server and Telnet client. This provides a way to manage services.

7.1 Configuring Source IP Address for Telnet Service Packets

I. Configuration in user view

Table 7-1 Configure a source IP address for service packets in user view

Operation	Command	Description
Specify a source IP address for the Telnet client	**telnet** *remote-server* **source-ip** *ip-address*	Optional
Specify a source interface for the Telnet client	**telnet** *remote-server* **source-interface** *interface-type interface-number*	Optional

II. Configuration in system view

Table 7-2 Configure a source IP address for service packets in system view

Operation	Command	Description
Specify a source IP address for Telnet server	**telnet-server source-ip** *ip-address*	Optional
Specify a source interface for Telnet server	**telnet-server source-interface** *interface-type interface-number*	Optional
Specify source IP address for Telnet client	**telnet source-ip** *ip-address*	Optional
Specify a source interface for Telnet client	**telnet source-interface** *interface-type interface-number*	Optional

🕮 **Note:**

- To perform the configurations listed in Table 7-1 and Table 7-2, make sure that:
- The IP address specified is that of the local device.
- The interface specified exists.

7.2 Displaying Source IP Address Configuration

Execute the **display** command in any view to display the operation state after the above configurations. You can verify the configuration effect through the displayed information.

Table 7-3 Display the source IP address configuration

Operation	Command
Display the source IP address configured for the Telnet client	**display telnet source-ip**
Display the source IP address configured for the Telnet server	**display telnet-server source-ip**

Chapter 8 User Control

8.1 Introduction

A switch provides ways to control different types of login users, as listed in Table 8-1.

Table 8-1 Ways to control different types of login users

Login mode	Control method	Implementation	Related section
Telnet	By source IP address	Through basic ACL	Section 8.2.2 “Controlling Telnet Users by Source IP Addresses”.
	By source and destination IP address	Through advanced ACL	Section 8.2.3 “Controlling Telnet Users by Source and Destination IP Addresses”.
	By source MAC address	Through Layer 2 ACL	Section 8.2.4 “Controlling Telnet Users by Source MAC Addresses”
SNMP	By source IP addresses	Through basic ACL	Section 8.3 “Controlling Network Management Users by Source IP Addresses”.
WEB	By source IP addresses	Through basic ACL	Section 8.4 “Controlling Web Users by Source IP Address”.
	Disconnect Web users by force	By executing commands in CLI	Section 8.4.3 “Disconnecting a Web User by Force”.

8.2 Controlling Telnet Users

8.2.1 Prerequisites

The controlling policy against Telnet users is determined, including the source and destination IP addresses and source MAC addresses to be controlled and the controlling actions (permitting or denying).

8.2.2 Controlling Telnet Users by Source IP Addresses

Controlling Telnet users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999.

Table 8-2 Control Telnet users by source IP addresses

Operation	Command	Description
Enter system view	**system-view**	—
Create a basic ACL or enter basic ACL view	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **permit** | **deny** } [**fragment** | **source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name*]*	Required
Quit to system view	**quit**	—
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	—
Apply the ACL to control Telnet users by source IP addresses	**acl** *acl-number* { **inbound** | **outbound** }	Required The **inbound** keyword specifies to filter the users trying to Telnet to the current switch. The **outbound** keyword specifies to filter users trying to Telnet to other switches from the current switch.

8.2.3 Controlling Telnet Users by Source and Destination IP Addresses

Controlling Telnet users by source and destination IP addresses is achieved by applying advanced ACLs, which are numbered from 3000 to 3999. Refer to the ACL module for information about defining an ACL.

Table 8-3 Control Telnet users by source and destination IP addresses

Operation	Command	Description
Enter system view	**system-view**	—
Create an advanced ACL or enter advanced ACL view	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	As for the **acl number** command, the **config** keyword is specified by default.

Operation	Command	Description
Define rules for the ACL	**rule** [*rule-id*] { **permit** | **deny** } *protocol* [**source** { *source-addr wildcard* | **any** }] [**destination** { *dest-addr wildcard* | **any** }] [**source-port** *operator port1* [*port2*]] [**destination-port** *operator port1* [*port2*]] [**icmp-type** *type code*] [**established**] [{ **precedence** *precedence* **tos** *tos* | **dscp** *dscp* }* | **fragment** | **time-range** *name*]*	Required You can define rules as needed to filter by specific source and destination IP addresses.
Quit to system view	**quit**	—
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	—
Apply the ACL to control Telnet users by specified source and destination IP addresses	**acl** *acl-number* { **inbound** | **outbound** }	Required The **inbound** keyword specifies to filter the users trying to Telnet to the current switch. The **outbound** keyword specifies to filter users trying to Telnet to other switches from the current switch.

8.2.4 Controlling Telnet Users by Source MAC Addresses

Controlling Telnet users by source MAC addresses is achieved by applying Layer 2 ACLs, which are numbered from 4000 to 4999. Refer to the ACL module for information about defining an ACL.

Table 8-4 Control Telnet users by source MAC addresses

Operation	Command	Description
Enter system view	**system-view**	—
Create or enter Layer 2 ACL view	**acl number** *acl-number*	—

Operation	Command	Description
Define rules for the ACL	**rule** [*rule-id*] { **permit** | **deny** } [[**type** *protocol-type type-mask* | **lsap** *lsap-type type-mask*] | *format-type* | **cos** *cos* | **source** { *source-vlan-id* | *source-mac-addr source-mac-mask* }* | **dest** { *dest-mac-addr dest-mac-mask* } | **time-range** *name*]*	Required You can define rules as needed to filter by specific source MAC addresses.
Quit to system view	**quit**	—
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	—
Apply the ACL to control Telnet users by specified source MAC addresses	**acl** *acl-number* { **inbound** | **outbound** }	Required The **inbound** keyword specifies to filter the users trying to Telnet to the current switch. The **outbound** keyword specifies to filter users trying to Telnet to other switches from the current switch.

8.2.5 Configuration Example

I. Network requirements

Only the Telnet users sourced from the IP address of 10.110.100.52 and 10.110.100.46 are permitted to log into the switch.

II. Network diagram

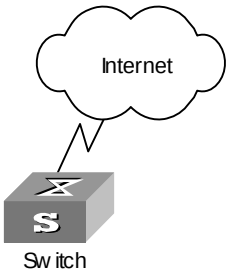


Figure 8-1 Network diagram for controlling Telnet users using ACLs

III. Configuration procedure

Define a basic ACL.

```
<H3C> system-view
[H3C] acl number 2000 match-order config
[H3C-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[H3C-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[H3C-acl-basic-2000] rule 3 deny source any
[H3C-acl-basic-2000] quit
```

Apply the ACL.

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] acl 2000 inbound
```

8.3 Controlling Network Management Users by Source IP Addresses

You can manage an S3600 Ethernet switch through network management software. Network management users can access switches through SNMP.

You need to perform the following two operations to control network management users by source IP addresses.

- Defining an ACL
- Applying the ACL to control users accessing the switch through SNMP

8.3.1 Prerequisites

The controlling policy against network management users is determined, including the source IP addresses to be controlled and the controlling actions (permitting or denying).

8.3.2 Controlling Network Management Users by Source IP Addresses

Controlling network management users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999.

Table 8-5 Control network management users by source IP addresses

Operation	Command	Description
Enter system view	**system-view**	—
Create a basic ACL or enter basic ACL view	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **permit** | **deny** } [**fragment** | **source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name*]*	Required
Quit to system view	**quit**	—

Operation	Command	Description
Apply the ACL while configuring the SNMP community name	**snmp-agent community** { **read** | **write** } *community-name* [**mib-view** *view-name* | **acl** *acl-number*]*	Optional By default, SNMPv1 and SNMPv2c use community name to access.
Apply the ACL while configuring the SNMP group name	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*] **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]	Optional By default, the authentication mode and the encryption mode are configured as none for the group.
Apply the ACL while configuring the SNMP user name	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*] **snmp-agent usm-user v3** *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode des56** *priv-password*] [**acl** *acl-number*]	Optional

Note:

You can specify different ACLs while configuring the SNMP community name, SNMP group name, and SNMP user name..

As SNMP community name is a feature of SNMPv1 and SNMPv2c, the specified ACLs in the command that configures SNMP community names (the **snmp-agent community** command) take effect in the network management systems that adopt SNMPv1 or SNMPv2c.

Similarly, as SNMP group name and SNMP username name are a feature of SNMPv2c and the higher SNMP versions, the specified ACLs in the commands that configure SNMP group names and SNMP user names take effect in the network management systems that adopt SNMPv2c or higher SNMP versions. If you specify ACLs in the commands, the network management users are filtered by the SNMP group name and SNMP user name.

8.3.3 Configuration Example

I. Network requirements

Only SNMP users sourced from the IP addresses of 10.110.100.52 and 10.110.100.46 are permitted to access the switch.

II. Network diagram

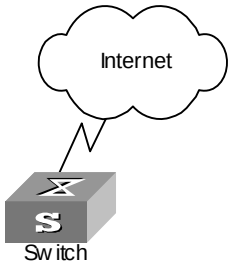


Figure 8-2 Network diagram for controlling SNMP users using ACLs

III. Configuration procedure

Define a basic ACL.

```
<H3C> system-view
[H3C] acl number 2000 match-order config
[H3C-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[H3C-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[H3C-acl-basic-2000] rule 3 deny source any
[H3C-acl-basic-2000] quit
```

Apply the ACL to only permit SNMP users sourced from the IP addresses of 10.110.100.52 and 10.110.100.46 to access the switch.

```
[H3C] snmp-agent community read aaa acl 2000
[H3C] snmp-agent group v2c groupa acl 2000
[H3C] snmp-agent usm-user v2c usera groupa acl 2000
```

8.4 Controlling Web Users by Source IP Address

You can manage an S3600 Ethernet switch remotely through Web. Web users can access a switch through HTTP connections.

You need to perform the following two operations to control Web users by source IP addresses.

- Defining an ACL
- Applying the ACL to control Web users

8.4.1 Prerequisites

The controlling policy against Web users is determined, including the source IP addresses to be controlled and the controlling actions (permitting or denying).

8.4.2 Controlling Web Users by Source IP Addresses

Controlling Web users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999.

Table 8-6 Control Web users by source IP addresses

Operation	Command	Description
Enter system view	**system-view**	—
Create a basic ACL or enter basic ACL view	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **permit** | **deny** } [**fragment** | **source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name*]*	Required
Quit to system view	**quit**	—
Apply the ACL to control Web users	**ip http acl** *acl-number*	Optional

8.4.3 Disconnecting a Web User by Force

The administrator can disconnect a Web user by force using the related command.

Table 8-7 Disconnect a Web user by force

Operation	Command	Description
Disconnect a Web user by force	**free web-users** { **all** | **user-id** *user-id* | **user-name** *user-name* }	Required Execute this command in user view.

8.4.4 Configuration Example

I. Network requirements

Only the users sourced from the IP address of 10.110.100.46 are permitted to access the switch.

II. Network diagram

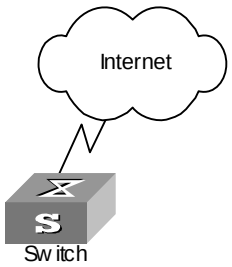


Figure 8-3 Network diagram for controlling Web users using ACLs

III. Configuration procedure

Define a basic ACL.

```
<H3C> system-view
[H3C] acl number 2030 match-order config
[H3C-acl-basic-2030] rule 1 permit source 10.110.100.46 0
[H3C-acl-basic-2030] rule 2 deny source any
```

Apply the ACL to only permit the Web users sourced from the IP address of 10.110.100.46 to access the switch.

```
[H3C] ip http acl 2030
```

Table of Contents

Chapter 1 Configuration File Management 1-1
1.1 Introduction to Configuration File 1-1
1.2 Configuration File-Related Operations 1-1

Chapter 1 Configuration File Management

1.1 Introduction to Configuration File

A configuration file records and stores user configurations performed to a switch. It also enables users to check switch configurations easily.

Upon powered on, a switch loads the configuration file known as saved-configuration file, which resides in the Flash, for initialization. If the Flash contains no configuration file, the system performs initialization using the default settings. Comparing to saved-configuration file, the configuration file which is currently adopted by a switch is known as the current-configuration.

A configuration file conforms to the following conventions:

- The content of a configuration file is a series of commands.
- Only the non-default configuration parameters are saved.
- The commands are grouped into sections by command view. The commands that are of the same command view are grouped into one section. Sections are separated by empty lines or comment lines. (A line is a comment line if it starts with the character “#”.)
- The sections are listed in this order: system configuration section, physical port configuration section, logical interface configuration section, routing protocol configuration section, and so on.
- A configuration file ends with a “return”.

1.2 Configuration File-Related Operations

You can perform the following operations on an S3600 Ethernet switch:

- Saving the current configuration to a configuration file
- Removing a configuration file from the Flash
- Checking/Setting the configuration file to be used when the switch starts the next time
- Setting a configuration file to be the primary/secondary configuration file

Perform the following configuration in user view.

Table 1-1 Configure a configuration file

Operation	Command	Description
Save the current configuration to a specified configuration file and specify the configuration file to be the primary/secondary configuration file	**save** [*cfgfile* | [**safely**] [**backup** | **main**]]	Optional The **save** command can be executed in any view.
Remove a specific configuration file from the Flash	**reset saved-configuration** [**backup** | **main**]	Optional
Specify the name and attribute of the configuration file to be used in the next startup	**startup saved-configuration** *cfgfile* [**backup** | **main**]	Optional By default, the switch uses the main configuration file in the next startup.
Specify that the switch starts without loading the configuration file	**undo startup saved-configuration** [**unit** *unit-id*]	Optional
Display the primary configuration file	**display saved-configuration** [**unit** *unit-id*] [**by-linenum**]	Optional The **display** command can be executed in any view.
Display the current configuration	**display current-configuration** [**configuration** [*configuration-type*] | **interface** [*interface-type*] [*interface-number*] | **vlan** [*vlan-id*]] [**by-linenum**] [**|** { **begin** | **include** | **exclude** } *regular-expression*]	
Display the configuration performed in the current view	**display this** [**by-linenum**]	
Display the information about the configuration file to be used for startup.	**display startup** [**unit** *unit-id*]	

Caution:

Currently, the extension of a configuration file is cfg. Configuration files are saved in the root directory of the Flash.

In the following conditions, it may be necessary for you to remove the configuration files from the Flash:

- The system software does not match the configuration file after the software of the Ethernet switch is updated.
- The configuration files in the Flash are damaged. The common reason is that wrong configuration files are loaded.

You can save the current configuration files in one of the following two ways:

- If the **safely** keyword is not provided, the system saves the configuration files in the fast mode. In this mode, the configuration files are saved fast. However, the configuration files will be lost if the device is restarted or the power is off when the configuration files are being saved.
- If the **safely** keyword is provided, the system saves the configuration files in the safe mode. In this mode, the configuration files are saved slowly. However, the configuration files will be saved in the Flash if the device is restarted or the power is off when the configuration files are being saved.

You are recommended to adopt the fast saving mode in the conditions of stable power and adopt the safe mode in the conditions of unstable power or remote maintenance.

Note:

- You are recommended to use the **save** command to save the configuration before restarting a device, so that the current configuration remains after the device is restarted.
- If you use the **save** command to save the current configuration file without specifying any option, the configuration file is saved as the name of the configuration file used in this start. If the device is started using the default configuration file this time, the current configuration file is saved as the name of the default configuration file.
- If you use the **save** command after a fabric is formed on the switch, the units in the fabric save their own startup configuration files automatically.

Table of Contents

Chapter 1 VLAN Overview 1-1
1.1 VLAN Overview 1-1
1.1.1 Introduction to VLAN 1-1
1.1.2 VLAN Principles 1-2
1.2 Port-Based VLAN 1-3
1.3 Protocol-Based VLAN 1-3
1.3.1 Introduction to Protocol-Based VLAN 1-3
1.3.2 Encapsulation Format of Ethernet Data 1-3
1.3.3 Procedure for the Switch to Judge Packet Protocol 1-6
1.3.4 Encapsulation Formats 1-6
1.3.5 Implementation of Protocol-Based VLAN 1-7
Chapter 2 VLAN Configuration 2-1
2.1 VLAN Configuration 2-1
2.1.1 Basic VLAN Configuration 2-1
2.1.2 Basic VLAN Interface Configuration 2-1
2.1.3 Displaying VLAN Configuration 2-2
2.2 Configuring a Port-Based VLAN 2-3
2.2.1 Configuring a Port-Based VLAN 2-3
2.2.2 Protocol-Based VLAN Configuration Example 2-3
2.3 Configuring a Protocol-Based VLAN 2-4
2.3.1 Creating Protocol Template for Protocol-Based VLAN 2-4
2.3.2 Associating a Port with the Protocol-Based VLAN 2-5
2.3.3 Displaying Protocol-Based VLAN Configuration 2-6
2.3.4 Protocol-Based VLAN Configuration Example 2-6

Chapter 1 VLAN Overview

1.1 VLAN Overview

1.1.1 Introduction to VLAN

The traditional Ethernet is a broadcast network, where all hosts are in the same broadcast domain and connected with each other through hubs or switches. The hub is a physical layer device without the switching function, so it forwards the received packet to all ports. The switch is a link layer device which can forward the packet according to the MAC address of the packet. However, when the switch receives a broadcast packet or an unknown unicast packet whose MAC address is not included in the MAC address table of the switch, it will forward the packet to all the ports except the inbound port of the packet. In this case, a host in the network receives a lot of packets whose destination is not the host itself. Thus, plenty of bandwidth resources are wasted, causing potential serious security problems.

The traditional way to isolate broadcast domains is to use routers. However, routers are expensive and provide few ports, so they cannot subnet the network particularly.

The virtual local area network (VLAN) technology is developed for switches to control broadcast in LANs.

By creating VLANs in a physical LAN, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own. Hosts in the same VLAN communicate with each other as if they are in a LAN. However, hosts in different VLANs cannot communicate with each other directly. Figure 1-1 illustrates a VLAN implementation.

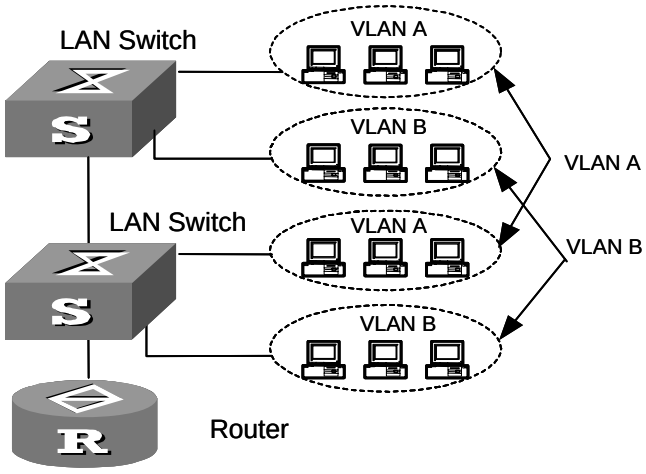


Figure 1-1 A VLAN implementation

A VLAN can span across multiple switches, or even routers. This enables hosts in a VLAN to be dispersed in a looser way. That is, hosts in a VLAN can belong to different physical network segment.

Compared with the traditional Ethernet, VLAN enjoys the following advantages.

- Broadcasts are confined to VLANs. This decreases bandwidth utilization and improves network performance.
- Network security is improved. VLANs cannot communicate with each other directly. That is, a host in a VLAN cannot access resources in another VLAN directly, unless routers or Layer 3 switches are used.
- Network configuration workload for the host is reduced. VLAN can be used to group specific hosts. When the physical position of a host changes within the range of the VLAN, you need not change its network configuration.

1.1.2 VLAN Principles

VLAN tags in the packets are necessary for the switch to identify packets of different VLANs. The switch works at Layer 2 (Layer 3 switches are not discussed in this chapter) and it can identify the data link layer encapsulation of the packet only, so you can add the VLAN tag field into only the data link layer encapsulation if necessary.

In 1999, IEEE issues the IEEE 802.1Q protocol to standardize VLAN implementation, defining the structure of VLAN-tagged packets.

In traditional Ethernet data frames, the type field of the upper layer protocol is encapsulated after the destination MAC address and source MAC address, as shown in Figure 1-2



Figure 1-2 Encapsulation format of traditional Ethernet frames

In Figure 1-2 DA refers to the destination MAC address, SA refers to the source MAC address, and Type refers to the protocol type of the packet. IEEE 802.1Q protocol defines that a 4-byte VLAN tag is encapsulated after the destination MAC address and source MAC address to show the information about VLAN.

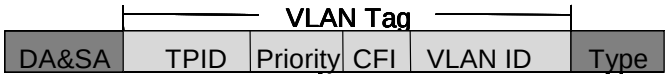


Figure 1-3 Format of VLAN tag

As shown in Figure 1-3, a VLAN tag contains four fields, including TPID, priority, CFI, and VLAN ID.

- TPID is a 16-bit field, indicating that this data frame is VLAN-tagged. By default, it is 0x8100 in H3C series Ethernet switches.

- Priority is a 3-bit field, referring to 802.1p priority. Refer to section “QoS & QoS profile” for details.
- CFI is a 1-bit field, indicating whether the MAC address is encapsulated in the standard format in different transmission media. This field is not described in detail in this chapter.
- VLAN ID is a 12-bit field, indicating the ID of the VLAN to which this packet belongs. It is in the range of 0 to 4,095. Generally, 0 and 4,095 is not used, so the field is in the range of 1 to 4,094.

VLAN ID identifies the VLAN to which a packet belongs. When the switch receives a packet carrying no VLAN tag, it will encapsulate a VLAN tag with the default VLAN ID of the inbound port for the packet, and the packet will be assigned to the default VLAN of the inbound port for transmission. For the details about setting the default VLAN of a port, refer to section “Port Basic Configuration” in *H3C S3600 Series Ethernet Switches Operation Manual*.

1.2 Port-Based VLAN

Port-based VLAN technology introduces the simplest way to classify VLANs. You can isolate the hosts and divide them into different virtual workgroups through assigning the ports on the device connecting to hosts to different VLANs.

This way is easy to implement and manage and it is applicable to hosts with relatively fixed positions.

1.3 Protocol-Based VLAN

1.3.1 Introduction to Protocol-Based VLAN

Protocol-based VLAN is also known as protocol VLAN, which is another way to classify VLANs besides port-based VLAN. Through the protocol-based VLANs, the switch can analyze the received packets carrying no VLAN tag on the port and match the packets with the user-defined protocol template automatically according to different encapsulation formats and the values of the special fields. If a packet is matched, the switch will add a corresponding VLAN tag to it automatically. Thus, the data of the specific protocol is assigned automatically to the corresponding VLAN for transmission.

This feature is used for binding the ToS provided in the network to VLAN to facilitate management and maintenance.

1.3.2 Encapsulation Format of Ethernet Data

This section introduces the common encapsulation formats of Ethernet data for you to understand well the procedure for the switch to identify the packet protocols.

I. Ethernet II and 802.2/802.3 encapsulation

In the link layer, there are two main packet encapsulation types: Ethernet II and 802.2/802.3, whose encapsulation formats are described in the following figures.

Ethernet II packet:



Figure 1-4 Ethernet II encapsulation format

802.2/802.3 packet:

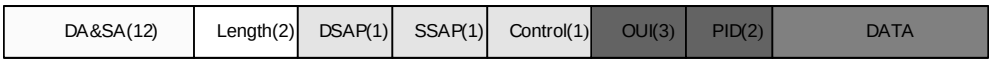


Figure 1-5 802.2/802.3 encapsulation format

In the two figures, DA and SA refer to the destination MAC address and source MAC address of the packet respectively. The number in the bracket indicates the field length in bits.

The maximum length of an Ethernet packet is 1500 bytes, that is, 5DC in hexadecimal, so the length field in 802.2/802.3 encapsulation is in the range of 0x0000 to 0x05DC.

Whereas, the type field in Ethernet II encapsulation is in the range of 0x0600 to 0xFFFF.

Notes:

Presently, H3C S3600 series switches recognize packets with the value of the type field being in the range 0x05DD to 0x05FF as 802.2/802.3 encapsulated packets.

The switch identifies whether a packet is an Ethernet II packet or an 802.2/802.3 packet according to the ranges of the two fields.

II. Encapsulation formats of 802.2/802.3 packets

802.2/802.3 packets are encapsulated in the following three formats:

- 802.3 raw encapsulation: only the length field is encapsulated after the source and destination address field, followed by the upper layer data. The type field is not included.



Figure 1-6 802.3 raw encapsulation format

Only the IPX protocol supports 802.3 raw encapsulation format currently. This format is identified by the two bytes whose value is 0xFFFF after the length field.

- 802.2 logical link control (LLC) encapsulation: the length field, the destination service access point (DSAP) field, the source service access point (SSAP) field and the control field are encapsulated after the source and destination address field.

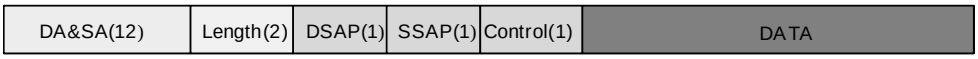


Figure 1-7 802.2 LLC encapsulation format

The DSAP field and the SSAP field in the LLC part are used to identify the upper layer protocol. For example, the two fields are both 0xE0, meaning that the upper layer protocol is IPX protocol.

- 802.2 sub-network access protocol (SNAP) encapsulation: the length field, the DSAP filed, the SSAP field, the control field, the OUI field and the PID field are encapsulated according to 802.2/802.3 packets.



Figure 1-8 802.2 SNAP encapsulation format

In 802.2 SNAP encapsulation format, the values of the DSAP field and the SSAP field are always AA, and the value of the control field is always 3.

The switch differentiates between 802.2 LLC encapsulation and 802.2 SNAP encapsulation according to the values of the DSAP field and the SSAP field.

Note:

When the OUI is 00-00-00 in 802.2 SNAP encapsulation, the PID field has the same meaning as the type field in Ethernet II encapsulation, which both refer to globally unique protocol number. Such encapsulation is also known as SNAP RFC1042 encapsulation, which is standard SNAP encapsulation. The SNAP encapsulation mentioned in this chapter refers to SNAP RFC 1042 encapsulation.

1.3.3 Procedure for the Switch to Judge Packet Protocol

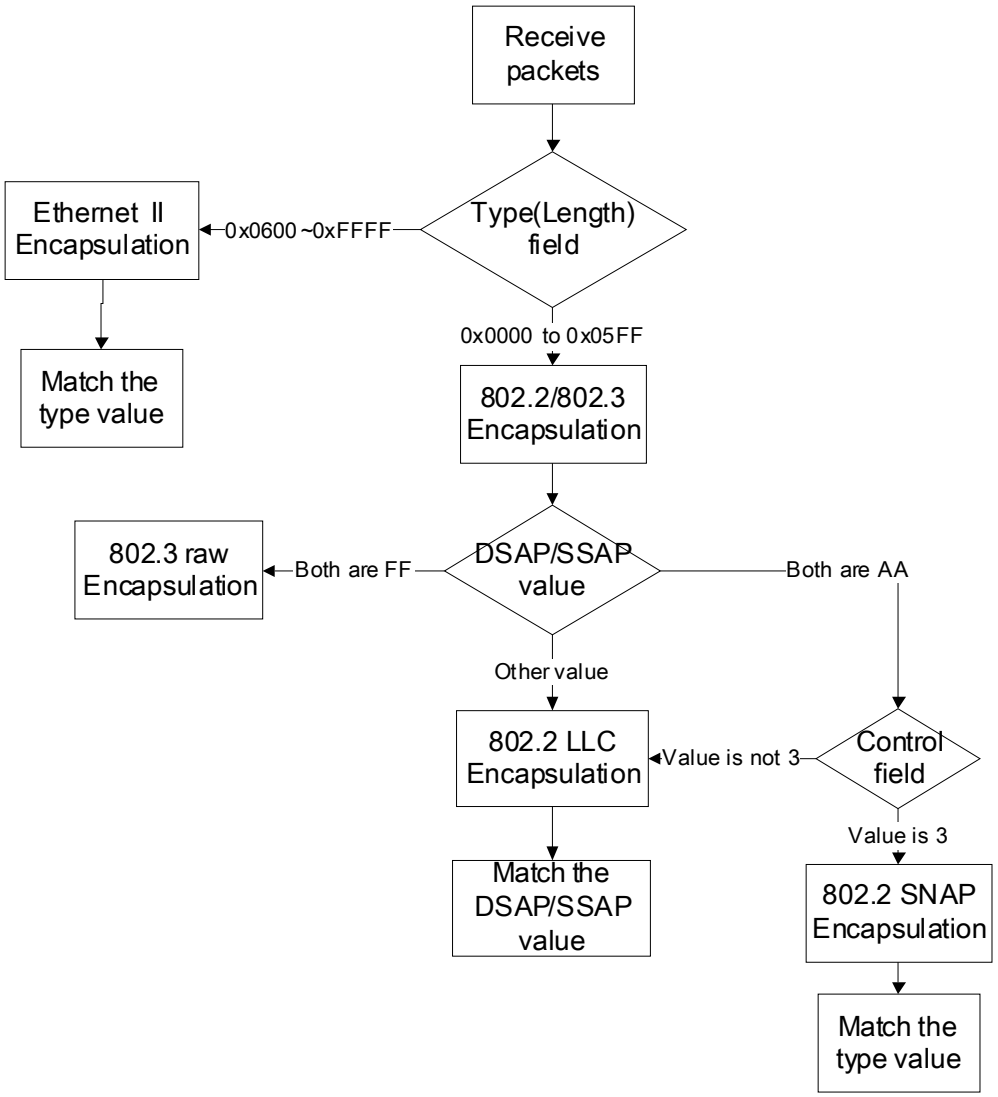


Figure 1-9 Procedure for the switch to judge packet protocol

1.3.4 Encapsulation Formats

Table 1-1 Encapsulation formats

Encapsulation / Protocol	Ethernet II	802.3 raw	802.2 LLC	802.2 SNAP	Type value
IP	Supported	Not supported	Not supported	Supported	0x0800
IPX	Supported	Supported	Supported	Supported	0x8137

Encapsulation / Protocol	Ethernet II	802.3 raw	802.2 LLC	802.2 SNAP	Type value
AppleTalk	Supported	Not supported	Not supported	Supported	0x809B

1.3.5 Implementation of Protocol-Based VLAN

S3600 series Ethernet switches assign the packet to the specific VLAN by matching the packet with the protocol template.

The protocol template is the standard to determine the protocol to which a packet belongs. Protocol templates include standard templates and user-defined templates:

- The standard template adopts the RFC-defined packet encapsulation formats and values of some specific fields as the matching criteria.
- The user-defined template adopts the user-defined encapsulation formats and values of some specific fields as the matching criteria.

After configuring the protocol template, you must add a port to the protocol-based VLAN and associate this port with the protocol template. This port will add VLAN tags to the packets based on protocol types. The port in the protocol-based VLAN must be connected to a client. However, a common client cannot process VLAN-tagged packets. In order that the client can process the packets out of this port, you must configure the port in the protocol-based VLAN as a hybrid port and configure the port to remove VLAN tags when forwarding packets of all VLANs.

Note:

For the operation of removing VLAN tags when the hybrid port sends packets, refer to the section “Port Basic Configuration” in this manual.

Chapter 2 VLAN Configuration

2.1 VLAN Configuration

2.1.1 Basic VLAN Configuration

Table 2-1 Basic VLAN configuration

Operation	Command	Description
Enter system view	**system-view**	—
Create multiple VLANs in batch	**vlan** { *vlan-id1* **to** *vlan-id2* | **all** }	Optional
Create a VLAN and enter VLAN view	**vlan** *vlan-id*	Required The *vlan-id* argument ranges from 1 to 4,094.
Assign a name for the current VLAN	**name** *text*	Optional By default, the name of a VLAN is its VLAN ID.
Specify the description string of the current VLAN	**description** *text*	Optional By default, the description string of a VLAN is its VLAN ID.

Caution:

When you use the **vlan** command to create VLANs, if the destination VLAN is an existing dynamic VLAN, it will be transformed into a static VLAN and the switch will output the prompt information.

2.1.2 Basic VLAN Interface Configuration

I. Configuration prerequisites

Create a VLAN before configuring a VLAN interface.

II. Configuration procedure

Table 2-2 Basic VLAN interface configuration

Operation	Command	Description
Enter system view	**system-view**	—
Create a VLAN interface and enter VLAN interface view	**interface Vlan-interface** *vlan-id*	Required The *vlan-id* argument ranges from 1 to 4,094.
Specify the description string for the current VLAN interface	**description** *text*	Optional By default, the description string of a VLAN interface is the name of this VLAN interface
Disable the VLAN interface	**shutdown**	Optional
Enable the VLAN Interface	**undo shutdown**	Optional

Note that the operation of enabling/disabling a VLAN interface does not influence the enabling/disabling states of the Ethernet ports belonging to this VLAN.

By default, the VLAN interface's management state is enabled. In this case, the physical state of the VLAN interface is affected by the ports state in the VLAN. When all the Ethernet ports of a VLAN are down, the VLAN interface of the VLAN is down, that is, the VLAN interface is disabled; when one or more Ethernet ports of a VLAN are up, the VLAN interface of the VLAN is up, that is, the VLAN interface is enabled.

If you disable the VLAN interface's management state, the VLAN interface will always be down, regardless of the states of the ports in the VLAN.

2.1.3 Displaying VLAN Configuration

After the configuration above, you can execute the **display** command in any view to display the running status after the configuration, so as to verify the configuration.

Table 2-3 Display VLAN configuration

Operation	Command	Description
Display the VLAN interface information	**display interface Vlan-interface** [*vlan-id*]	You can execute the **display** command in any view.
Display the VLAN information	**display vlan** [*vlan-id* [**to** *vlan-id*] | **all** | **dynamic** | **static**]	

2.2 Configuring a Port-Based VLAN

2.2.1 Configuring a Port-Based VLAN

I. Configuration prerequisites

Create a VLAN before configuring a port-based VLAN.

II. Configuration procedure

Table 2-4 Configure a port-based VLAN

Operation	Command	Description
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	—
Add Ethernet ports to the specific VLAN	**port** *interface-list*	Required By default, all the ports belong to the default VLAN

Caution:

The commands above are effective for access ports only. If you want to add trunk ports or hybrid ports to a VLAN, you can use the **port trunk permit vlan** command or the **port hybrid vlan** command in Ethernet port view. For the configuration procedure, refer to the section "Port Basic Configuration – Operation" in *H3C S3600 Series Ethernet Switches Operation Manual*.

2.2.2 Protocol-Based VLAN Configuration Example

I. Network requirements

- Create VLAN 2 and VLAN 3 and specify the description string of VLAN 2 as home;
- Add Ethernet1/0/1 and Ethernet1/0/2 to VLAN 2 and add Ethernet1/0/3 and Ethernet1/0/4 to VLAN 3.

II. Network diagram

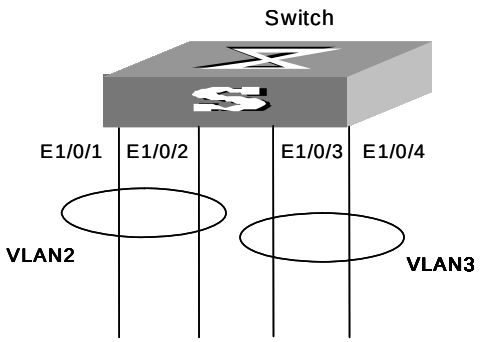


Figure 2-1 Network diagram for VLAN configuration

III. Configuration procedure

Create VLAN 2 and enter its view.

```
<H3C> system-view
[H3C] vlan 2
```

Specify the description string of VLAN 2 as home.

```
[H3C-vlan2] description home
```

Add Ethernet1/0/1 and Ethernet1/0/2 ports to VLAN 2.

```
[H3C-vlan2] port Ethernet 1/0/1 Ethernet 1/0/2
```

Create VLAN 3 and enter its view.

```
[H3C-vlan2] vlan 3
```

Add Ethernet1/0/3 and Ethernet1/0/4 ports to VLAN 3.

```
[H3C-vlan3] port Ethernet 1/0/3 Ethernet 1/0/4
```

2.3 Configuring a Protocol-Based VLAN

2.3.1 Creating Protocol Template for Protocol-Based VLAN

I. Configuration prerequisites

Create a VLAN before configuring a protocol-based VLAN.

II. Configuration procedure

Table 2-5 Create protocol types of VLANs

Operation	Command	Description
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	Required

Operation	Command	Description
Create the protocol template for the VLAN	**protocol-vlan** [*protocol-index*] { **at** | **ip** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* **ssap** *ssap-id* } | **snap etype** *etype-id* } }	Required

When you are creating protocol templates for protocol-based VLANs, the **at**, **ip** and **ipx** keywords are used to create standard templates, and the **mode** keyword is used to create user-defined templates.

Caution:

- Because the IP protocol is closely associated with the ARP protocol, you are recommended to configure the ARP protocol type when configuring the IP protocol type and associate the two protocol types with the same port, in case that ARP packets and IP packets are not assigned to the same VLAN, which will cause IP address resolution failure.
- The **mode llc dsap** *ff* **ssap** *ff* and **ipx raw** keywords match the same type of packets, the **ipx raw** keyword takes precedence over the **mode llc dsap** *ff* **ssap** *ff* keyword, and a packet will not be further matched if it does not match the **ipx raw** keyword, therefore, the **protocol-vlan mode llc dsap** *ff* **ssap** *ff* command takes no effect.
- Packet encapsulation type is **snap**, instead of **llc**, if the values of the *dsap-id* and *ssap-id* arguments are both AA.
- When you use the **mode** keyword to configure protocol-based VLANs, if you set the *etype-id* argument to 0x0800, 0x809b, or 0x8137 for Ethernet II or SNAP packets, the matched packets have the same format as that of IP, IPX, and AppleTalk packets respectively. In order that the two commands do not configure the same protocol repetitively, the switch will prompt that you cannot specify the *etype-id* argument of Ethernet II and SNAP packets to 0x0800, 0x089b, or 0x8137.

2.3.2 Associating a Port with the Protocol-Based VLAN

I. Configuration prerequisites

- The protocol template for the protocol-based VLAN is created
- The port is configured as a hybrid port, and the port is configured to remove VLAN tags when it forwards the packets of the protocol-based VLANs.

II. Configuration procedure

Table 2-6 Associate a port with the protocol-based VLAN

Operation	Command	Description
Enter system view	**system-view**	—
Enter port view	**interface** *interface-type interface-number*	Required
Associate a port with the protocol-based VLAN	**port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }	Required

Caution:

For the operation of adding a hybrid port to the VLAN, refer to the section “Port Basic Configuration” in this manual.

2.3.3 Displaying Protocol-Based VLAN Configuration

After the configuration above, you can execute the **display** command in any view to display the running status, so as to verify the configuration.

Table 2-7 Display VLAN configuration

Operation	Command	Description
Display the information about the protocol-based VLAN	**display vlan** [*vlan-id* [**to** *vlan-id*] | **all** | **static** | **dynamic**]	You cam execute the **display** command in any view
Display the protocol information and protocol indexes configured on the specified VLAN	**display protocol-vlan vlan** { *vlan-id* [**to** *vlan-id*] | **all** }	
Display the protocol information and protocol indexes configured on the specified port	**display protocol-vlan interface** { *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

2.3.4 Protocol-Based VLAN Configuration Example

I. Standard-template-based protocol VLAN configuration example

1) Network requirements

- Create VLAN 5 and configure it to be a protocol-based VLAN, with the protocol-index being 1 and the protocol being IP.
- Associate Ethernet1/0/5 port with the protocol-based VLAN to enable IP packets received by this port to be tagged with the tag of VLAN 5 and be transmitted in VLAN 5.

2) Configuration procedure

Create VLAN 5 and enter its view.

```
<H3C> system-view
[H3C] vlan 5
[H3C-vlan5]
```

Configure the protocol-index to be 1, and the associated protocol to be IP.

```
[H3C-vlan5] protocol-vlan 1 ip
```

Enter Ethernet1/0/5 port view.

```
[H3C-vlan5] interface Ethernet 1/0/5
```

Configure the port to be a hybrid port.

```
[H3C-Ethernet1/0/5] port link-type hybrid
```

Add the port to VLAN 5 and add VLAN 5 to the untagged VLAN list of the port.

```
[H3C-Ethernet1/0/5] port hybrid vlan 5 untagged
```

Associate the port with protocol-index 1.

```
[H3C-Ethernet1/0/5] port hybrid protocol-vlan vlan 5 1
```

II. User-defined-template-based protocol VLAN configuration example

1) Network requirement

- Create VLAN 7 and configure it as a protocol-based VLAN.
- Create two indexes in VLAN 7. Index 1 is used to match the packets with DSAP and SSAP value being 01 and ac respectively in 802.2 LLC encapsulation; Index 2 is used to match the packets with the type value being 0xabcd in 802.2 SNAP encapsulation.
- Associate Ethernet1/0/7 port with the two indexes of the protocol-based VLAN 7 to enable IP packets matching one of the indexes received by this port to be tagged with the tag of VLAN 7.

2) Configuration procedure

Create VLAN 7 and enter its view.

```
<H3C> system-view
[H3C] vlan 7
[H3C-vlan7]
```

Configure index 1 of VLAN 7 according to the network requirement.

```
[H3C-vlan7] protocol-vlan 1 mode llc dsap 01 ssap ac
```

Configure index 2 of VLAN 7 according to the network requirement.

```
[H3C-vlan7] protocol-vlan 2 mode snap etype abcd
```

Enter port view of the Ethernet1/0/7.

```
[H3C-vlan7] interface Ethernet 1/0/7
```

configure the port as a hybird port.

```
[H3C-Ethernet1/0/7] port link-type hybrid
```

Add the port to VLAN 7, and add VLAN 7 to the list of untagged VLANs permitted to pass through the port.

```
[H3C-Ethernet1/0/7] port hybrid vlan 7 untagged
```

Associate the port with the two indexes of VLAN 7.

```
[H3C-Ethernet1/0/7] port hybrid protocol-vlan vlan 7 1 to 2
```

Table of Contents

Chapter 1 IP Address Configuration 1-1
1.1 IP Address Overview 1-1
1.1.1 IP Address Classification and Representation 1-1
1.1.2 Subnet and Mask 1-3
1.2 Configuring an IP Address 1-3
1.3 Configuring an IP Address for a VLAN Interface 1-4
1.4 Displaying IP Address Configuration 1-4
1.5 IP Address Configuration Example 1-5
1.6 Troubleshooting 1-5
Chapter 2 IP Performance Configuration 2-1
2.1 IP Performance Configuration 2-1
2.1.1 Introduction to IP Performance Configuration 2-1
2.1.2 Introduction to FIB 2-1
2.1.3 TCP Attributes Configuration 2-1
2.1.4 Subnet-Directed Broadcast Suppression Configuration 2-2
2.2 Displaying and Maintaining IP Performance 2-2
2.3 Troubleshooting 2-4

Chapter 1 IP Address Configuration

1.1 IP Address Overview

1.1.1 IP Address Classification and Representation

An IP address is a 32-bit address allocated to a device connected to the Internet. It consists of two fields: net-id and host-id. To facilitate IP address management, IP addresses are divided into five classes, as shown in Figure 1-1.

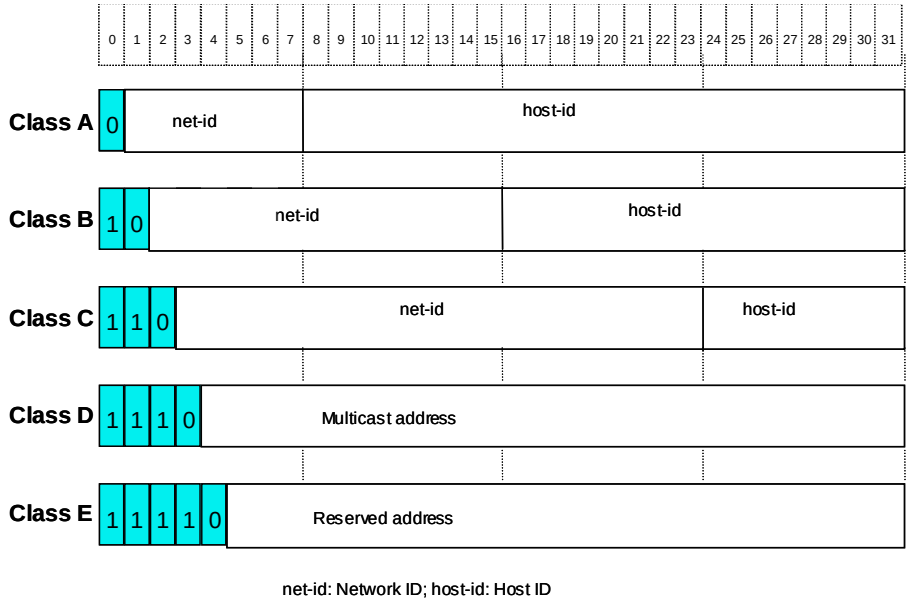


Figure 1-1 Five classes of IP addresses

Class A, Class B, and Class C IP addresses are unicast addresses. Class D IP addresses are multicast addresses and Class E addresses are reserved for future special use. The first three types are commonly used.

IP addresses are in the dotted decimal notation. Each IP address contains four decimal integers, with each integer corresponding to one byte (for example,10.110.50.101).

Some IP addresses are reserved for special use. The IP address ranges that can be used by users are listed in Table 1-1.

Table 1-1 Classes and ranges of IP addresses

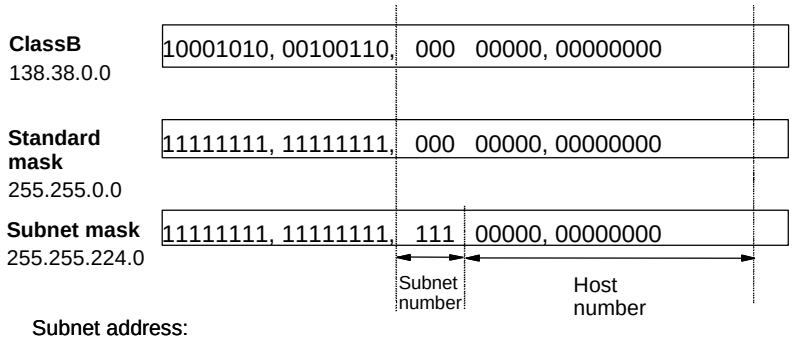
Network type	Address range	IP network range available for users	Description
A	0.0.0.0 to 127.255.255.255	1.0.0.0 to 126.0.0.0	• An IP address with all 0s host ID is a network address and is used for network routing. • An IP address with all 1s host ID is a broadcast address and is used for broadcast to all hosts on the network. • The IP address 0.0.0.0 is used by hosts when they are booted but is not used afterward. • An IP address with all 0s network ID represents a specific host on the local network and can be used as a source address but cannot be used as a destination address. • All the IP addresses in the format of 127.X.Y.Z are reserved for loopback test and the packets sent to these addresses will not be output to lines; instead, they are processed internally and regarded as incoming packets.
B	128.0.0.0 to 191.255.255.255	128.0.0.0 to 191.254.0.0	• An IP address with all 0s host ID is a network address and is used for network routing. • An IP address with all 1s host ID is a broadcast address and is used for broadcast to all hosts on the network.
C	192.0.0.0 to 223.255.255.255	192.0.0.0 to 223.255.254.0	• An IP address with all 0s host ID is a network address and is used for network routing. • An IP address with all 1s host ID is a broadcast address and is used for broadcast to all hosts on the network.
D	224.0.0.0 to 239.255.255.255	None	Class D addresses are multicast addresses.
E	240.0.0.0 to 255.255.255.254	None	These IP addresses are reserved for future use.
Others	255.255.255.255	255.255.255.255	255.255.255.255 is used as a LAN broadcast address.

1.1.2 Subnet and Mask

The traditional IP address classification method wastes IP addresses greatly. In order to make full use of the available IP addresses, the concepts of mask and subnet were introduced.

A mask is a 32-bit number corresponding to an IP address. The number consists of 1s and 0s. These 1s and 0s can be arbitrarily combined in principle. However, a mask is usually defined as follows: the bits of the network number and subnet number are set to 1, and the bits of the host number are set to 0. The mask divides the IP address into two parts: subnet address and host address. In an IP address, the part corresponding to the "1" bits in the mask is the subnet address, and the part corresponding to the remaining "0" bits in the mask is the host address. If there is no subnet division, the subnet mask uses the default value. In this case, the length of 1s in the mask is equal to the net-id length. Therefore, for IP addresses of classes A, B and C, the default values of the corresponding subnet masks 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 (see Figure 1-2). Each subnet can contain more than 8000 hosts.



Subnet address:

000	Subnet address: 138.38. 0. 0
001	Subnet address: 138.38. 32. 0
010	Subnet address: 138.38. 64. 0
011	Subnet address: 138.38. 96. 0
100	Subnet address: 138.38.128. 0
101	Subnet address: 138.38.160. 0
110	Subnet address: 138.38.192. 0
111	Subnet address: 138.38.224. 0

Figure 1-2 Subnet division of the IP address

1.2 Configuring an IP Address

For a VLAN interface, an IP address can be obtained in one of the three ways:

- Manually configured by using the IP address configuration command
- Allocated by the BOOTP server
- Allocated by the DHCP server

The three methods are mutually exclusive and the use of a new method will result in the IP address obtained by the old method being released. For example, if you obtain an IP address by using the IP address configuration command, and then use the **ip address bootp-alloc** command to apply for an IP address, the originally configured IP address is deleted and a new IP address will be allocated by BOOTP for the VLAN interface.

This chapter only introduces how to configure an IP address with the IP address configuration command. For the other two methods, refer to the “Management VLAN Configuration” module.

1.3 Configuring an IP Address for a VLAN Interface

Generally, it is enough to configure one IP address for a VLAN interface. However, you can configure up to five IP addresses for a VLAN interface so that the interface can be connected to several subnets. Among these IP addresses, one is the primary IP address and the others are secondary ones.

Table 1-2 Configure an IP address for a VLAN interface

Operation	Command	Description
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Configure an IP address for a VLAN interface	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	Required By default, a VLAN interface has no IP address. After an IP address is assigned to the VLAN interface through BOOTP or DHCP, you cannot configure a secondary IP address for the VLAN interface.

1.4 Displaying IP Address Configuration

After the above configuration, you can execute the **display** command in any view to display the operating status and configuration on the interface to verify your configuration.

Table 1-3 Display IP address configuration

Operation	Command	Description
Display VLAN interface information	**display ip interface** [**brief** [*interface-type* [*interface-number*]] | [*interface-type interface-number*]]	You can execute the **display** command in any view.

1.5 IP Address Configuration Example

I. Network requirements

Set the IP address and subnet mask of VLAN-interface1 to 129.2.2.1 and 255.255.255.0 respectively.

II. Network diagram

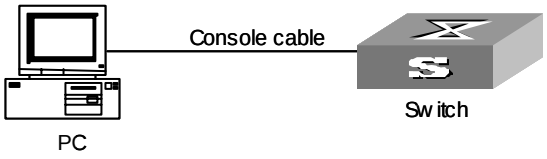


Figure 1-3 IP address configuration

III. Configuration procedure

Configure an IP address for VLAN-interface1.

```
<H3C> system-view
[H3C] interface Vlan-interface 1
[H3C-Vlan-interface1] ip address 129.2.2.1 255.255.255.0
```

1.6 Troubleshooting

Symptom: The switch cannot ping the host directly-connected to a port.

Solution: You can perform troubleshooting as follows:

- Check the configuration of the switch, and then use the **display arp** command to check whether the host has an corresponding ARP entry in the ARP table maintained by the Switch.
- Check the VLAN that includes the switch port connecting the host. Check whether the VLAN has been configured with the VLAN interface. Then check whether the IP addresses of the VLAN interface and the host are on the same network segment.

- If the configuration is correct, enable ARP debugging on the switch, and check whether the switch can correctly send and receive ARP packets. If it can only send but cannot receive ARP packets, errors may occur at the Ethernet physical layer.

Chapter 2 IP Performance Configuration

2.1 IP Performance Configuration

2.1.1 Introduction to IP Performance Configuration

IP performance configuration mainly refers to TCP attribute configuration. The TCP attributes that can be configured include:

- synwait timer: This timer is started when TCP sends a syn packet. If no response packet is received before the timer times out, the TCP connection will be terminated. The timeout time of the synwait timer ranges from 2 to 600 seconds and is 75 seconds by default.
- finwait timer: This timer is started when the TCP connection turns from the FIN_WAIT_1 state to the FIN_WAIT_2 state. If no FIN packet is received before the timer times out, the TCP connection will be terminated. The timeout time of the finwait timer ranges from 76 to 3,600 seconds and is 675 seconds by default.
- The connection-oriented socket receive/send buffer size ranges from 1 to 32 KB and is 8 KB by default.

2.1.2 Introduction to FIB

Every switch stores a forwarding information base (FIB). FIB is used to store the forwarding information of the switch and guide Layer 3 packet forwarding.

You can know the forwarding information of the switch through the FIB table. Each FIB entry includes: destination address/mask length, next hop, current flag, timestamp, and outbound interface.

When the switch is running normally, the contents of the FIB and the routing table are the same. For routing and routing tables, refer to the “Routing Protocol” module of this manual.

2.1.3 TCP Attributes Configuration

Table 2-1 Configure TCP attributes

Operation	Command	Description
Enter system view	**system-view**	—
Configure timeout time for the synwait timer in TCP	**tcp timer syn-timeout** *time-value*	Required By default, the timeout time of the TCP synwait timer is 75 seconds.

Operation	Command	Description
Configure timeout time for the finwait timer in TCP	**tcp timer fin-timeout** *time-value*	Required By default, the timeout time of the TCP finwait timer is 675 seconds.
Configure the socket receive/send buffer size of TCP	**tcp window** *window-size*	Required By default, the receive/send buffer size is 8 KB.

2.1.4 Subnet-Directed Broadcast Suppression Configuration

Broadcast packets include the general broadcast packets and the subnet-directed broadcast packets. For a subnet-directed broadcast packet, its destination IP address is a sub network address, but its source IP address is not in this sub network segment.

You can perform the following configuration to determine whether to receive the subnet-directed broadcast packets.

Table 2-2 Configure to receive subnet-directed broadcast packets

Operation	Command	Description
Enter system view	**system-view**	—
Receive subnet-directed broadcast packets	**ip forward-broadcast**	Optional By default, the subnet-directed packets will be suppressed.

2.2 Displaying and Maintaining IP Performance

After the above configurations, you can execute the **display** command in any view to display the running status to verify your IP performance configuration.

Table 2-3 Display IP performance

Operation	Command	Description
Display TCP connection status	**display tcp status**	You can execute the **display** command in any view.
Display TCP connection statistics	**display tcp statistics**	
Display UDP traffic statistics	**display udp statistics**	
Display IP traffic statistics	**display ip statistics**	
Display ICMP traffic statistics	**display icmp statistics**	
Display the current socket information of the system	**display ip socket** [**socktype** *sock-type*] [*task-id socket-id*]	
Display the forwarding information base (FIB) entries	**display fib**	
Display the FIB entries matching the destination IP address	**display fib** *ip_address1* [{ *mask1* | *mask-length1* } [*ip_address2* { *mask2* | *mask-length2* } | **longer**] | **longer**]	
Display the FIB entries filtering through a specific ACL	**display fib acl** *number*	
Display the FIB entries in the buffer which begin with, include or exclude the specified character string.	**display fib** | { **begin** | **include** | **exclude** } *text*	
Display the FIB entries filtering through a specific prefix list	**display fib ip-prefix** *listname*	
Display the total number of the FIB entries	**display fib statistics**	

Use the **reset** command in user view to clear the IP, TCP, and UDP traffic statistics.

Table 2-4 Maintain IP performance

Configuration	Command	Description
Clear IP traffic statistics	**reset ip statistics**	You can execute the **reset** command in user view.
Clear TCP traffic statistics	**reset tcp statistics**	
Clear UDP traffic statistics	**reset udp statistics**	

2.3 Troubleshooting

Symptom: IP packets are forwarded normally, but TCP and UDP cannot work normally.

Solution: Enable the corresponding debugging information output to view the debugging information.

- Use the **display** command to display the IP performance and check whether the PC runs normally.
- Use the **terminal debugging** command to enable debugging information to be output to the console.
- Use the **debugging udp packet** command to enable the UDP debugging to trace UDP packets.

```
<H3C> terminal debugging
<H3C> debugging udp packet
```

The UDP packets are shown in the following format:

```
UDP output packet:
Source IP address:202.38.160.1
Source port:1024
Destination IP Address 202.38.160.1
Destination port: 4296
```

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

```
<H3C> terminal debugging
<H3C> debugging tcp packet
```

Then the TCP packets received or sent will be displayed in the following format in real time:

```
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
```

Table of Contents

Chapter 1 Management VLAN Configuration 1-1
1.1 Introduction to Management VLAN 1-1
1.1.1 Management VLAN 1-1
1.1.2 Static Route 1-1
1.2 Management VLAN Configuration 1-2
1.2.1 Prerequisites 1-2
1.2.2 Configuring the Management VLAN 1-2
1.2.3 Configuration Example 1-3
1.3 Displaying Management VLAN Configuration 1-4
Chapter 2 DHCP/BOOTP Client Configuration 2-1
2.1 Introduction to DHCP Client 2-1
2.2 Introduction to BOOTP Client 2-3
2.3 DHCP/BOOTP Client Configuration 2-4
2.3.1 Prerequisites 2-4
2.3.2 Configuring a DHCP/BOOTP Client 2-4
2.3.3 Configuration Example 2-5
2.4 Displaying the Information about a DHCP/BOOTP Client 2-6

Chapter 1 Management VLAN Configuration

1.1 Introduction to Management VLAN

1.1.1 Management VLAN

To manage an Ethernet switch remotely through Telnet or the built-in Web server, the switch need to be assigned an IP address. On H3C S3600 series Ethernet swithes, you can specify a management VLAN through related command.

The management VLAN interface of a switch can obtain an IP address in one of the following three ways:

- Through the command used to configure IP address
- Through BOOTP (In this case, the switch operates as a BOOTP client.)
- Through dynamic host configuration protocol (DHCP) (In this case, the switch operates as a DHCP client)

The latest IP address obtained overwrites the previous one. That is, the latest IP address obtained causes the previously IP address to be released. For example, if you assign an IP address to a VLAN interface by using the corresponding commands and then apply for another IP address through BOOTP (using the **ip address bootp-alloc** command), the former IP address will be released, and the final IP address of the VLAN interface is the one obtained through BOOTP.

1.1.2 Static Route

A static route is configured manually by an administrator. You can make a network with relatively simple topology to operate properly by simply configuring static routes for it. Configuring and using static routes wisely helps to improve network performance and can guarantee bandwidth for important applications.

The disadvantages of static route lie in that: When a fault occurs or the network topology changes, static routes may become unreachable, which in turn results in network failures. In this case, manual configurations are needed to recover the network.

To access an S3600 series Ethernet switch through networks, you can configure static routes for it.

1.2 Management VLAN Configuration

1.2.1 Prerequisites

Before configuring the management VLAN, make sure the VLAN operating as the management VLAN exists. If VLAN 1 (the default VLAN) is the management VLAN, just go ahead.

1.2.2 Configuring the Management VLAN

Table 1-1 Configure the management VLAN

Operation	Command	Description
Enter system view	**system-view**	—
Configure a specified VLAN to be the management VLAN	**management-vlan** *vlan-id*	Required By default, VLAN 1 operates as the management VLAN.
Configure the default route	**ip route-static** 0.0.0.0 0.0.0.0 { **null** *null-interface-number* | *next-hop* } [**preference** *preference-value*] [**reject** | **blackhole**] [**detect-group** *detect-group-id*] [**description** *text*]	Required
Create the management VLAN interface and enter the corresponding VLAN interface view	**interface vlan-interface** *vlan-id*	Required
Assign an IP address to the management VLAN interface	**ip address** *ip-address mask* [**sub**]	Required By default, the management VLAN interface has no IP address.
Provide a description string for the management VLAN interface	**description** *string*	Optional By default, the description string of the management VLAN interface is “Vlan-interface vlan-id Interface”.

Operation	Command	Description
Shut down the management VLAN interface	**shutdown**	Optional By default, a management VLAN interface is down if all the Ethernet ports in the management VLAN are down; a management VLAN interface is up if one or more Ethernet ports in the management VLAN are up.
Bring up the management VLAN interface	**undo shutdown**	

Caution:

- To configure the management VLAN of a switch operating as a cluster management device to be a cluster management VLAN (using the **management-vlan** *vlan-id* command) successfully, make sure the *vlan-id* argument provided in the **management-vlan** *vlan-id* command is consistent with that of the management VLAN.
- Bringing up or shutting down a management VLAN interface has no effect on the up/down status of the Ethernet ports in the management VLAN.

1.2.3 Configuration Example

I. Network requirements

To manage the switch SwitchA remotely through Telnet, These requirements are to be met: SwitchA has an IP address, and the route between SwitchA and the remote console is reachable.

You need to configure the switch as follows:

- Assigning an IP address to the management VLAN interface
- Configuring the default route

II. Configuration procedure

Enter system view.

```
<H3C> system-view
```

Create VLAN 10 and configure VLAN 10 to be the management VLAN.

```
[H3C] vlan 10
[H3C-vlan10] quit
[H3C] management-vlan 10
```

Create the VLAN 10 interface and enter VLAN interface view.

```
[H3C] interface vlan-interface 10
```

Configure the IP address of VLAN 10 interface to be 1.1.1.1.

```
[H3C-Vlan-interface10] ip address 1.1.1.1 255.255.255.0
[H3C-Vlan-interface10] quit
```

Configure the default route.

```
[H3C] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

1.3 Displaying Management VLAN Configuration

Table 1-2 Display management VLAN configuration

Operation	Command	Description
Display the IP-related information about a management VLAN interface	**display ip interface** [**brief** [**Vlan-interface** [*vlan-id*]] | [**Vlan-interface** *vlan-id*]]	Optional You can execute the **display** commands in any view.
Display the information about a management VLAN interface	**display interface vlan-interface** [*vlan-id*]	
Display summary information about the routing table	**display ip routing-table**	
Display detailed information about the routing table	**display ip routing-table verbose**	
Display the routes leading to a specified IP address	**display ip routing-table** *ip-address* [*mask*] [**longer-match**] [**verbose**]	
Display the routes leading to a specified IP address range	**display ip routing-table** *ip-address1 mask1 ip-address2 mask2* [**verbose**]	
Display the routing information of the specified protocol	**display ip routing-table protocol** *protocol* [**inactive** | **verbose**]	
Display the routing table in a tree structure	**display ip routing-table radix**	
Display the statistics on the routing table	**display ip routing-table statistics**	

Chapter 2 DHCP/BOOTP Client Configuration

2.1 Introduction to DHCP Client

As the network scale expands and the network complexity increases, the network configurations become more and more complex accordingly. It is usually the case that the computer locations change (such as the portable computers in wireless networks) or the number of the computers exceeds that of the available IP addresses. The dynamic host configuration protocol (DHCP) is developed to meet these requirements. DHCP adopts the client/server model, where DHCP clients request DHCP servers dynamically for configuration information, and the DHCP servers in turn return corresponding configuration information based on policies.

A typical DHCP implementation usually involves a DHCP server and multiple clients (such as PCs and portable computers), as shown in Figure 2-1.

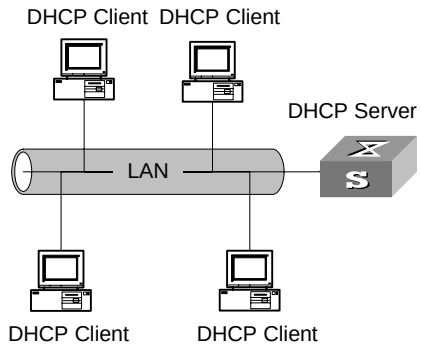


Figure 2-1 A typical DHCP implementation

The interactions between a DHCP client and a DHCP server are shown in Figure 2-2.

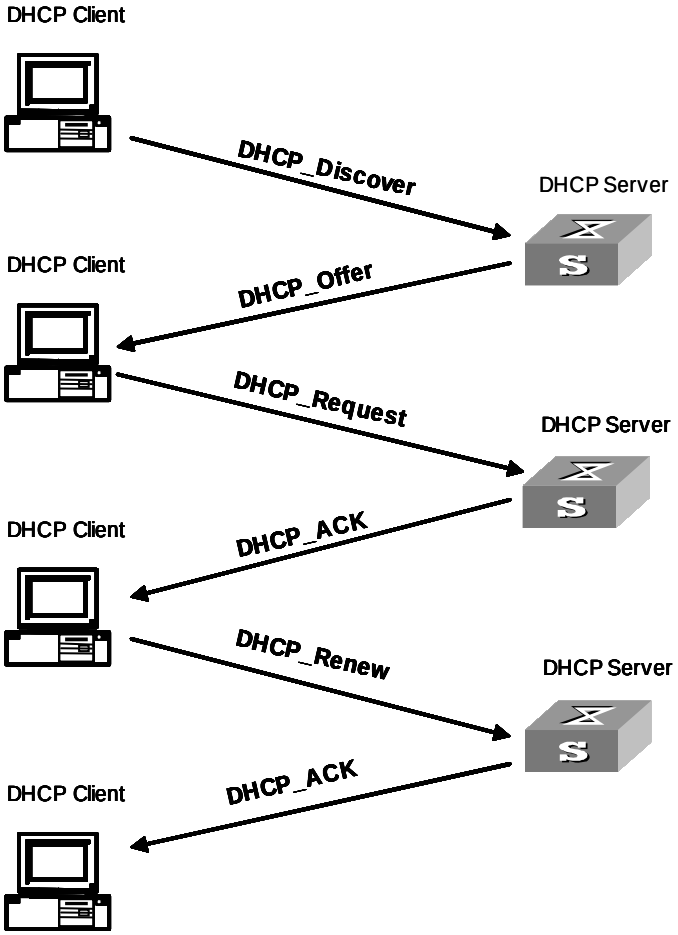


Figure 2-2 The interaction between a DHCP client and a DHCP server

To obtain a valid IP address dynamically, a DHCP client exchanges different information with the DHCP server in different phases. Usually, the following three phases are involved.

1) The DHCP client accesses the network for the first time

When a DHCP client accesses a network for the first time, it goes through the following four phases to establish connections with the DHCP server.

- Discovery. The DHCP client tries to discover a DHCP server by broadcasting DHCP_Discover packets in the network. Only DHCP servers respond to this type of packets.
- Offering IP addresses. Upon receiving DHCP_Discover packets, each DHCP server selects a free 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.
- Selecting the IP address to be used. The DHCP client only accepts and processes the first-arrived DHCP_Offer packet (if multiple DHCP servers send DHCP_Offer packets to it), and broadcasts a DHCP_Request packet to each DHCP server. The

packet contains the IP address carried in the DHCP_Offer packet the DHCP client receives.

- Acknowledgement. Upon receiving the DHCP_Request packet, the DHCP server that owns the IP address carried in the DHCP_Request sends a DHCP_ACK packet to the DHCP client. The packet contains the IP address offered and other configuration information. The DHCP client binds TCP/IP protocol components to its MAC address after receiving the packet.

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) The DHCP client accesses the network for the second and the followed time

In this case, the DHCP client establishes connections with the DHCP server through the following steps.

- After accessing the network successfully for the first time, the DHCP client can access the network again by broadcasting a DHCP_Request packet that contains the IP address assigned to it last time instead of a DHCP_Discover packet.
- Upon receiving the DHCP_Request packet and, when the IP address applied by the client is available, the DHCP server that owns the IP address responds 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 assigned to another DHCP client), the DHCP server responds with a DHCP_NAK packet, which enables the DHCP client to request for a new IP address by sending a DHCP_Discover packet once again.

3) The DHCP client extends the lease of an IP address

IP addresses assigned dynamically are only valid for a specified period of time and the DHCP servers reclaim their assigned IP addresses at the expiration of these periods. Therefore, a DHCP client need to extend the lease period if it is to use a dynamically assigned IP address for a period longer than allowed.

By default, a DHCP client updates its IP address lease automatically by sending DHCP_Request packets to the DHCP server when half of the lease period expires. The DHCP server, in turn, responds with a DHCP_ACK packet to notify the DHCP client of the new lease if the IP address is still available. An S3600 series switch operating as a DHCP support this lease auto-update process.

2.2 Introduction to BOOTP Client

A BOOTP client can request the server for an IP address through BOOTP. It goes through the following two phases to apply for an IP address.

- Sending a BOOTP request packet to the server
- Processing the BOOTP response packet received from the server

To obtain an IP address through BOOTP, a BOOTP client first sends a BOOTP request packet to the server. Upon receiving the request packet, the server returns a BOOTP

response packet. The BOOTP client then retrieves the assigned IP address from the response packet.

The BOOTP packets are sent using user datagram protocol (UDP). To ensure reliable packet transmission, a timer is triggered when a BOOTP client sends a request packet to the server. If no response packet is received from the server after the timer times out, the client sends the request packet again. BOOTP request packets are sent every five seconds and three times at most. A BOOTP client stops sending BOOTP request packets if it fails to obtain an IP address after sending three successive BOOTP request packets.

2.3 DHCP/BOOTP Client Configuration

An S3600 series Ethernet switch can operate as a DHCP client or BOOTP client. In this case, the IP address of the management VLAN interface is obtained through DHCP or BOOTP.

2.3.1 Prerequisites

Before configuring the management VLAN, you need to create the VLAN that is to act as the management VLAN. As VLAN 1 is the default VLAN, there is no need to create it if you configure VLAN 1 to be the management VLAN.

2.3.2 Configuring a DHCP/BOOTP Client

Table 2-1 Configure a DHCP/BOOTP client

Operation	Command	Description
Enter system view	**system-view**	Required
Configure a specified VLAN to be the management VLAN	**management-vlan** *vlan-id*	Required By default, VLAN 1 operates as the management VLAN.
Create the management VLAN interface and enter VLAN interface view	**interface vlan-interface** *vlan-id*	Required
Configure the way in which the management VLAN interface obtains an IP address	**ip address** { **bootp-alloc** | **dhcp-alloc** }	Required By default, no IP address is assigned to the management VLAN interface.

Caution:

Note that as a DHCP client, an S3600 switch can occupy an IP address for up to 24 days. That is, even if the lease period of the address pool on the DHCP server is longer than 24 days, the DHCP client can only obtain a 24-day lease.

2.3.3 Configuration Example

I. Network requirements

To manage the switch SwitchA remotely, which operates as a DHCP client, through Telnet, The following are required:

- SwitchA obtains an IP address through DHCP
- The route between SwitchA and the remote console is reachable.

To achieve this, you need to perform the following configuration for the switch:

- Configuring the management VLAN interface to obtain an IP address through DHCP
- Configuring a default route

II. Configuration procedures

Enter system view.

```
<H3C> system-view
```

Create VLAN 10 and configure VLAN 10 to be the management VLAN.

```
[H3C] vlan 10
[H3C-vlan10] quit
[H3C] management-vlan 10
```

Create VLAN 10 interface and enter VLAN interface view.

```
[H3C] interface vlan-interface 10
```

Configure the management VLAN interface to obtain an IP address through DHCP.

```
[H3C-Vlan-interface10] ip address dhcp-alloc
[H3C-Vlan-interface10] quit
```

Configure the default route.

```
[H3C] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

2.4 Displaying the Information about a DHCP/BOOTP Client

Table 2-2 Display the information about a DHCP/BOOTP client

Operation	Command	Description
Display the information about IP address assignment on the DHCP client	**display dhcp client** [**verbose**]	Optional You can execute the **display** commands in any view.
Display the information about the BOOTP client	**display bootp client** [**interface vlan-interface** *vlan-id*]	

Table of Contents

Chapter 1 Voice VLAN Configuration 1-1
1.1 Voice VLAN Overview 1-1
1.1.1 Configuring Operation Mode for Voice VLAN 1-1
1.1.2 Supporting Information of Voice VLAN on Various Ports 1-2
1.2 Configuring Voice VLAN 1-4
1.2.1 Configuration Prerequisites 1-4
1.2.2 Configuring a Voice VLAN to Operate in Automatic Mode 1-4
1.2.3 Configuring a Voice VLAN to Operate in Manual Mode 1-6
1.3 Displaying Voice VLAN 1-8
1.4 Voice VLAN Configuration Example 1-8
1.4.1 Voice VLAN Configuration Example (Automatic Mode) 1-8
1.4.2 Voice VLAN Configuration Example (Manual Mode) 1-9

Chapter 1 Voice VLAN Configuration

1.1 Voice VLAN Overview

Voice VLANs are VLANs configured specially for voice traffic. By adding the ports with voice devices attached to voice VLANs, you can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

S3600 series Ethernet switches determine whether a received packet is a voice packet by checking its source MAC address. If the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the system, the packets are determined as voice packets and transmitted in voice VLAN.

You can configure an OUI address for voice packets or specify to use the default OUI address.

Note:

An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

The following table shows the five default OUI addresses of a switch.

Table 1-1 Default OUI addresses preset by the switch

Number	OUI Address	Vendor
1	0003-6b00-0000	Cisco phone
2	000f-e200-0000	H3C Aolynk phone
3	00d0-1e00-0000	Pingtel phone
4	00e0-7500-0000	Polycom phone
5	00e0-bb00-0000	3Com phone

1.1.1 Configuring Operation Mode for Voice VLAN

A voice VLAN can operate in two modes: automatic and manual. You can configure the operation mode for the voice VLAN according to data traffic passing through a port.

I. Processing mode of untagged packets sent by IP voice devices

- Automatic mode: an S3600 Ethernet switch automatically adds a port connecting an IP voice device to the voice VLAN by learning the source MAC address in the untagged packet sent by the IP voice device when it is powered on. When the aging time of a port expires, voice ports on which the OUI addresses are not updated (no voice traffic passes) will be automatically removed from the voice VLAN; voice ports can not be added into or removed from the voice VLAN through manual configurations.
- Manual mode: add a voice port to the voice VLAN or remove a voice port from the voice VLAN through manual configuration.

II. Processing mode of tagged packets sent by IP voice devices

For the tagged packets sent by IP voice devices, they are processed in the same way in either of the above two modes: forwarded within corresponding VLAN according to their VLAN ID in the tags.

Note:

- An untagged packet refers to the packet without the VLAN tag.
- A tagged packet refers to the packet with the VLAN tag.

1.1.2 Supporting Information of Voice VLAN on Various Ports

Voice VLAN packets can be forwarded by both trunk and hybrid ports in voice VLAN. You can enable a trunk or hybrid port belonging to other VLANs to forward voice and service packets simultaneously by enabling the voice VLAN.

As multiple types of IP voice devices exist, you need to match port mode with types of voice traffic sent by IP voice devices, as listed in Table 1-2.

Table 1-2 Matching relationship between port modes and voice traffic types

Port voice VLAN mode	Voice traffic type	Port type	Supported or not
Automatic mode	Tagged voice traffic	Access	Not supported
		Trunk	Supported Make sure the default VLAN of the port exists and is not a voice VLAN. And the access port permits the traffic of the default VLAN.
		Hybrid	Supported Make sure the default VLAN of the port exists and is not a voice VLAN. The default VLAN must be in the list of the tagged VLANs whose traffic is permitted by the access port.
	Untagged voice traffic	Access	Not supported, because the default VLAN of the port must be a voice VLAN and the access port is in the voice VLAN. This can be done by adding the port to the voice VLAN manually.
		Trunk	
		Hybrid	
Manual mode	Tag voice traffic	Access	Not supported
		Trunk	Supported Make sure the default VLAN of the port exists and is not a voice VLAN. And the access port permits the traffic of the default VLAN.
		Hybrid	Supported Make sure the default VLAN of the port exists and is in the list of the tagged VLANs whose traffic is permitted by the access port.
	Untag voice traffic	Access	Supported Make sure the default VLAN of the port is a voice VLAN.
		Trunk	Supported Make sure the default VLAN of the port is a voice VLAN and the port permits the traffic of the VLAN.
		Hybrid	Supported Make sure the default VLAN of the port is a voice VLAN and is in the list of untagged VLANs whose traffic is permitted by the port.

Caution:

- If the voice traffic transmitted by an IP voice device is with VLAN tag, and the port which the IP voice device is attached to is enabled with 802.1x authentication and 802.1x guest VLAN, assign different VLAN IDs for the voice VLAN, the default VLAN of the port, and the 802.1x guest VLAN to ensure the effective operation of these functions.
- If the voice traffic transmitted by the IP voice device is without VLAN tag, the default VLAN of the port which the IP voice device is attached to can only be configured to a voice VLAN to ensure the effective operation of the voice VLAN function. In this case, the 802.1x authentication is unavailable.

1.2 Configuring Voice VLAN

1.2.1 Configuration Prerequisites

- Create the corresponding VLAN before configuring a voice VLAN.
- VLAN 1 is the default VLAN and do not need to be created. And VLAN 1 does not support voice VLAN .

1.2.2 Configuring a Voice VLAN to Operate in Automatic Mode

Table 1-3 Configure a voice VLAN to operate in automatic mode

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	Required
Enable the voice VLAN function on a port	**voice vlan enable**	Required By default, voice VLAN is disabled.
Set the voice VLAN operation mode on a port to automatic.	**voice vlan mode auto**	Optional The default voice VLAN operation mode on a port is automatic.
Quit to system view	**quit**	—
Set an OUI address that can be identified by the voice VLAN	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	Optional By default, the switch determines the voice traffic according to the default OUI address.

Operation	Command	Description
Enable the voice VLAN security mode	**voice vlan security enable**	Optional By default, the voice VLAN security mode is enabled.
Set the aging time for the voice VLAN	**voice vlan aging** *minutes*	Optional The default aging time is 1,440 minutes.
Enable the voice VLAN function globally	**voice vlan** *vlan-id* **enable**	Required

Caution:

- For a voice VLAN operates in automatic mode, it does not support the adding of an Access port, and thus a voice VLAN cannot function when configuring with the VLAN VPN function.
- For a voice VLAN operates in automatic mode, it only supports that the Hybrid port to process the tagged voice traffic. However, the protocol VLAN feature requires the Hybrid port to remove tags from the packets, see the VLAN part of this manual for details. Therefore, a VLAN cannot be configured as a voice VLAN and a protocol VLAN simultaneously.
- For a port operates in automatic mode, a default VLAN cannot be configured as a voice VLAN, otherwise the system prompts you for unsuccessful configuration.

Note:

When the voice VLAN is working normally, if the device restarts or the Unit ID of a device in a stack changes, in order to make the established voice connections work normally, the system does not need to be triggered by the voice traffic to add the port in automatic mode to the local devices as well as the IRF of the voice VLAN but does so immediately after the restart or the changes.

1.2.3 Configuring a Voice VLAN to Operate in Manual Mode

Table 1-4 Configure a voice VLAN to operate in manual mode

<table>
<tr><th colspan="3">Operation</th><th>Command</th><th>Description</th></tr>
<tr><td colspan="3">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td colspan="3">Enter port view</td><td>interface interface-type interface-number</td><td>Required</td></tr>
<tr><td colspan="3">Enable voice VLAN on a port</td><td>voice vlan enable</td><td>Required
By default, voice VLAN is disabled on a port.</td></tr>
<tr><td colspan="3">Set voice VLAN operation mode on a port to manual</td><td>undo voice vlan mode auto</td><td>Required
The default voice VLAN operation mode on a port is automatic.</td></tr>
<tr><td colspan="3">Quit to system view</td><td>quit</td><td>—</td></tr>
<tr><td rowspan="5">Add a port in manual mode to the voice VLAN</td><td rowspan="2">Access port</td><td>Enter VLAN view</td><td>vlan vlan-id</td><td rowspan="5">Required</td></tr>
<tr><td>Add the port to the VLAN</td><td>port interface-list</td></tr>
<tr><td rowspan="3">Trunk or Hybrid port</td><td>Enter port view</td><td>interface interface-type interface-num</td></tr>
<tr><td>Add the port to the VLAN</td><td>port trunk permit vlan vlan-id
port hybrid vlan vlan-id { tagged | untagged }</td></tr>
<tr><td>Configure the voice VLAN to be the default VLAN of the port</td><td>port trunk pvid vlan vlan-id
port hybrid pvid vlan vlan-id</td><td>Optional
Refer to Table 1-2 to determine whether or not this operation is needed.</td></tr>
<tr><td colspan="3">Quit to system view</td><td>quit</td><td>—</td></tr>
<tr><td colspan="3">Set an OUI address that can be identified by the voice VLAN</td><td>voice vlan mac-address oui mask oui-mask [description text]</td><td>Optional
Without this address, the default OUI address is used.</td></tr>
</table>

Operation	Command	Description
Enable the voice VLAN security mode	**voice vlan security enable**	Optional By default, the voice VLAN security mode is enabled.
Set the aging time for a voice VLAN	**voice vlan aging** *minutes*	Optional The default aging time is 1,440 minutes.
Enable the voice VLAN function globally	**voice vlan** *vlan-id* **enable**	Required

Caution:

- The voice VLAN function can be enabled for only one VLAN at one time.
- If the Link Aggregation Control Protocol (LACP) is enabled on a port, voice VLAN feature cannot be enabled on it.
- Voice VLAN function can be enabled only for the static VLAN. A dynamic VLAN cannot be configured as a voice VLAN.
- When ACL number applied to a port reaches to its threshold, voice VLAN cannot be enabled on this port. You can use the **display voice vlan error-info** command to locate such ports.
- When a voice VLAN operates in security mode, the device in it permits only the packets whose source addresses are the identified voice OUI addresses. Packets whose source addresses cannot be identified, including certain authentication packets (such as 802.1x authentication packets), will be dropped. Therefore, you are suggested not to transmit both voice data and service data in a voice VLAN. If you have to do so, make sure that the voice VLAN does not operate in security mode.

Note:

To add a Trunk port or a Hybrid port to the voice VLAN, refer to the Port Basic Configurations part of the *H3C S3600 Series Ethernet Switches Command Manual* for the related command.

1.3 Displaying Voice VLAN

After the above configurations, you can execute the **display** command in any view to view the running status and verify the configuration effect.

Table 1-5 Display configurations of a Voice VLAN

Operation	Command	Description
Display the information about ports on which voice VLAN configuration fails	**display voice vlan error-info**	You can execute the **display** command in any view.
Display the voice VLAN configuration status	**display voice vlan status**	
Display the currently valid OUI addresses	**display voice vlan oui**	
Display the ports operating in the current voice VLAN	**display vlan** *vlan-id*	

1.4 Voice VLAN Configuration Example

1.4.1 Voice VLAN Configuration Example (Automatic Mode)

I. Network requirements

- Create VLAN 2 and configure it as a voice VLAN.
- Configure port Ethernet1/0/1 as a Trunk port, with VLAN 6 as the default VLAN and permits the traffic of the default VLAN.
- Ethernet1/0/1 can be added to/removed from the voice VLAN automatically according to the data stream that reaches the port.

II. Configuration procedure

Create VLAN 2.

```
<H3C> system-view
[H3C] vlan 2
```

Configure Ethernet1/0/1 port to be a Trunk port, with VLAN 6 as the default VLAN and permits the traffic of the default VLAN.

```
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] port link-type trunk
[H3C-Ethernet1/0/1] port trunk pvid vlan 6
[H3C-Ethernet1/0/1] port trunk permit vlan 6
```

Enable the voice VLAN function on the port and configure its voice VLAN operation mode to automatic.

```
[H3C-Ethernet1/0/1] voice vlan enable
[H3C-Ethernet1/0/1] voice vlan mode auto
```

Enable the voice VLAN function globally.

```
[H3C-Ethernet1/0/1] quit
[H3C] voice vlan 2 enable
```

1.4.2 Voice VLAN Configuration Example (Manual Mode)

I. Network requirements

- Create VLAN 3 and configure it as a voice VLAN.
- Configure Ethernet1/0/1 port as a Trunk port for it to be added to/removed from the voice VLAN manually.
- Configure the OUI address to be 0011-2200-0000, with the description string being “test”.

II. Configuration procedure

Create VLAN 3.

```
<H3C> system-view
[H3C] vlan 3
[H3C-vlan3] quit
```

Configure Ethernet1/0/3 port to be a Trunk port and add it to VLAN 3.

```
[H3C] interface Ethernet 1/0/3
[H3C-Ethernet1/0/3] port link-type trunk
[H3C-Ethernet1/0/3] port trunk permit vlan 3
```

Enable the voice VLAN function on the port and configure its voice VLAN operation mode to manual.

```
[H3C-Ethernet1/0/3] voice vlan enable
[H3C-Ethernet1/0/3] undo voice vlan mode auto
[H3C-Ethernet1/0/3] quit
```

Specify an OUI address.

```
[H3C] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000 description
test
```

Enable the voice VLAN function globally.

```
[H3C] voice vlan 3 enable
```

Display voice VLAN-related configurations.

```
[H3C] display voice vlan status
Voice Vlan status: ENABLE
Voice Vlan ID: 3
Voice Vlan security mode: Security
```

```
Voice Vlan aging time: 1440 minutes
Current voice vlan enabled port mode:
PORT                    MODE
----------------------------------------
Ethernet1/0/3           MANUAL
```

Remove Ethernet1/0/3 port from the voice VLAN.

```
[H3C] interface Ethernet 1/0/3
[H3C-Ethernet1/0/3] undo port trunk permit vlan 3
```

Table of Contents

Chapter 1 GVRP Configuration 1-1
1.1 Introduction to GVRP 1-1
1.1.1 GVRP Mechanism 1-1
1.1.2 GVRP Packet Format 1-3
1.1.3 Protocol Specifications 1-4
1.2 GVRP Configuration 1-4
1.2.1 Configuration Prerequisite 1-4
1.2.2 Configuration Procedure 1-4
1.3 Displaying and Debugging GVRP 1-6
1.4 GVRP Configuration Example 1-6
1.4.1 Network requirements 1-6
1.4.2 Network diagram 1-6
1.4.3 Configuration procedure 1-7

Chapter 1 GVRP Configuration

1.1 Introduction to GVRP

GARP VLAN registration protocol (GVRP) is an implementation of generic attribute registration protocol (GARP). It maintains dynamic VLAN registration information and propagates the information to other switches by adopting the same mechanism as that of GARP.

Note:

GARP provides a mechanism for the switching members in a switched network to register, distribute and propagate information about VLANs, multicast addresses, and so on between each other.

After the GVRP feature is enabled on a switch, the switch receives the VLAN registration information from other switches to dynamically update the local VLAN registration information (including VLAN members, ports through which the VLAN members can be reached, and so on). The switch also propagates the local VLAN registration information to other switches so that all the switching devices in the same switched network can have the same VLAN information. The VLAN registration information includes not only the static registration information configured locally, but also the dynamic registration information received from other switches.

1.1.1 GVRP Mechanism

I. GARP timers

The information exchange between GARP members is completed by messages. The messages performing important functions for GARP fall into three types: Join, Leave and LeaveAll.

- When a GARP entity expects other switches to register certain attribute information of its own, it sends out a Join message.
- When a GARP entity expects other switches to unregister certain attribute information of its own, it sends out a Leave message.
- Once a GARP entity starts up, it starts the LeaveAll timer. After the timer times out, the GARP entity sends out a LeaveAll message.

The Join message and the Leave message are used together to complete the unregistration and re-registration of information. Through message exchange, all the

attribute information to be registered can be propagated to all the switches in the same switched network.

GARP uses the following timers:

- Hold: When a GARP entity receives a piece of registration information, it does not send out a Join message immediately. Instead, to save the bandwidth resources, it starts the Hold timer and puts all received registration information before the timer times out into one Join message and sends out the message after the timer times out.
- Join: To transmit the Join messages reliably to other entities, a GARP entity sends each Join message two times. The Join timer is used to define the interval at which each Join message is sent.
- Leave: When a GARP entity expects to unregister a piece of attribute information, it sends out a Leave message. Any GARP entity receiving this message starts its Leave timer, and unregisters the attribute information if it does not receives a Join message again before the timer times out.
- LeaveAll: Once a GARP entity starts up, it starts the LeaveAll timer, and sends out a LeaveALL message after the timer times out, so that other GARP entities can re-register all the attribute information on this entity. After that, the entity restarts the LeaveAll timer to begin a new cycle.

II. GVRP port registration mode

GVRP has the following three port registration modes: Normal, Fixed, and Forbidden.

- Normal: In this mode, a port can dynamically register/deregister a VLAN and propagate the dynamic/static VLAN information.
- Fixed: In this mode, a port cannot register/deregister a VLAN dynamically. It only propagates static VLAN information. That is, a trunk port only permits the packets of manually configured VLANs in this mode even if you configure the port to permit the packets of all the VLANs.
- Forbidden: In this mode, a port cannot register/deregister VLANs. It only propagates VLAN 1 information. That is, a trunk port only permits the packets of the default VLAN (namely VLAN 1) in this mode even if you configure the port to permit the packets of all the VLANs.

III. GARP operation procedure

Through the mechanism of GARP, the configuration information on a GARP member will be propagated to the entire switched network. A GARP member can be a terminal workstation or a bridge; it instructs other GARP members to register/unregister its attribute information by declaration/recant, and register/unregister other GARP member's attribute information according to other member's declaration/recant.

The protocol packets of GARP entities use specific multicast MAC addresses as their destination MAC addresses. When receiving these packets, the switch distinguishes

them by their destination MAC addresses and delivers them to different GARP application (for example, GVRP) for further processing.

1.1.2 GVRP Packet Format

The GVRP packets are in the following format:

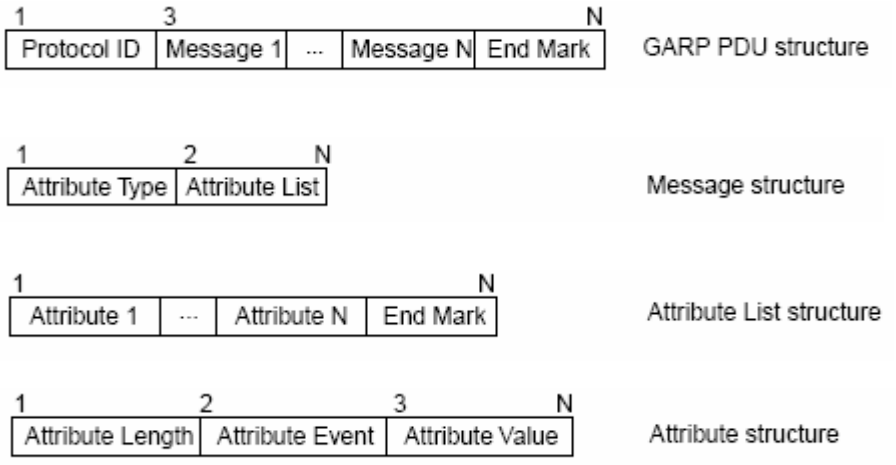


Figure 1-1 Format of GVRP packets

The following table describes the fields of a GVRP packet.

Table 1-1 Description of GVRP packet fields

Field	Description	Value
Protocol ID	Protocol ID	1
Message	Each message consists of two parts: Attribute Type and Attribute List.	—
Attribute Type	Defined by the specific GARP application	The attribute type of GVRP is 0x01.
Attribute List	It contains multiple attributes.	—
Attribute	Each general attribute consists of three parts: Attribute Length, Attribute Event, and Attribute Value. Each LeaveAll attribute consists of two parts: Attribute Length and LeaveAll Event.	—
Attribute Length	The length of the attribute	2 to 255

Field	Description	Value
Attribute Event	The event described by the attribute	0: LeaveAll Event 1: JoinEmpty 2: JoinIn 3: LeaveEmpty 4: LeaveIn 5: Empty
Attribute Value	The value of the attribute	The attribute value of GVRP is the VID.
End Mark	End mark of the GVRP PDU.	—

1.1.3 Protocol Specifications

GVRP is defined in IEEE 802.1Q standard.

1.2 GVRP Configuration

The GVRP configuration tasks include configuring the timers, enabling GVRP, and configuring the GVRP port registration mode.

1.2.1 Configuration Prerequisite

The port on which GVRP will be enabled must be set to a trunk port.

1.2.2 Configuration Procedure

Table 1-2 Configuration procedure

Operation	Command	Description
Enter system view	**system-view**	—
Configure the LeaveAll timer	**garp timer leaveall** *timer-value*	Optional By default, the LeaveAll timer is set to 1,000 centiseconds.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the Hold, Join, and Leave timers	**garp timer** { **hold** | **join** | **leave** } *timer-value*	Optional By default, the Hold, Join, and Leave timers are set to 10, 20, and 60 centiseconds respectively.
Exit and return to system view	**quit**	—

Operation	Command	Description
Enable GVRP globally	**gvrp**	Required By default, GVRP is disabled globally.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable GVRP on the port	**gvrp**	Required By default, GVRP is disabled on the port. After you enable GVRP on a trunk port, you cannot change the port to a different type.
Configure GVRP port registration mode	**gvrp registration** { **fixed** | **forbidden** | **normal** }	Optional You can choose one of the three modes. By default, GVRP port registration mode is normal.

The timeout ranges of the timers vary depending on the timeout values you set for other timers. If you want to set the timeout time of a timer to a value out of the current range, you can set the timeout time of the associated timer to another value to change the timeout range of this timer.

The following table describes the relations between the timers:

Table 1-3 Relations between the timers

Timer	Lower threshold	Upper threshold
Hold	10 centiseconds	This upper threshold is less than or equal to one-half of the timeout time of the Join timer. You can change the threshold by changing the timeout time of the Join timer.
Join	This lower threshold is greater than or equal to twice the timeout time of the Hold timer. You can change the threshold by changing the timeout time of the Hold timer.	This upper threshold is less than one-half of the timeout time of the Leave timer. You can change the threshold by changing the timeout time of the Leave timer.
Leave	This lower threshold is greater than twice the timeout time of the Join timer. You can change the threshold by changing the timeout time of the Join timer.	This upper threshold is less than the timeout time of the LeaveAll timer. You can change the threshold by changing the timeout time of the LeaveAll timer.

Timer	Lower threshold	Upper threshold
LeaveAll	This lower threshold is greater than the timeout time of the Leave timer. You can change threshold by changing the timeout time of the Leave timer.	32,765 centiseconds

1.3 Displaying and Debugging GVRP

After the above configuration, you can use the **display** command in any view to display the configuration information and operating status of GVRP/GARP, and thus verify your configuration. You can use the **reset** command in user view to clear GARP statistics.

Table 1-4 Display and debug GVRP

Operation	Command	Description
Display GARP statistics	**display garp statistics** [**interface** *interface-list*]	The **display** command can be executed in any view.
Display the settings of the GARP timers	**display garp timer** [**interface** *interface-list*]	
Display GVRP statistics	**display gvrp statistics** [**interface** *interface-list*]	
Display the global GVRP status	**display gvrp status**	
Clear GARP statistics	**reset garp statistics** [**interface** *interface-list*]	The **reset** command can be executed in user view.

1.4 GVRP Configuration Example

1.4.1 Network requirements

You need to enable GVRP on the switches to enable dynamic VLAN information registration and update between the switches.

1.4.2 Network diagram

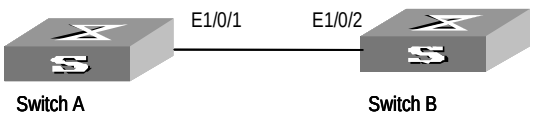


Figure 1-2 Network diagram for GVRP configuration

1.4.3 Configuration procedure

- Configure switch A.

Enable GVRP globally.

```
<H3C> system-view
[H3C] gvrp
GVRP is enabled globally.
```

Configure Ethernet1/0/1 to be a trunk port and to permit the packets of all the VLANs.

```
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] port link-type trunk
[H3C-Ethernet1/0/1] port trunk permit vlan all
```

Enable GVRP on the trunk port.

```
[H3C-Ethernet1/0/1] gvrp
GVRP is enabled on port Ethernet1/0/1.
```

- Configure switch B.

Enable GVRP globally.

```
<H3C> system-view
[H3C] gvrp
GVRP is enabled globally.
```

Configure Ethernet1/0/2 to be a trunk port and to permit the packets of all the VLANs.

```
[H3C] interface Ethernet 1/0/2
[H3C-Ethernet1/0/2] port link-type trunk
[H3C-Ethernet1/0/2] port trunk permit vlan all
```

Enable GVRP on the trunk port.

```
[H3C-Ethernet1/0/2] gvrp
GVRP is enabled on port Ethernet1/0/2.
```

Table of Contents

Chapter 1 Port Basic Configuration 1-1
1.1 Ethernet Port Overview 1-1
1.1.1 Types and Numbers of Ethernet Ports 1-1
1.1.2 Link Types of Ethernet Ports 1-2
1.1.3 Configuring the Default VLAN ID for an Ethernet Port 1-2
1.1.4 Adding an Ethernet Port to Specified VLANs 1-3
1.2 Ethernet Port Configuration 1-4
1.2.1 Initially Configuring a Port 1-4
1.2.2 Limiting Traffic on individual Ports 1-5
1.2.3 Enabling Flow Control on a Port 1-5
1.2.4 Configuring Access Port Attribute 1-6
1.2.5 Configuring Hybrid Port Attribute 1-6
1.2.6 Configuring Trunk Port Attribute 1-7
1.2.7 Copying the Configuration of a Port to Other Ports 1-7
1.2.8 Configuring Loopback Detection for an Ethernet Port 1-8
1.2.9 Configuring the Ethernet Port to Run Loopback Test 1-10
1.2.10 Enabling the System to Test Connected Cable 1-11
1.2.11 Configuring the Interval to Perform Statistical Analysis on Port Traffic 1-11
1.2.12 Enabling Giant-Frame Statistics Function 1-11
1.2.13 Displaying Basic Port Configuration 1-12
1.3 Ethernet Port Configuration Example 1-13
1.4 Troubleshooting Ethernet Port Configuration 1-14

Chapter 1 Port Basic Configuration

1.1 Ethernet Port Overview

1.1.1 Types and Numbers of Ethernet Ports

Table 1-1 lists the types and numbers of the ports available on the H3C S3600 series Ethernet switches.

Table 1-1 Models in the S3600 series

Model	Number of service ports	Number of 100 Mbps ports	Number of 1000 Mbps uplink ports	Console port
H3C S3600-28P-SI	28	24 10/100 Mbps (electrical)	4 (SFP)	1
H3C S3600-28P-PWR-SI	28	24 10/100 Mbps (electrical)	4 (SFP)	1
H3C S3600-28TP-SI	28	24 10/100 Mbps (electrical)	2 (SFP) 2 10/100/1000 Mbps (electrical)	1
H3C S3600-52P-SI	52	48 10/100 Mbps (electrical)	4 (SFP)	1
H3C S3600-28P-EI	28	24 10/100 Mbps (electrical)	4 (SFP)	1
H3C S3600-28F-EI	28	24 100 Mbps (SFP)	2 (SFP) 2 10/100/1000 Mbps (electrical)	1
H3C S3600-28P-PWR-EI	28	24 10/100 Mbps (electrical)	4 (SFP)	1
H3C S3600-52P-EI	52	48 10/100 Mbps (electrical)	4 (SFP)	1

Model	Number of service ports	Number of 100 Mbps ports	Number of 1000 Mbps uplink ports	Console port
H3C S3600-52P-PWR-EI	52	48 10/100 Mbps (electrical)	4 (SFP)	1
H3C S3600-52P-PWR-SI	52	48 10/100 Mbps (electrical)	4 (SFP)	1

1.1.2 Link Types of Ethernet Ports

An Ethernet port on an S3600 switch can operate in one of the three link types:

- Access: An access port can belong to only one VLAN, and is generally used to connect user PCs.
- Trunk: A trunk port can belong to more than one VLAN. It can receive/send packets from/to multiple VLANs, and is generally used to connect another switch.
- Hybrid: A hybrid port can belong to more than one VLAN. It can receive/send packets from/to multiple VLANs, and can be used to connect either a switch or user PCs.

Note:

A hybrid port allows the packets of multiple VLANs to be sent without tags, but a trunk port only allows the packets of the default VLAN to be sent without tags.

You can configure all the three types of ports on the same device. However, note that you cannot directly switch a port between trunk and hybrid and you must set the port as access before the switching. For example, to change a trunk port to hybrid, you must first set it as access and then hybrid.

1.1.3 Configuring the Default VLAN ID for an Ethernet Port

An access port can belong to only one VLAN. Therefore, the VLAN an access port belongs to is also the default VLAN of the access port. A hybrid/trunk port can belong to several VLANs, and so a default VLAN ID for the port is required.

After you configure default VLAN IDs for Ethernet ports, the packets passing through the ports are processed in different ways depending on different situations. See Table 1-2 for details.

Table 1-2 Processing of incoming/outgoing packets

Port type	Processing of an incoming packet		Processing of an outgoing packet
	If the packet does not carry a VLAN tag	If the packet carries a VLAN tag	
Access	Receive the packet and add the default tag to the packet.	• If the VLAN ID is just the default VLAN ID, receive the packet. • If the VLAN ID is not the default VLAN ID, discard the packet.	Deprive the tag from the packet and send the packet.
Trunk		• If the VLAN ID is just the default VLAN ID, receive the packet. • If the VLAN ID is not the default VLAN ID but is one of the VLAN IDs allowed to pass through the port, receive the packet. • If the VLAN ID is neither the default VLAN ID, nor one of the VLAN IDs allowed to pass through the port, discard the packet.	• If the VLAN ID is just the default VLAN ID, deprive the tag and send the packet. • If the VLAN ID is not the default VLAN ID, keep the original tag unchanged and send the packet.
Hybrid			Send the packet if the VLAN ID is allowed to pass through the port. Use the **port hybrid vlan** command to configure whether the port tags the packet when sending a packet in this VLAN (including default VLAN).

Caution:

You are recommended to set the default VLAN ID of the local hybrid or trunk ports to the same value as that of the hybrid or trunk ports on the peer switch. Otherwise, packet forwarding may fail on the ports.

1.1.4 Adding an Ethernet Port to Specified VLANs

You can add the specified Ethernet port to a specified VLAN. After that, the Ethernet port can forward the packets of the specified VLAN, so that the VLAN on this switch can intercommunicate with the same VLAN on the peer switch.

An access port can only be added to one VLAN, while hybrid and trunk ports can be added to multiple VLANs.

🕮 **Note:**

The access ports or hybrid ports must be added to an existing VLAN.

1.2 Ethernet Port Configuration

1.2.1 Initially Configuring a Port

Table 1-3 Initially configure a port

Operation	Command	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the Ethernet port	**undo shutdown**	Optional By default, the port is enabled. Use the **shutdown** command to disable the port.
Set the description of the Ethernet port	**description** *text*	Optional By default, no description is defined for the port.
Set the duplex mode of the Ethernet port	**duplex** { **auto** | **full** | **half** }	Optional By default, the duplex mode of the port is **auto** (auto-negotiation).
Set the speed of the Ethernet port	**speed** { **10** | **100** | **1000** | **auto** }	Optional By default, the speed of the port is **auto** (auto-negotiation).
Set the medium dependent interface (MDI) attribute of the Ethernet port	**mdi** { **across** | **auto** | **normal** }	Optional Be default, the MDI attribute of the port is **auto**.
Allow jumbo frames that are not larger than 9216 bytes to pass through the Ethernet port	**jumboframe enable**	Optional By default, jumbo frames that are not larger than 9216 bytes are allowed to pass through the port.

1.2.2 Limiting Traffic on individual Ports

By performing the following configurations, you can limit different types of incoming traffic on individual ports. When a type of incoming traffic exceeds the threshold you set, the system drops the packets exceeding the traffic limit to reduce the traffic ratio of this type to the reasonable range, so as to keep normal network service.

Table 1-4 Limit traffic on port

Operation	Command	Remarks
Enter system view	**system-view**	—
Limit broadcast traffic received on each port	**broadcast-suppression** { *ratio* | **pps** *max-pps* }	Optional By default, the switch does not suppress broadcast traffic.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Limit broadcast traffic received on the current port	**broadcast-suppression** { *ratio* | **pps** *max-pps* }	Optional By default, the switch does not suppress broadcast traffic.
Limit multicast traffic received on the current port	**multicast-suppression** { *ratio* | **pps** *max-pps* }	Optional By default, the switch does not suppress multicast traffic.
Limit unknown unicast traffic received on the current port	**unicast-suppression** { *ratio* | **pps** *max-pps* }	Optional By default, the switch does not suppress unknown unicast traffic.

1.2.3 Enabling Flow Control on a Port

Flow control is enabled on both the local and peer switches. If congestion occurs on the local switch:

- The local switch sends a message to notify the peer switch of stopping sending packets to itself or reducing the sending rate temporarily.
- The peer switch will stop sending packets to the local switch or reduce the sending rate temporarily when it receives the message; and vice versa. By this way, packet loss is avoided and the network service operates normally.

Table 1-5 Enable flow control on a port

Operation	Command	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable flow control on the Ethernet port	**flow-control**	By default, flow control is not enabled on the port.

1.2.4 Configuring Access Port Attribute

Table 1-6 Configure access port attribute

Operation	Command	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the link type of the port to access	**port link-type access**	Optional By default, the link type of a port is access.
Add the current access port to a specified VLAN	**port access vlan** *vlan-id*	Optional

1.2.5 Configuring Hybrid Port Attribute

Table 1-7 Configure hybrid port attribute

Operation	Command	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the link type of the port to hybrid	**port link-type hybrid**	Required
Set the default VLAN ID for the hybrid port	**port hybrid pvid vlan** *vlan-id*	Optional If no default VLAN ID is set for a hybrid port, VLAN 1 (system default VLAN) is used as the default VLAN of the port.

Operation	Command	Remarks
Add the current hybrid port to a specified VLAN	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Optional For a hybrid port, you can configure whether the system keeps VLAN tags when the packets of the specified VLANs are forwarded on this port.

1.2.6 Configuring Trunk Port Attribute

Table 1-8 Configure trunk port attribute

Operation	Command	Remarks
Enter system view	**System-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the link type of the port to trunk	**port link-type trunk**	Required
Set the default VLAN ID for the trunk port	**port trunk pvid vlan** *vlan-id*	Optional If no default VLAN ID is set for a trunk port, VLAN 1 (system default VLAN) is used as the default VLAN of the port.
Add the current trunk port to a specified VLAN	**port trunk permit vlan** { *vlan-id-list* | **all** }	Optional

1.2.7 Copying the Configuration of a Port to Other Ports

To make some other ports have the same configuration as that of a specific port, you can copy the configuration of the specific port to the ports.

Specifically, the following types of port configuration can be copied from one port to other ports: VLAN configuration, protocol-based VLAN configuration, LACP configuration, QoS configuration, GARP configuration, STP configuration and initial port configuration.

- VLAN configuration: includes IDs of the VLANs allowed on the port and the default VLAN ID of the port;
- Protocol-based VLAN configuration: includes IDs and indexes of the protocol-based VLANs allowed on the port;

- Link aggregation control protocol (LACP) configuration: includes LACP enable/disable status;

Note:

The copy command can only be used to copy the configuration of LACP's enable state, but not to copy the configuration of aggregation group, i.e., you can not add a port to the aggregation group bye the command.

- QoS configuration: includes rate limit, port priority, and default 802.1p priority on the port;
- STP configuration: includes STP enable/disable status on the port, link attribute on the port (point-to-point or non-point-to-point), STP priority, path cost, packet transmission rate limit, whether loop protection is enabled, whether root protection is enabled, and whether the port is an edge port;
- Generic attribute registration protocol (GARP) configuration: includes GVRP enable/disable status, timer settings, and registration mode;
- Port configuration: includes link type of the port, port rate and duplex mode.

Table 1-9 Copy the configuration of a port to other ports

Operation	Command	Remarks
Enter system view	**system-view**	—
Copy the configuration of a port to other ports	**copy configuration source** { *interface-type interface-number* | **aggregation-group** *source-agg-id* } **destination** { *interface-list* [**aggregation-group** *destination-agg-id*] | **aggregation-group** *destination-agg-id* }	Required

---

Note:

- If you specify a source aggregation group ID, the system will use the port with the smallest port number in the aggregation group as the source.
- If you specify a destination aggregation group ID, the configuration of the source port will be copied to all ports in the aggregation group and all ports in the group will have the same configuration as that of the source port.

1.2.8 Configuring Loopback Detection for an Ethernet Port

Loopback detection is used to monitor if loopback occurs on a switch port.

After you enable loopback detection on Ethernet ports, the switch can monitor if external loopback occurs on them. If there is a loopback port found, the switch will put it under control.

- If loopback is found on an access port, the system disables the port, sends a Trap message to the client and removes the corresponding MAC forwarding entry.
- If loopback is found on a trunk or hybrid port, the system sends a Trap message to the client. When the loopback port control function is enabled on these ports, the system disables the port, sends a Trap message to the client and removes the corresponding MAC forwarding entry.

Table 1-10 Set loopback detection for an Ethernet port

Operation	Command	Remarks
Enter system view	**system-view**	—
Enable loopback detection globally	**loopback-detection enable**	Optional By default, loopback detection is disabled globally.
Set time interval for port loopback detection	**loopback-detection interval-time** *time*	Optional The default interval is 30 seconds.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable loopback detection on a specified port	**loopback-detection enable**	Optional By default, port loopback detection is disabled.
Enable loopback port control on the trunk or hybrid port	**loopback-detection control enable**	Optional By default, loopback port control is not enabled.
Configure the system to run loopback detection on all VLANs of the current trunk or hybrid port	**loopback-detection per-vlan enable**	Optional By default, the system runs loopback detection only on the default VLAN of the current trunk or hybrid port.
Display port loopback detection information	**display loopback-detection**	Optional You can use the command in any view.

Caution:

- To enable loopback detection on a specific port, you must use the **loopback-detection enable** command in both system view and the specific port view.
- After you use the **undo loopback-detection enable** command in system view, loopback detection will be disabled on all ports.

1.2.9 Configuring the Ethernet Port to Run Loopback Test

You can configure the Ethernet port to run loopback test to check if it operates normally. The port running loopback test cannot forward data packets normally. The loopback test terminates automatically after a specific period.

Table 1-11 Configure the Ethernet port to run loopback test

Operation	Command	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the Ethernet port to run loopback test	**loopback** { **external** | **internal** }	Optional

Note:

- **external:** Performs external loop test. In the external loop test, self-loop headers must be used on the port of the switch (for 100M port, the self-loop headers are made from four cores of the 8-core cables, for 1000M port, the self-loop header are made from eight cores of the 8-core cables, then the packets forwarded by the port will be received by itself.). The external loop test can locate the hardware failures on the port.
- **internal**: Performs internal loop test. In the internal loop test, self loop is established in the switching chip to locate the chip failure which is related to the port.

After you use the **shutdown** command on a port, the port cannot run loopback test. You cannot use the **speed**, **duplex**, **mdi** and **shutdown** commands on the ports running loopback test. Some ports do not support loopback test, and corresponding prompts will be given when you perform loopback test on them.

1.2.10 Enabling the System to Test Connected Cable

You can enable the system to test the cable connected to a specific port. The test result will be returned in five seconds. The system can test these attributes of the cable: Receive and transmit directions (RX and TX), short circuit/open circuit or not, the length of the faulty cable.

Table 1-12 Enable the system to test connected cables

Operation	Command	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the system to test connected cables	**virtual-cable-test**	Required

1.2.11 Configuring the Interval to Perform Statistical Analysis on Port Traffic

By performing the following configuration, you can set the interval to perform statistical analysis on the traffic of a port.

When you use the **display interface** *interface-type interface-number* command to display the information of a port, the system performs statistical analysis on the traffic flow passing through the port during the specified interval and displays the average rates in the interval. For example, if you set this interval to 100 seconds, the displayed information is as follows:

```
Last 100 seconds input:  0 packets/sec 0 bytes/sec
Last 100 seconds output:  0 packets/sec 0 bytes/sec
```

Table 1-13 Set the interval to perform statistical analysis on port traffic

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the interval to perform statistical analysis on port traffic	**flow-interval** *interval*	Optional By default, this interval is 300 seconds.

1.2.12 Enabling Giant-Frame Statistics Function

The giant-frame statistics function is used to ensure transmission of network traffic and to facilitate statistics and analysis of unusual traffic on the network.

Table 1-14 Enable the giant-frame statistics function

Operation	Command	Description
Enter system view	**system-view**	—
Enable the giant-frame statistics function	**giant-frame statistics enable**	Optional By default, the giant-frame statistics function is not enabled.

1.2.13 Displaying Basic Port Configuration

After the above configurations, you can execute the **display** commands in any view to display information about Ethernet ports, so as to verify your configurations.

You can execute the **reset counters** command in user view to clear the statistics of Ethernet ports.

Table 1-15 Display basic port configuration

Operation	Command	Remarks
Display port configuration information	**display interface** [*interface-type* | *interface-type interface-number*]	You can execute the **display** commands in any view.
Display information about a specified optical port	**display transceiver-information interface** *interface-type interface-number*	
Display the enable/disable status of port loopback detection	**display loopback-detection**	
Display brief information about port configuration	**display brief interface** [*interface-type interface-number*] [**|** { **begin** | **include** | **exclude** } *string*]	
Display the hybrid or trunk ports	**display port** { **hybrid** | **trunk** }	
Display port information about a specified unit	**display unit** *unit-id* **interface**	
Clear port statistics	**reset counters interface** [*interface-type* | *interface-type interface-number*]	You can execute the **reset** command in user view. After 802.1x is enabled on a port, clearing the statistics on the port will not work.

1.3 Ethernet Port Configuration Example

I. Network requirements

- Switch A and Switch B are connected to each other through two trunk port (Ethernet1/0/1).
- Configure the default VLAN ID of both Ethernet1/0/1 to 100.
- Allow the packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass both Ethernet1/0/1.

II. Network diagram

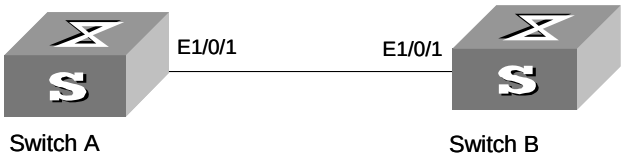


Figure 1-1 Network diagram for Ethernet port configuration

III. Configuration procedure

Note:

- Only the configuration for Switch A is listed below. The configuration for Switch B is similar to that of Switch A.
- This example supposes that VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 have been created.

Enter Ethernet port view of Ethernet1/0/1.

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface ethernet1/0/1
```

Set Ethernet1/0/1 as a trunk port.

```
[H3C-Ethernet1/0/1] port link-type trunk
```

Allow packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass Ethernet1/0/1.

```
[H3C-Ethernet1/0/1] port trunk permit vlan 2 6 to 50 100
```

Configure the default VLAN ID of Ethernet1/0/1 to 100.

```
[H3C-Ethernet1/0/1] port trunk pvid vlan 100
```

1.4 Troubleshooting Ethernet Port Configuration

Symptom: Fail to configure the default VLAN ID of a port.

Solution: Take the following steps.

- Use the **display interface** or **display port** command to check if the port is a trunk port or a hybrid port. If not, configure it to a trunk port or a hybrid port.
- Configure the default VLAN ID.

Table of Contents

Chapter 1 Link Aggregation Configuration 1-1
1.1 Overview 1-1
1.1.1 Introduction to Link Aggregation 1-1
1.1.2 Introduction to LACP 1-2
1.1.3 Operation Key 1-2
1.1.4 Manual Aggregation Group 1-2
1.1.5 Static LACP Aggregation Group 1-3
1.1.6 Dynamic LACP Aggregation Group 1-5
1.1.7 Aggregation Group Categories 1-6
1.2 Link Aggregation Configuration 1-8
1.2.1 Configuring a Manual Aggregation Group 1-9
1.2.2 Configuring a Static LACP Aggregation Group 1-9
1.2.3 Configuring a Dynamic LACP Aggregation Group 1-10
1.3 Displaying and Maintaining Link Aggregation Configuration 1-11
1.4 Link Aggregation Configuration Example 1-12

Chapter 1 Link Aggregation Configuration

1.1 Overview

1.1.1 Introduction to Link Aggregation

Link aggregation means aggregating several ports together to form an aggregation group, so as to implement outgoing/incoming load sharing among the member ports in the group and to enhance the connection reliability.

Depending on different aggregation modes, link aggregation falls into three types: manual, static LACP, and dynamic LACP aggregations. Depending on whether or not load sharing is implemented, aggregation groups can be load-sharing or non-load-sharing aggregation groups.

For the member ports in an aggregation group, their basic configuration must be the same. The basic configuration includes STP, QoS, VLAN, port attributes and other associated settings.

- STP configuration, including STP status (enabled or disabled), link attribute (point-to-point or not), STP priority, path cost, standard packet format, maximum packet transmission speed, loop prevention status, root protection status, edge port or not.
- QoS configuration, including traffic limit, priority remarking, default 802.1p priority, bandwidth assurance, congestion avoidance, traffic redirection, traffic statistics, and so on.
- VLAN configuration, including permitted VLANs, and default VLAN ID.
- Port attribute configuration, including port rate, duplex mode, and link type (Trunk, Hybrid or Access). The ports for a manual or static aggregation group must have the same link type, and the ports for a dynamic aggregation group must have the same rate, duplex mode and link type.

Note:

S3600 series Ethernet switches support cross-device link aggregation if IRF fabric is enabled.

1.1.2 Introduction to LACP

The purpose of link aggregation control protocol (LACP) is to implement dynamic link aggregation and deaggregation. This protocol is based on IEEE802.3ad and uses LACPDUs (link aggregation control protocol data unit) to interact with its peer.

After LACP is enabled on a port, LACP notifies the following information of the port to its peer by sending LACPDUs: priority and MAC address of this system, priority, number and operation key of the port. Upon receiving the information, the peer compares the information with the information of other ports on the peer device to determine the ports that can be aggregated. In this way, the two parties can reach an agreement in adding/removing the port to/from a dynamic aggregation group.

1.1.3 Operation Key

An operation key of an aggregation port is a configuration combination generated by system depending on the configurations of the port (rate, duplex mode, other basic configuration, and management key) when the port is aggregated.

1) The selected ports in a manual/static aggregation group have the same operation key.
2) The management key of an LACP-enabled static aggregation port is equal to its aggregation group ID.
3) The management key of an LACP-enabled dynamic aggregation port is zero by default.
4) The member ports in a dynamic aggregation group must have the same operation key.

1.1.4 Manual Aggregation Group

I. Introduction to manual aggregation group

A manual aggregation group is manually created. All its member ports are manually added and can be manually removed (it inhibits the system from automatically adding/removing ports to/from it). Each manual aggregation group must contain at least one port. When a manual aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

LACP is disabled on the member ports of manual aggregation groups, and enabling LACP on such a port will not take effect.

II. Port status in manual aggregation group

A port in a manual aggregation group can be in one of the two states: selected or unselected. In a manual aggregation group, the selected ports can forward user service packets, but the unselected ports cannot.

The selected port with the smallest port number serves as the master port of the group, and other selected ports serve as member ports of the group.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the member ports serving as selected ports in an aggregation group exceeds the maximum number supported by the device, the system will choose the ports with lower port numbers as the selected ports, and set others as unselected ports.

In a manual aggregation group, the system sets the ports to selected or unselected state by the following rules:

- The system sets the "most preferred" ports (that is, the ports take most precedence over other ports) to selected state, and others to unselected state. Port precedence descends in the following order: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed.
- The system sets the ports unable to aggregate with the master port (due to some hardware limit, for example, cross-board aggregation unavailability) to unselected state.
- The system sets the ports with port attribute configuration (rate, duplex mode, and link type) different from that of the master port to unselected state.

III. Requirements on ports for manual aggregation

Generally, there is no limit on the rate and duplex mode of the ports (also including initially DOWN port) you want to add to a manual aggregation group. After aggregation, the smallest-numbered selected port is the master port of the aggregation group and the other selected ports are the member ports of the aggregation group.

Note:

For an aggregation group:

- When the rate or duplex mode of a port in the aggregation group changes, packet loss may occur on this port;
- When the rate of a port decreases, if the port belongs to a manual or static LACP aggregation group, the port will be switched to the unselected state; if the port belongs to a dynamic LACP aggregation group, deaggregation will occur on the port.

1.1.5 Static LACP Aggregation Group

I. Introduction to static LACP aggregation

A static LACP aggregation group is also manually created. All its member ports are manually added and can be manually removed (it inhibits the system from

automatically adding/removing ports to/from it). Each static aggregation group must contain at least one port. When a static aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

LACP is enabled on the member ports of static aggregation groups. When you remove a static aggregation group, the system will remain the member ports of the group in LACP-enabled state and re-aggregate the ports to form one or more dynamic LACP aggregation groups. You must not disable LACP on static aggregation ports.

II. Port status of static aggregation group

A port in a static aggregation group can be in one of the two states: selected or unselected. In a static aggregation group, both the selected and the unselected ports can transceive LACP protocol packets; the selected ports can transceive user service packets, but the unselected ports cannot.

Note:

In an aggregation group, the selected port with the smallest port number serves as the master port of the group, and other selected ports serve as member ports of the group.

In a static aggregation group, the system sets the ports to selected or unselected state by the following rules:

- The system sets the "most preferred" ports (that is, the ports take most precedence over other ports) to selected state, and others to unselected state. Port precedence descends in the following order: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed.
- The system sets the state of the following ports to unselected: port connected to a peer device different from the one the master port is connected to; port connected to the same peer device as the master port but to a peer port that is not in the same aggregation group as the peer port of the master port.
- The system sets the ports unable to aggregate with the master port (due to some hardware limit, for example, cross-board aggregation unavailability) to unselected state.
- The system sets the ports with basic port configuration different from that of the master port to unselected state.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the member ports that serves as selected ports in an aggregation group exceeds the maximum number supported by the device, the system will choose the ports with lower port numbers as the selected ports, and set others as unselected ports.

1.1.6 Dynamic LACP Aggregation Group

I. Introduction to dynamic LACP aggregation group

A dynamic LACP aggregation group is automatically created and removed by the system. Users cannot add/remove ports to/from it. A port can participate in dynamic link aggregation only when it is LACP-enabled. Ports can be aggregated into a dynamic aggregation group only when they are connected to the same peer device and have the same basic configuration (such as rate and duplex mode).

Besides multiple-port aggregation groups, the system is also able to create single-port aggregation groups, each of which contains only one port. LACP is enabled on the member ports of dynamic aggregation groups.

II. Port status of dynamic aggregation group

A port in a dynamic aggregation group can be in one of the two states: selected or unselected. In a dynamic aggregation group, both the selected and the unselected ports can transceive LACP protocol packets; the selected ports can transceive user service packets, but the unselected ports cannot.

Note:

In an aggregation group, the selected port with the smallest port number serves as the master port of the group, and other selected ports serve as member ports of the group.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the member ports that can be set as selected ports in an aggregation group exceeds the maximum number supported by the device, the system will negotiate with its peer end, to determine the states of the member ports according to the port IDs of the preferred device (that is, the device with smaller system ID). The following is the negotiation procedure:

1) Compare device IDs (system priority + system MAC address) between the two parties. First compare the two system priorities, then the two system MAC addresses if the system priorities are equal. The device with smaller device ID will be considered as the preferred one.
2) Compare port IDs (port priority + port number) on the preferred device. The comparison between two port IDs is as follows: First compare the two port priorities, then the two port numbers if the two port priorities are equal; the port with the smallest port ID is the selected port and the left ports are unselected ports.

III. Configuring system priority

LACP determines the selected and unselected states of the dynamic aggregation group members according to the priority of the port ID on the end with the preferred device ID.

The device ID consists of two-byte system priority and six-byte system MAC address, that is, device ID = system priority + system MAC address.

When two device IDs are compared, the system priorities are compared first, and the system MAC addresses are compared when the system priorities are the same. The device with smaller device ID will be considered as the preferred one.

Note:

Changing the system priority of a device may change the preferred device between the two parties, and may further change the states (selected or unselected) of the member ports of dynamic aggregation groups.

IV. Configuring port priority

LACP determines the selected and unselected states of the dynamic aggregation group members according to the port IDs on the device with the preferred device ID. When the number of members in an aggregation group exceeds the number of selected ports supported by the device in each group, LACP determines the selected and unselected states of the ports according to the port IDs. The ports with superior port IDs will be set to selected state and the ports with inferior port IDs will be set to unselected state.

The port ID consists of two-byte port priority and two-byte port number, that is, port ID = port priority + port number. When two port IDs are compared, the port priorities are compared first, and the port numbers are compared if the port priorities are the same. The port with smaller port ID is considered as the preferred one.

1.1.7 Aggregation Group Categories

Depending on whether or not load sharing is implemented, aggregation groups can be load-sharing or non-load-sharing aggregation groups. When load sharing is implemented,

- For IP packets, the system will implement load-sharing based on source IP address and destination IP address;
- For non-IP packets, the system will implement load-sharing based on source MAC address and destination MAC address.

In general, the system only provides limited load-sharing aggregation resources (currently N/2 load-sharing aggregation groups can be created at most, N is the number of ports), so the system needs to reasonably allocate the resources among different aggregation groups.

The system always allocates hardware aggregation resources to the aggregation groups with higher priorities. When load-sharing aggregation resources are used up by existing aggregation groups, newly-created aggregation groups will be non-load-sharing ones.

Load-sharing aggregation resources are allocated to aggregation groups in the following order:

- An aggregation group containing special ports (such as 10GE port) which require hardware aggregation resources has higher priority than any aggregation group containing no special port.
- A manual or static aggregation group has higher priority than a dynamic aggregation group (unless the latter contains special ports while the former does not).
- For aggregation groups, the one that might gain higher speed if resources were allocated to it has higher priority than others. If the groups can gain the same speed, the one with smallest master port number has higher priority than other groups.

When an aggregation group of higher priority appears, the aggregation groups of lower priorities release their hardware resources. For single-port aggregation groups, they can transceive packets normally without occupying aggregation resources

Caution:

- A load-sharing aggregation group contains at least two selected ports, but a non-load-sharing aggregation group can only have one selected port at most, while others are unselected ports.
- When more than eight load-sharing aggregation groups are configured on a single switch, fabric ports cannot be enabled on this switch.
- When no more than eight load-sharing aggregation groups are configured on a single switch, fabric ports can be enabled on this switch. The aggregation groups added subsequently are all non-load-sharing aggregation groups. If the fabric ports are disabled, the state of these non-load-sharing aggregation groups will not be changed automatically. These non-load-sharing aggregation groups will become load-sharing aggregation groups only after the unselected ports in these aggregation groups are unplugged and then plugged or the **shutdown** command and then the **undo shutdown** command are executed.

1.2 Link Aggregation Configuration

Caution:

- The commands of link aggregation cannot be configured with the commands of port loopback detection feature at the same time.
- The ports where the **mac-address max-mac-count** command is configured cannot be added to an aggregation group. Contrarily, the **mac-address max-mac-count** command cannot be configured on a port that has already been added to an aggregation group.
- MAC-authentication-enabled ports and 802.1x-enabled ports cannot be added to an aggregation group.
- Mirroring destination ports and mirroring reflector ports cannot be added to an aggregation group.
- Ports configured with blackhole MAC addresses, static MAC addresses or the static ARP protocol cannot be added to the aggregation group.
- Ports where the IP-MAC address binding is configured cannot be added to an aggregation group.
- Port-security-enabled ports cannot be added to an aggregation group.
- The port with Voice VLAN enabled cannot be added to an aggregation group.

1.2.1 Configuring a Manual Aggregation Group

You can create a manual aggregation group, or remove an existing manual aggregation group (after that, all the member ports in the group are removed from the ports).

For a manual aggregation group, a port can only be manually added/removed to/from the manual aggregation group.

Table 1-1 Configure a manual aggregation group

Operation	Command	Description
Enter system view	**system-view**	—
Create a manual aggregation group	**link-aggregation group** *agg-id* **mode manual**	Required
Configure a description for the aggregation group	**link-aggregation group** *agg-id* **description** *agg-name*	Optional By default, an aggregation group has no description.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add the Ethernet port to the aggregation group	**port link-aggregation group** *agg-id*	Required

Note that:

1) When creating an aggregation group:

- If the aggregation group you are creating already exists but contains no port, its type will change to the type you set.
- If the aggregation group you are creating already exists and contains ports, the possible type changes may be: changing from dynamic or static to manual, and changing from dynamic to static; and no other kinds of type change can occur.
- When you change a dynamic/static group to a manual group, the system will automatically disable LACP on the member ports. When you change a dynamic group to a static group, the system will remain the member ports LACP-enabled.

2) When a manual or static aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

1.2.2 Configuring a Static LACP Aggregation Group

You can create a static LACP aggregation group, or remove an existing static aggregation group (after that, the system will re-aggregate the original member ports in the group to form one or more dynamic aggregation groups.).

For a static aggregation group, a port can only be manually added/removed to/from the static aggregation group.

Note:

When you add an LACP-enabled port to a manual aggregation group, the system will automatically disable LACP on the port. Similarly, when you add an LACP-disabled port to a static aggregation group, the system will automatically enable LACP on the port.

Table 1-2 Configure a static LACP aggregation group

Operation	Command	Description
Enter system view	**system-view**	—
Create a static aggregation group	**link-aggregation group** *agg-id* **mode static**	Required
Configure a description for the aggregation group	**link-aggregation group** *agg-id* **description** *agg-name*	Optional By default, an aggregation group has no description.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add the port to the aggregation group	**port link-aggregation group** *agg-id*	Required

Note:

For a static LACP aggregation group or a manual aggregation group, you are recommended not to cross cables between the two devices at the two ends of the aggregation group. For example, suppose port 1 of the local device is connected to port 2 of the peer device. To avoid cross-connecting cables, do not connect port 2 of the local device to port 1 of the peer device. Otherwise, packets may be lost.

1.2.3 Configuring a Dynamic LACP Aggregation Group

A dynamic LACP aggregation group is automatically created by the system based on LACP-enabled ports. The adding and removing of ports to/from a dynamic aggregation group are automatically accomplished by LACP.

You need to enable LACP on the ports which you want to participate in dynamic aggregation of the system, because, only when LACP is enabled on those ports at both ends, can the two parties reach agreement in adding/removing ports to/from dynamic aggregation groups.

Note:

You cannot enable LACP on a port which is already in a manual aggregation group.

Table 1-3 Configure a dynamic LACP aggregation group

Operation	Command	Description
Enter system view	**system-view**	—
Configure a description for an aggregation group	**link-aggregation group** *agg-id* **description** *agg-name*	Optional By default, an aggregation group has no description.
Configure the system priority	**lacp system-priority** *system-priority*	Optional By default, the system priority is 32,768.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable LACP on the port	**lacp enable**	Required By default, LACP is disabled on a port.
Configure the port priority	**lacp port-priority** *port-priority*	Optional By default, the port priority is 32,768.

1.3 Displaying and Maintaining Link Aggregation Configuration

After the above configuration, execute the **display** command in any view to display the running status after the link aggregation configuration and verify your configuration. Execute the **reset** command in user view to clear LACP statistics on ports.

Table 1-4 Display and maintain link aggregation configuration

Operation	Command	Description
Display summary information of all aggregation groups	**display link-aggregation summary**	You can execute the **display** command in any view.
Display detailed information of a specific aggregation group or all aggregation groups	**display link-aggregation verbose** [*agg-id*]	
Display link aggregation details of a specified port or port range	**display link-aggregation interface** *interface-type interface-number* [**to** *interface-type interface-number*]	
Display local device ID	**display lacp system-id**	
Clear LACP statistics about a specified port or port range	**reset lacp statistics** [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]	Execute the **reset** command in user view.

1.4 Link Aggregation Configuration Example

I. Network requirements

- Switch A connects to Switch B with three ports Ethernet1/0/1 to Ethernet1/0/3. It is required that incoming/outgoing load between the two switches can be shared among the three ports.
- Adopt three different aggregation modes to implement link aggregation on the three ports between switch A and B.

II. Network diagram

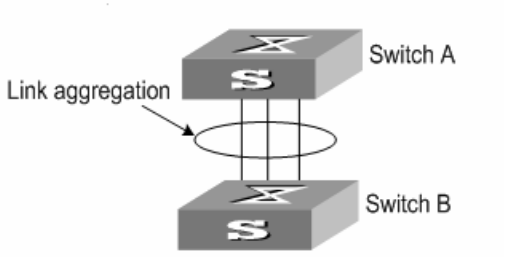


Figure 1-1 Network diagram for link aggregation configuration

III. Configuration procedure

The following only lists the configuration on Switch A; you must perform the similar configuration on Switch B to implement link aggregation.

1) Adopting manual aggregation mode

Create manual aggregation group 1.

```
<H3C> system-view
[H3C] link-aggregation group 1 mode manual
```

Add Ethernet1/0/1 through Ethernet1/0/3 to aggregation group 1.

```
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] port link-aggregation group 1
[H3C-Ethernet1/0/1] interface Ethernet1/0/2
[H3C-Ethernet1/0/2] port link-aggregation group 1
[H3C-Ethernet1/0/2] interface Ethernet1/0/3
[H3C-Ethernet1/0/3] port link-aggregation group 1
```

2) Adopting static LACP aggregation mode

Create static aggregation group 1.

```
<H3C> system-view
[H3C] link-aggregation group 1 mode static
```

Add Ethernet1/0/1 through Ethernet1/0/3 to aggregation group 1.

```
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] port link-aggregation group 1
[H3C-Ethernet1/0/1] interface Ethernet1/0/2
[H3C-Ethernet1/0/2] port link-aggregation group 1
[H3C-Ethernet1/0/2] interface Ethernet1/0/3
[H3C-Ethernet1/0/3] port link-aggregation group 1
```

3) Adopting dynamic LACP aggregation mode

Enable LACP on Ethernet1/0/1 through Ethernet1/0/3.

```
<H3C> system-view
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] lacp enable
[H3C-Ethernet1/0/1] interface Ethernet1/0/2
[H3C-Ethernet1/0/2] lacp enable
[H3C-Ethernet1/0/2] interface Ethernet1/0/3
[H3C-Ethernet1/0/3] lacp enable
```

Note that, the three LACP-enabled ports can be aggregated into a dynamic aggregation group to implement load sharing only when they have the same basic configuration (such as rate and duplex mode and so on).

Table of Contents

Chapter 1 Port Isolation Configuration 1-1
1.1 Port Isolation Overview 1-1
1.2 Port Isolation Configuration 1-1
1.3 Displaying Port Isolation Configuration 1-2
1.4 Port Isolation Configuration Example 1-2

Chapter 1 Port Isolation Configuration

1.1 Port Isolation Overview

Through the port isolation feature, you can add the ports to be controlled into an isolation group to isolate the Layer 2 and Layer 3 data between each port in the isolation group. Thus, you can construct your network in a more flexible way and improve your network security.

Currently, an S3600 Series Ethernet Switch supports only one isolation group, but does not limit the number of Ethernet ports in the unique isolation group.

🕮 **Note:**

Port isolation is independent of VLAN configuration.

1.2 Port Isolation Configuration

You can perform the following operations to add individual Ethernet ports to the isolation group, thus isolating Layer 2 and Layer 3 data between each port in the isolation group.

Table 1-1 Configure port isolation

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add the Ethernet port to the isolation group	**port isolate**	Required By default, an isolation group contains no port.

🕮 **Note:**

When the **port isolate** command or the **undo port isolate** command is executed on a member port of an aggregation group, the other ports in the same aggregation group on the local device will be added to or removed from the isolation group together at the same time.

1.3 Displaying Port Isolation Configuration

After the above configuration, you can execute the **display** command in any view to display the result of your port isolation configuration, thus verifying your configuration.

Table 1-2 Display port isolation configuration

Operation	Command	Description
Display information about the Ethernet ports added to the isolation group	**display isolate port**	You can execute the **display** command in any view.

1.4 Port Isolation Configuration Example

I. Network requirements

- PC2, PC3 and PC4 connect to the switch ports Ethernet1/0/2, Ethernet1/0/3, and Ethernet1/0/4 respectively.
- The switch connects to the Internet through Ethernet1/0/1.
- It is desired that PC2, PC3 and PC4 are isolated from each other so that they cannot communicate with each other.

II. Network diagram

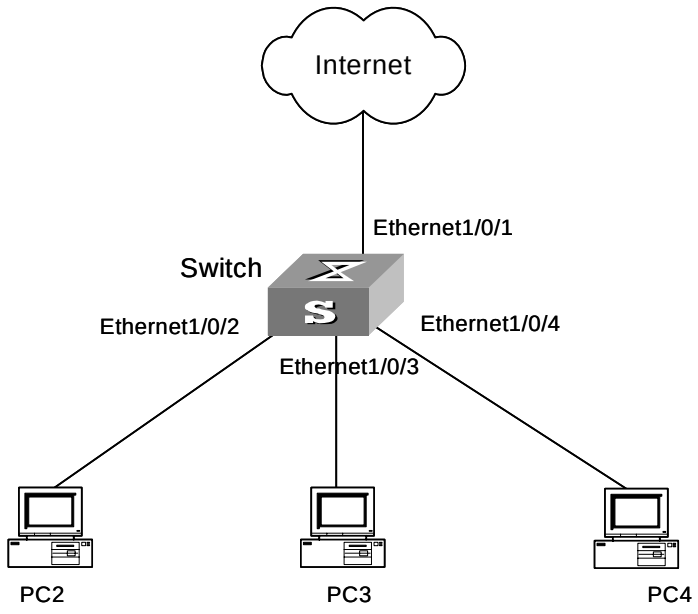


Figure 1-1 Network diagram for port isolation configuration

III. Configuration procedure

Add Ethernet1/0/2, Ethernet1/0/3, and Ethernet1/0/4 to the isolation group.

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface ethernet1/0/2
[H3C-Ethernet1/0/2] port isolate
[H3C-Ethernet1/0/2] quit
[H3C] interface ethernet1/0/3
[H3C-Ethernet1/0/3] port isolate
[H3C-Ethernet1/0/3] quit
[H3C] interface ethernet1/0/4
[H3C-Ethernet1/0/4] port isolate
[H3C-Ethernet1/0/4] quit
[H3C] quit
```

Display information about the ports in the isolation group.

```
<H3C> display isolate port
Isolated port(s) on UNIT 1:
 Ethernet1/0/2, Ethernet1/0/3, Ethernet1/0/4
```

Table of Contents

Chapter 1 Port Security Configuration 1-1
1.1 Port Security Overview 1-1
1.1.1 Introduction 1-1
1.1.2 Port Security Features 1-1
1.1.3 Port Security Modes 1-1
1.2 Port Security Configuration 1-4
1.2.1 Configuring Port Security 1-4
1.2.2 Configuring Security MAC Addresses 1-5
1.3 Displaying Port Security Configuration 1-7
1.4 Port Security Configuration Example 1-7
Chapter 2 Port Binding Configuration 2-1
2.1 Port Binding Overview 2-1
2.1.1 Introduction 2-1
2.1.2 Configuring Port Binding 2-1
2.2 Displaying Port Binding Configuration 2-1
2.3 Port Binding Configuration Example 2-2

Chapter 1 Port Security Configuration

1.1 Port Security Overview

1.1.1 Introduction

Port security is a security mechanism for network access control. It is an expansion to the current 802.1x and MAC address authentication.

Port security defines various security modes that allow devices to learn legal source MAC addresses, in order for you to implement different network security management as needed. With port security, packets whose source MAC addresses cannot be learned by your switch in a security mode are considered illegal packets, and 802.1x authentication failure events are considered illegal events.

Upon detecting an illegal packet or illegal event, the system triggers the corresponding port security features and takes pre-defined actions automatically. This reduces your maintenance workload and greatly enhances system security and manageability.

1.1.2 Port Security Features

The following port security features are provided:

1) NTK (need to know): By checking the destination MAC addresses in outbound data frames on a port, NTK ensures that only successfully authenticated devices can obtain data frames from the port, thus preventing illegal devices from intercepting network data.
2) Intrusion protection: By checking the source MAC addresses in inbound data frames or the username and password in 802.1x authentication requests on a port, intrusion protection detects illegal packets (packets with illegal MAC address) or events and takes a pre-set action accordingly. The actions you can set include: disconnecting the port temporarily/permanently, and blocking packets with invalid MAC addresses.
3) Device tracking: When special data packets (generated from illegal intrusion, abnormal login/logout or other special activities) are passing through a switch port, device tracking enables the switch to send Trap messages to help the network administrator monitor special activities.

1.1.3 Port Security Modes

Table 1-1 describes the available port security modes:

Table 1-1 Description of port security modes

Security mode	Description	Feature
autolearn	In this mode, the port automatically learns MAC addresses and changes them to security MAC addresses. This security mode will automatically change to the **secure** mode after the amount of security MAC addresses on the port reaches the maximum number configured with the **port-security max-mac-count** command. After changing to the **secure** mode, only those packets whose source MAC addresses are security MAC addresses learned or dynamic MAC addresses configured can pass through the port.	In either mode, the device will trigger NTK and intrusion protection upon detecting an illegal packet.
secure	In this mode, the port is disabled from learning MAC addresses. Only those packets whose source MAC addresses are security MAC addresses learned, static MAC addresses or dynamic MAC addresses configured can pass through the port.	
userlogin	In this mode, port-based 802.1x authentication is performed for access users.	In this mode, neither NTK nor intrusion protection will be triggered.

Security mode	Description	Feature
userlogin-secure	The port is enabled only after an access user passes the 802.1x authentication. When the port is enabled, only the packets of the successfully authenticated user can pass through the port. In this mode, only one 802.1x-authenticated user is allowed to access the port. When the port changes from the normal mode to this security mode, the system automatically removes the existing dynamic MAC address entries and authenticated MAC address entries on the port.	In any of these modes, the device will trigger NTK and intrusion protection upon detecting an illegal packet.
userlogin-withoui	This mode is similar to the **userlogin-secure** mode, except that, besides the packets of the single 802.1x-authenticated user, the packets whose source MAC addresses have a particular OUI are also allowed to pass through the port. When the port changes from the normal mode to this security mode, the system automatically removes the existing dynamic/authenticated MAC address entries on the port.	
mac-authentication	In this mode, MAC address–based authentication is performed for access users.	
userlogin-secure-or-mac	In this mode, if either of the **mac-authentication** and **userlogin-secure** modes succeeds, the user passes the authentication.	
mac-else-userlogin-secure	In this mode, first the MAC-based authentication is performed. If this authentication succeeds, the **mac-authentication** mode is adopted, or else, the authentication in **userlogin-secure** mode is performed.	
userlogin-secure-ext	This mode is similar to the **userlogin-secure** mode, except that there can be more than one 802.1x-authenticated user on the port.	
userlogin-secure-or-mac-ext	This mode is similar to the **userlogin-secure-or-mac** mode, except that there can be more than one 802.1x-authenticated user on the port.	
mac-else-userlogin-secure-ext	This mode is similar to the **mac-else-userlogin-secure** mode, except that there can be more than one 802.1x-authenticated user on the port.	

1.2 Port Security Configuration

1.2.1 Configuring Port Security

Table 1-2 Configure port security

Operation	Command	Description
Enter system view	**system-view**	—
Enable port security	**port-security enable**	Required
Set OUI value for user authentication	**port-security oui** *OUI-value* **index** *index-value*	Optional
Enable the sending of specific types of trap messages	**port-security trap** { **addresslearned** | **intrusion** | **dot1xlogon** | **dot1xlogoff** | **dot1xlogfailure** | **ralmlogon** | **ralmlogoff** | **ralmlogfailure** }*	Optional By default, the sending of trap messages is disabled.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the security mode of the port	**port-security port-mode** *mode*	Required You can choose a mode as required.
Set the maximum number of MAC addresses allowed on the port	**port-security max-mac-count** *count-value*	Optional By default, there is no limit on the number of MAC addresses.
Set the NTK transmission mode	**port-security ntk-mode** { **ntkonly** | **ntk-withbroadcasts** | **ntk-withmulticasts** }	Required By default, no packet transmission mode of the NTK feature is set on the port.
Set the action to be taken after intrusion protection is triggered.	**port-security intrusion-mode** { **disableport** | **disableport-temporarily** | **blockmac** }	Required By default, no specific intrusion detection mode is configured.
Configure the port to ignore the authorization information delivered from the RADIUS server	**port-security authorization ignore**	Optional By default, the authorization information delivered by the server is applied to the port.
Return to system view	**quit**	—

Operation	Command	Description
Set the time during which a port is temporarily disabled	**port-security timer disableport** *timer*	Optional By default, it is 20 seconds.

Note:

After the **port-security intrusion-mode disableport-temporarily** command is executed on a port, the time set by the **port-security timer disableport** *timer* command determines how long the port can be temporarily disabled.

To avoid confliction, the following restrictions on the 802.1x authentication and MAC address authentication will be taken after port security is enabled:

1) The access control mode (set by the **dot1x port-control** command) automatically changes to **auto**.
2) The **dot1x**, **dot1x port-method**, **dot1x port-control**, and **mac-authentication** commands cannot be used.

Note:

- For details about 802.1x authentication, refer to the 802.1x part of *S3600 S3600 Series Ethernet Switches Operation Manual.*
- You cannot add a port configured with port security to a link aggregation group.
- You cannot configure the **port-security port-mode** *mode* command on a port if the port is in a link aggregation group.

1.2.2 Configuring Security MAC Addresses

Security MAC addresses are special type of MAC addresses. They are similar to static MAC addresses. One security MAC address can only be added to one port in the same VLAN. So you can bind a MAC address to one port in the same VLAN.

Security MAC addresses can be learned by the auto-learn function of port security. In addition, you can manually configure them through CLI or MIB.

Before adding security MAC addresses to a port, you must configure the port security mode to **autolearn**. After this configuration, the port changes its way to learn MAC addresses.

- The port deletes original dynamic MAC addresses;

- If the amount of security MAC addresses has not yet reach the maximum number, the port will learn new MAC addresses and turn them to security MAC addresses;
- If the amount of security MAC addresses reaches the maximum number, the port will not be able to learn new MAC addresses and the port mode will be changed from **autolearn** to **secure**.

🕮 **Note:**

The security MAC addresses manually configured are written to the configuration file; they will not get lost when the port is up or down. As long as the configuration file is saved, the security MAC addresses can be restored after the switch reboots.

Table 1-3 Configure a security MAC address

Operation	Command	Description
Enter system view	**system-view**	—
Enable port security	**port-security enable**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the maximum number of security MAC addresses allowed on the port	**port-security max-mac-count** *count-value*	Required By default, there is no limit on the maximum number of security MAC addresses.
Set the port security mode to **autolearn**	**port-security port-mode autolearn**	Required
Add a security MAC address	**mac-address security mac-address** [**interface** *interface-type interface-number*] **vlan** *vlan-id*	Required You can execute this command in system view as well as Ethernet port view. When using this command in system view, you should specify **interface** *interface-type interface-number*.

Note that:

1) If the **port-security port-mode autolearn** command is configured on a port, you should not configure the following on the same port:

- Static and black-hole MAC addresses
- Voice VLAN feature
- 802.1x feature

- Link aggregation
- Configurate Mirror Reflector port

2) The **port-security max-mac-count** *count-value* command cannot be configured together with the **mac-address max-mac-count** *count* command.

1.3 Displaying Port Security Configuration

After the above configuration, you can use the **display** command in any view to display port security information and verify your configuration.

Table 1-4 Display port security configuration

Operation	Command	Description
Display information about port security configuration	**display port-security** [**interface** *interface-list*]	You can execute the **display** command in any view.
Display information about security MAC address configuration	**display mac-address security** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]	

1.4 Port Security Configuration Example

I. Network requirements

- Enable port security on port Ethernet1/0/1 of switch A.
- Set the maximum number of the MAC addresses allowed on the port to 80.
- Set the port security mode to **autolearn**.
- Add the MAC address 0001-0002-0003 of PC1 as a security MAC address to VLAN 1.

II. Network diagram

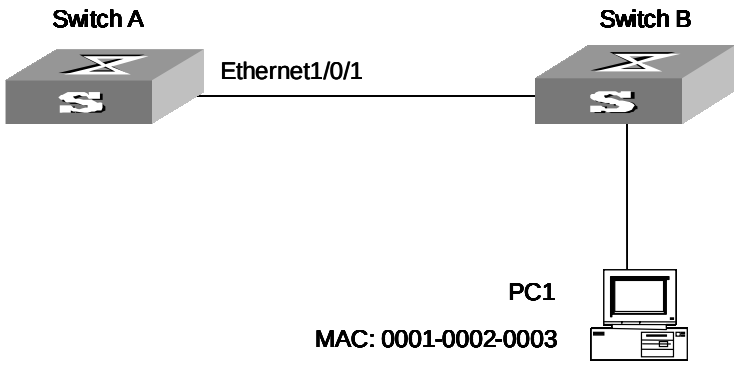


Figure 1-1 Network diagram for port security configuration

III. Configuration procedure

Configure switch A as follows:

Enter system view.

```
<S3600> system-view
```

Enable port security.

```
[S3600] port-security enable
```

Enter Ethernet1/0/1 port view.

```
[S3600] interface Ethernet1/0/1
```

Set the maximum number of MAC addresses allowed on the port to 80.

```
[S3600-Ethernet1/0/1] port-security max-mac-count 80
```

Set the port security mode to **autolearn**.

```
[S3600-Ethernet1/0/1] port-security port-mode autolearn
```

Add the MAC address 0001-0002-0003 of PC1 as a security MAC address to VLAN 1.

```
[S3600-Ethernet1/0/1] mac-address security 0001-0002-0003 vlan 1
```

Chapter 2 Port Binding Configuration

2.1 Port Binding Overview

2.1.1 Introduction

Port binding enables the network administrator to bind the MAC and IP addresses of a legal user to a specific port. After the binding, only the user whose device MAC address is identical with the bound MAC address can use the bound IP address to access the network through the port. This improves network security and enhances security monitoring.

2.1.2 Configuring Port Binding

Table 2-1 Configure port binding

Operation	Command	Description
Enter system view	**system-view**	—
Bind the MAC address and IP address of a legal user to a specific port	**am user-bind mac-addr** *mac-address* **ip-addr** *ip-address* **interface** *interface-type interface-number*	Optional
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Bind the MAC address and IP address of a legal user to the current port	**am user-bind mac-addr** *mac-address* **ip-addr** *ip-address*	Optional

Note:

An IP address can be bound with only one MAC address, and vice versa.

2.2 Displaying Port Binding Configuration

After the above configuration, you can use the **display** command in any view to display port binding information and verify your configuration.

Table 2-2 Display port binding configuration

Operation	Command	Description
Display port binding information	**display am user-bind** [**interface** *interface-type interface-number* | **mac-addr** *mac-addr* | **ip-addr** *ip-addr*]	You can execute the **display** command in any view.

2.3 Port Binding Configuration Example

I. Network requirements

It is required to bind the MAC and IP addresses of PC1 to Ethernet1/0/1 on switch A, so as to prevent malicious users from using the IP address they steal from PC1 to access the network.

II. Network diagram

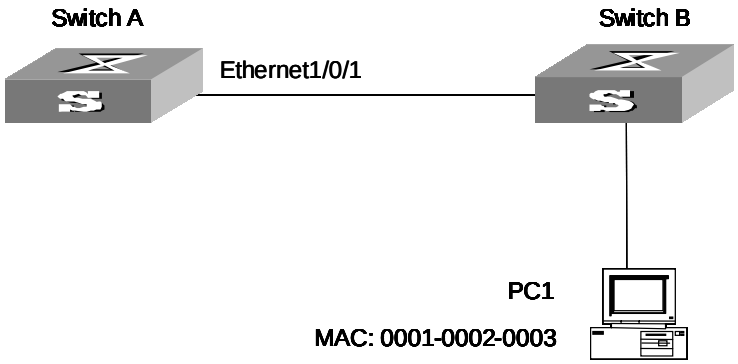


Figure 2-1 Network diagram for port binding configuration

III. Configuration procedure

Configure switch A as follows:

Enter system view.

```
<S3600> system-view
```

Enter Ethernet1/0/1 port view.

```
[S3600] interface Ethernet1/0/1
```

Bind the MAC address and the IP address of PC1 to Ethernet1/0/1.

```
[S3600-Ethernet1/0/1] am user-bind mac-addr 0001-0002-0003 ip-addr 10.12.1.1
```

Table of Contents

Chapter 1 DLDP Configuration 1-1
1.1 DLDP Overview 1-1
1.1.1 DLDP Fundamentals 1-2
1.1.2 Precautions during DLDP Configuration 1-6
1.2 DLDP Configuration 1-7
1.2.1 DLDP Configuration Tasks 1-7
1.2.2 Resetting DLDP State 1-9
1.3 DLDP Configuration Example 1-9

Chapter 1 DLDP Configuration

1.1 DLDP Overview

You may have encountered unidirectional links, namely, one-way audio, in networking. When a unidirectional link occurs, the local device can receive packets from the peer device through the link layer, but the peer device cannot receive packets from the local device.

Unidirectional links can be divided into two types: one is caused by fiber cross-connection, and the other is caused by a fiber being not connected or being disconnected. The cross-connected fibers in Figure 1-1 refer to optical fibers which are connected inversely. The hollow lines in Figure 1-2 refer to fibers which are not connected or are broken.

Unidirectional links can cause many problems, such as spanning tree protocol (STP) loop.

Device link detection protocol (DLDP) can detect the link status of an optical fiber cable or copper twisted pair (such as super category 5 twisted pair). If DLDP finds a unidirectional link, it disables the related port automatically or prompts you to disable it manually according to the configurations, to avoid network problems.

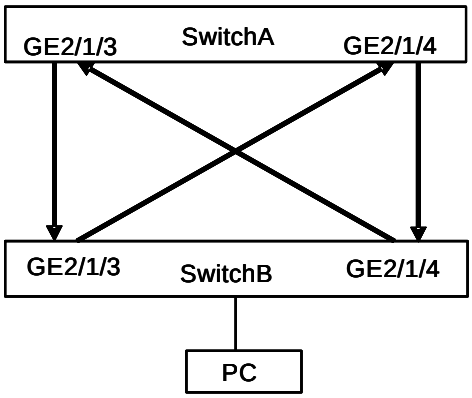


Figure 1-1 Fiber cross-connection

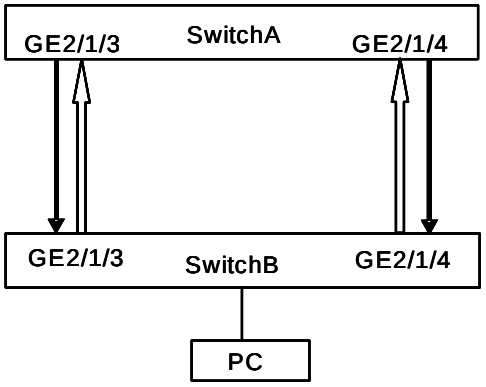


Figure 1-2 Fiber broken or not connected

DLDP provides the following features:

- As a link layer protocol, it works together with the physical layer protocols to monitor the link status of a device.
- The auto-negotiation mechanism at the physical layer detects physical signals and faults. DLDP identifies peer devices and unidirectional links, and disables unreachable ports.
- When auto-negotiation mechanism and DLDP are enabled, they work together to detect and disable physical and logical unidirectional links, and to prevent the failure of other protocols such as STP.
- Even if both ends of links can work normally at the physical layer, DLDP can detect whether these links are connected correctly and whether packets can be exchanged normally at both ends. However, the auto-negotiation mechanism cannot implement this detection.

1.1.1 DLDP Fundamentals

I. DLDP status

A link can be in one of these DLDP states: initial, inactive, active, advertisement, probe, disable, and delaydown.

Table 1-1 DLDP status

Status	Description
Initial	Initial status before DLDP is enabled.
Inactive	DLDP is enabled but the corresponding link is down
Active	DLDP is enabled, and the link is up or an neighbor entry is cleared
Advertisement	All neighbors communicate normally in both directions, or DLDP remains in active state for more than five seconds and enters this status. It is a stable state where no unidirectional link is found

Status	Description
Probe	DHCP sends packets to check whether the link is a unidirectional. It enables the probe sending timer and an echo waiting timer for each target neighbor.
Disable	DLDP detects a unidirectional link, or finds (in enhanced mode) that a neighbor disappears. In this case, DLDP does not receive or send DLDP packets.
Delaydown	When a device in the active, advertisement, or probe DLDP state receives a port down message, it does not removes the corresponding neighbor immediately, neither does it changes to the inactive state. Instead, it changes to the delaydown state first. When a device changes to the delaydown state, the related DLDP neighbor information remains, and the Delaydown timer is triggered.

II. DLDP timers

Table 1-2 DLDP timers

Timer	Description
Advertisement sending timer	Interval between sending advertisement packets, which can be configured on a command line interface. By default, the timer length is 10 seconds.
Probe sending timer	The interval is 0.5 seconds. In the probe state, DLDP sends two probe packets every second.
Echo waiting timer	It is enabled when DLDP enters the probe state. The echo waiting timer length is 10 seconds. If no echo packet is received from the neighbor when the Echo waiting timer expires, the state of the local end is set to unidirectional link (one-way audio) and the state machine turns into the **disable** state. DLDP outputs log and tracking information, sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompts you to disable the port manually. At the same time, DLDP deletes the neighbor entry.

Timer	Description
Entry aging timer	When a new neighbor joins, a neighbor entry is created and the corresponding entry aging timer is enabled When an advertisement packet is received from a neighbor, the neighbor entry is updated and the corresponding entry aging timer is updated In the normal mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP sends an advertisement packet with an RSY tag, and deletes the neighbor entry. In the enhanced mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP enables the enhanced timer The entry aging timer length is three times the advertisement timer length.
Enhanced timer	In the enhanced mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP enables the enhanced timer for the neighbor. The enhanced timer length is 10 seconds The enhanced timer then sends one probe packet every second and eight packets successively to the neighbor. If no echo packet is received from the neighbor when the enhanced timer expires, the state of the local end is set to unidirectional communication state and the state machine turns into the **disable** state. DLDP outputs log and tracking information and sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompts you to disable the port manually. Meanwhile, DLDP deletes the neighbor entry.
Delaydown timer	When a device in the active, advertisement, or probe DLDP state receives a port down message, it does not removes the corresponding neighbor immediately, neither does it changes to the inactive state. Instead, it changes to the delaydown state first. When a device changes to the delaydown state, the related DLDP neighbor information remains, and the Delaydown timer is triggered. The Delaydown timer is configurable and ranges from 1 to 5 seconds. A device in the delaydown state only responds to port up messages. A device in the delaydown state resumes its original DLDP state if it receives a port up message before the delaydown timer expires. Otherwise, it removes the DLDP neighbor information and changes to the inactive state.

III. DLDP operating mode

DLDP can operate in two modes: normal and enhanced.

Table 1-3 DLDP operating mode and neighbor entry aging

DLDP operating mode	DLDP detects whether neighbors exist or not when neighbor tables are aging	The entry aging timer is enabled or not during neighbor entry aging	The enhanced timer is enabled or not when the entry aging timer expires
Normal mode	No	Yes (The neighbor entry ages out after the entry aging timer expires)	No
Enhanced mode	Yes	Yes (The enhanced timer is enabled after the entry aging timer expires)	Yes (When the enhanced timer expires, the state of the local end is set to unidirectional link, and the neighbor entry is aged out.)

IV. DLDP implementation

1) If the DLDP-enabled link is up, DLDP sends DLDP packets to the peer device, and analyzes and processes the DLDP packets received from the peer device. DLDP in different states sends different types of packets.

Table 1-4 Types of packets sent by DLDP

DLDP state	Packet type
Active	Advertisement packets, including those with or without an RSY tag
Advertisement	Advertisement packets
Probe	Probe packets

2) DLDP analyzes and processes received packets from the peer device as follows:

- In authentication mode, DLDP authenticates the packets, and discards those failing to pass the authentication.
- DLDP processes the received DLDP packets.

Table 1-5 Process received DLDP packets

<table>
<tr><th>Packet type</th><th colspan="5">Processing procedure</th></tr>
<tr><td rowspan="2">Advertisement packet</td><td colspan="2" rowspan="2">Extracts neighbor information</td><td colspan="3">If this neighbor entry does not exist on the local device, DLDP creates the neighbor entry, enables the entry aging timer, and switches to the probe state.</td></tr>
<tr><td colspan="3">If the neighbor entry already exists on the local device, DLDP updates the entry aging timer.</td></tr>
<tr><td>Flush packet</td><td colspan="5">Deletes the neighbor entry from the local device</td></tr>
<tr><td rowspan="2">Probe packet</td><td colspan="2" rowspan="2">Sends echo packets containing both neighbor and its own information to the peer</td><td colspan="3">Creates the neighbor entry if this neighbor entry does not exist on the local device.</td></tr>
<tr><td colspan="3">If the neighbor entry already exists on the local device, updates the entry aging timer.</td></tr>
<tr><td rowspan="4">Echo packet</td><td rowspan="4">Checks whether the local device is in the probe state</td><td>No</td><td colspan="3">Discards this echo packet</td></tr>
<tr><td rowspan="3">Yes</td><td rowspan="3">Checks whether neighbor information in the packet is the same as that on the local device</td><td>No</td><td>Discards this echo packet</td></tr>
<tr><td rowspan="2">Yes</td><td>Sets the neighbor flag bit to bidirectional link</td></tr>
<tr><td>If all neighbors are in the bidirectional link state, DLDP switches from the probe state to the advertisement state, and sets the echo waiting timer to 0.</td></tr>
</table>

3) If no echo packet is received from the neighbor, DLDP performs the following processing:

Table 1-6 Processing procedure when no echo packet is received from the neighbor

No echo packet received from the neighbor	Processing procedure
In normal mode, no echo packet is received when the echo waiting timer expires.	DLDP switches to the **disable** state, outputs log and tracking information, and sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompts you to disable the port manually. DLDP sends an RSY message and deletes the neighbor entry.
In enhanced mode, no echo packet is received when the enhanced timer expires	

1.1.2 Precautions during DLDP Configuration

- DLDP works only when the link is up.

- To ensure unidirectional links can be detected, you must make sure that DLDP is enabled on both sides, and that the interval between sending advertisement packets, authentication mode, and password are consistent on both sides.
- You can adjust the interval between sending advertisement packets in different network circumstances so that DLDP can respond rapidly to a link failure. The interval must be shorter than one-third of the STP convergence time, which is generally 30 seconds. If too long an interval is set, an STP loop may occur before DLDP shuts down unidirectional links. On the contrary, if too short an interval is set, network traffic increases, and port bandwidth is reduced.
- DLDP does not process any LACP event, and treats each link in the aggregation group as independent.
- When connecting two DLDP-enabled devices, make sure the software running on them is of the same version. Otherwise, DLDP may operate improperly.

1.2 DLDP Configuration

1.2.1 DLDP Configuration Tasks

Table 1-7 DLDP configuration tasks

<table>
<tr><th colspan="3">Operation</th><th>Command</th><th>Description</th></tr>
<tr><td colspan="3">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td rowspan="3">Enable DLDP</td><td colspan="2">Enable DLDP globally</td><td>dldp enable</td><td rowspan="3">Required.
By default, DLDP is disabled.</td></tr>
<tr><td rowspan="2">Enable DLDP on a port</td><td>Enter Ethernet port view</td><td>interface interface-type interface-number</td></tr>
<tr><td>Enable DLDP on a port</td><td>dldp enable</td></tr>
<tr><td colspan="3">Set the authentication mode and password</td><td>dldp authentication-mode { none | simple simple-password | md5 md5-password }</td><td>Optional.
By default, the authentication mode is none.</td></tr>
<tr><td colspan="3">Set the interval of sending DLDP packets</td><td>dldp interval timer-value</td><td>Optional.
By default, the interval is 10 seconds.</td></tr>
<tr><td colspan="3">Set the delaydown timer</td><td>dldp delaydown-timer delaydown-time</td><td>Optional
By default, the delaydown timer expires after 1 second it is triggered.</td></tr>
</table>

Operation	Command	Description
Set the DLDP handling mode when an unidirectional link is detected	**dldp unidirectional-shutdown** { **auto** | **manual** }	Optional. By default, the handling mode is **auto**.
Set the DLDP operating mode	**dldp work-mode** { **enhance** | **normal** }	Optional. By default, DLDP works in normal mode and does not detect unidirectional links.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Force the duplex attribute	**duplex full**	Required
Force the speed value	**speed** *speed-value*	Required
Display the configuration information about the DLDP-enabled port	**display dldp** { *unit-id* | *interface-type interface-number* }	You can execute this command in any view.

Note:

- When you use the **dldp enable/dldp disable** command in system view to enable/disable DLDP on all optical ports of the switch, the configuration takes effect on the existing optical ports, instead of those added subsequently.
- DLDP can operate normally only when the same authentication mode and password are set on the local and peer ports.
- When the DLDP protocol works in the normal mode, the system can identify only one type of unidirectional link caused by fiber cross-connection.
- When the DLDP protocol works in enhanced mode, the system can identify two types of unidirectional links: one is caused by fiber cross-connection and the other is caused by one fiber being not connected or being broken.
- When the device is busy with services and the CPU utilization is high, DLDP may issue mistaken reports. You are recommended to configure the operating mode of DLDP as manual after unidirectional links are detected, so as to reduce the influence of mistaken reports.

1.2.2 Resetting DLDP State

Note:

After a port is down due to the detection of unidirectional link, you can use the **dldp reset** command to restore the DLDP state to perform DLDP detection.

Table 1-8 Reset DLDP state

Operation	Command	Description
Enter system view	**system-view**	—
Reset the DLDP state of the system	**dldp reset**	Optional
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Reset the DLDP state of a port	**dldp reset**	Optional

Caution:

The **dldp reset** command only applies to the ports in the DLDP down state.

1.3 DLDP Configuration Example

I. Network requirements

As shown in Figure 1-3,

- Switch A and Switch B are connected through two pairs of fibers. Both of them support DLDP.
- Suppose the fibers between Switch A and Switch B are connected inversely. DLDP disconnects a unidirectional link after detecting it.
- When the network administrator connects the fiber correctly, the port shut down by DLDP is restored.

II. Network diagram

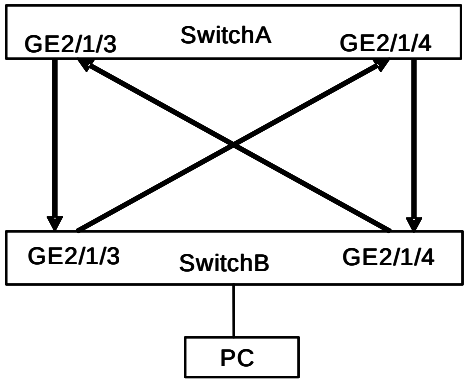


Figure 1-3 Fiber cross-connection

III. Configuration procedure

1) Configure Switch A

Configure the ports to work in mandatory full duplex mode at a rate of 1000 Mbps.

```
<H3CA> system-view
[H3CA] interface gigabitethernet 2/1/3
[H3CA-GigabitEthernet2/1/3] duplex full
[H3CA-GigabitEthernet2/1/3] speed 1000
[H3CA-GigabitEthernet2/1/3] quit
[H3CA] interface gigabitethernet 2/1/4
[H3CA-GigabitEthernet2/1/4] duplex full
[H3CA-GigabitEthernet2/1/4] speed 1000
[H3CA-GigabitEthernet2/1/4] quit
```

Enable DLDP globally

```
[H3CA] dldp enable
```

Set the interval between sending DLDP packets to 15 seconds.

```
[H3CA] dldp interval 15
```

Configure DLDP to work in enhanced mode

```
[H3CA] dldp work-mode enhance
```

Set the DLDP handling mode for unidirectional links to **auto**.

```
[H3CA] dldp unidirectional-shutdown auto
```

Display the DLDP state

```
[H3CA] display dldp 1
```

Note:

When two switches are connected through fibers in a crossed way, two or three ports may be in the disable state, and the rest in the inactive state.

When a fiber is connected to a device correctly on one end with the other end connected to no device:

- If the device operates in the normal DLDP mode, the end that receives optical signals is in the advertisement state; the other end is in the inactive state.
- If the device operates in the enhance DLDP mode, the end that receives optical signals is in the disable state; the other end is in the inactive state.

Restore the ports taken down by DLDP

```
[H3CA] dldp reset
```

2) Configure Switch B

The configuration of Switch B is the same to that of Switch A.

Note:

- In order for DLDP to detect fiber disconnection in one direction, you must configure the port to work in mandatory full duplex mode at a mandatory rate.
- When the port works in non-mandatory full duplex mode at a non-mandatory rate, even if DLDP is enabled, it does not take effect when the fiber in one direction is disconnected. In that case, the port is down.

Table of Contents

Chapter 1 MAC Address Table Management 1-1
1.1 Overview 1-1
1.1.1 Introduction to MAC Address Learning 1-1
1.1.2 Entries in a MAC Address Table 1-3
1.2 Configuring MAC Address Table Management 1-3
1.2.1 Configuring a MAC Address Entry 1-4
1.2.2 Setting the Aging Time of MAC Address Entries 1-5
1.2.3 Setting the Maximum Number of MAC Addresses a Port Can Learn 1-5
1.3 Displaying and Maintaining MAC Address Table Configuration 1-6
1.4 Configuration Example 1-6

Chapter 1 MAC Address Table Management

Note:

This chapter describes the management of static, dynamic, and blackhole MAC address entries. For information about the management of multicast MAC address entries, refer to the section related to multicast protocol in *H3C S3600 Series Ethernet Switches Operation Manual*.

1.1 Overview

1.1.1 Introduction to MAC Address Learning

An Ethernet switch maintains a MAC address table to forward packets quickly. A MAC address table is a port-based Layer 2 address table. It is the base for Ethernet switch to forward Layer 2 packet. Each entry in a MAC address table contains the following fields:

- Destination MAC address
- ID of the VLAN which a port belongs to
- Forwarding port number

Upon receiving a packet, a switch queries its MAC address table for the forwarding port number according to the destination MAC address carried in the packet and then forwards the packet through the port.

The dynamic address entries (not configured manually) in the MAC address table are learned by the Ethernet switch. When an Ethernet switch learns a MAC address, the following occurs:

When a switch receives a packet from one of its ports (referred to as Port 1), the switch extracts the source MAC address (referred to as MAC-SOURCE) of the packet and considers that the packets destined for MAC-SOURCE can be forwarded through Port 1.

- If the MAC address table already contains MAC-SOURCE, the switch updates the corresponding MAC address entry.
- If MAC-SOURCE does not exist in the MAC address table, the switch adds MAC-SOURCE and Port 1 as a new MAC address entry to the MAC address table.

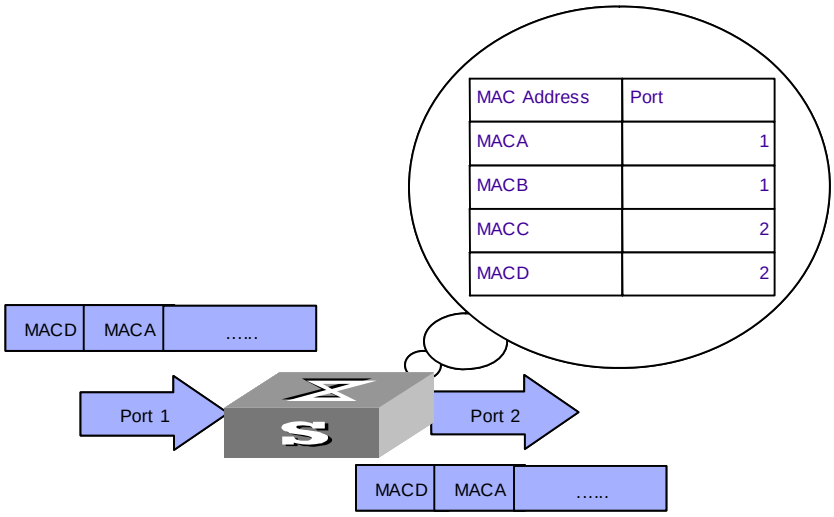


Figure 1-1 A switch uses a MAC address table to forward packets

After learning the source address of the packet, the switch searches the MAC address table for the destination MAC address of the received packet:

- If it finds a match, it directly forwards the packet.
- If it finds no match, it forwards the packet to all ports, except the receiving port, within the VLAN to which the receiving port belongs. Normally, this is referred to as broadcasting the packet.

After the packet is broadcast:

- If the network device returns a packet to the switch, this indicates the packet has been sent to the destination device. The MAC address of the device is carried in the packet. The switch adds the new MAC address to the MAC address table through address learning. After that, the switch can directly forward other packets destined for the same network device by using the newly added MAC address entry.
- If the destination device does not respond to the packet, this indicates that the destination device is unreachable or that the destination device receives the packet but gives no response. In this case, the switch still cannot learn the MAC address of the destination device. Therefore, the switch will still broadcast any other packet with this destination MAC address.

To fully utilize a MAC address table, which has a limited capacity, the switch uses an aging mechanism for updating the table. That is, the switch removes the MAC address entries related to a network device if no packet is received from the device within the aging time. Aging time only applies to dynamic MAC address entries.

You can manually configure (add or modify) a static or dynamic MAC address entry based on the actual network environment.

Note:

The switch learns only unicast addresses by using the MAC address learning mechanism but directly drops any packet with a broadcast source MAC address.

1.1.2 Entries in a MAC Address Table

Entries in a MAC address table fall into the following categories according to their characteristics and configuration methods:

- Static MAC address entry: Also known as permanent MAC address entry. This type of MAC address entries are added/removed manually and can not age out by themselves. Using static MAC address entries can reduce broadcast packets remarkably and are suitable for networks where network devices seldom change.
- Dynamic MAC address entry: This type of MAC address entries age out after the configured aging time. They are generated by the MAC address learning mechanism or configured manually.
- Blackhole MAC address entry: This type of MAC address entries are configured manually. A switch discards the packets destined for or originated from the MAC addresses contained in blackhole MAC address entries.

Table 1-1 lists the different types of MAC address entries and their characteristics.

Table 1-1 Characteristics of different types of MAC address entries

MAC address entry	Configuration method	Aging time	Reserved or not at reboot (if the configuration is saved)
Static MAC address entry	Manually configured	Unavailable	Yes
Dynamic MAC address entry	Manually configured or generated by MAC address learning mechanism	Available	No
Blackhole MAC address entry	Manually configured	Unavailable	Yes

1.2 Configuring MAC Address Table Management

The configuration to manage a MAC address table includes:

- Configuring a MAC address entry
- Configuring the aging time of MAC address entries

- Configuring the maximum number of MAC addresses a port can learn

1.2.1 Configuring a MAC Address Entry

You can add, modify, or remove one MAC address entry, remove all MAC address entries (unicast MAC addresses only) concerning a specific port, or remove specific type of MAC address entries (dynamic or static MAC address entries).

You can add a MAC address entry in either system view or Ethernet port view.

I. Adding a MAC address entry in system view

Table 1-2 Add a MAC address entry in system view

Operation	Command	Description
Enter system view	**system-view**	—
Add a MAC address entry	**mac-address** { **static** | **dynamic** | **blackhole** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	Required

Caution:

- When you add a MAC address entry, the port specified by the **interface** argument must belong to the VLAN specified by the **vlan** argument in the command. Otherwise, the entry will not be added.
- If the VLAN specified by the **vlan** argument is a dynamic VLAN, after a static MAC address is added, it will become a static VLAN.

II. Adding a MAC address entry in Ethernet port view

Table 1-3 Add a MAC address entry in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add a MAC address entry	**mac-address** { **static** | **dynamic** | **blackhole** } *mac-address* **vlan** *vlan-id*	Required

Caution:

- When you add a MAC address entry, the current port must belong to the VLAN specified by the **vlan** argument in the command. Otherwise, the entry will not be added.
- If the VLAN specified by the **vlan** argument is a dynamic VLAN, after a static MAC address is added, it will become a static VLAN.

1.2.2 Setting the Aging Time of MAC Address Entries

Setting aging time properly helps implement effective MAC address aging. The aging time that is too long or too short results in a large amount of broadcast packets wandering across the network and decreases the performance of the switch.

- If the aging time is too long, excessive invalid MAC address entries maintained by the switch may fill up the MAC address table. This prevents the MAC address table from being updated with network changes in time.
- If the aging time is too short, the switch may remove valid MAC address entries. This decreases the forwarding performance of the switch.

Table 1-4 Set aging time of MAC address entries

Operation	Command	Description
Enter system view	**system-view**	—
Set the aging time of MAC address entries	**mac-address timer** { **aging** *age* | **no-aging** }	Required The default aging time is 300 seconds.

This command is used in system view and applies to all ports. Aging applies to only dynamic MAC addresses that are learnt or configured to age.

Normally, you are recommended to use the default aging time, namely, 300 seconds. The **no-aging** keyword specifies that MAC address entries do not age out.

1.2.3 Setting the Maximum Number of MAC Addresses a Port Can Learn

The MAC address learning mechanism enables an Ethernet switch to acquire the MAC addresses of the network devices on the segment connected to the ports of the switch. The switch directly forwards the packets destined for these MAC addresses. A MAC address table too big in size may decrease the forwarding performance of the switch.

By setting the maximum number of MAC addresses that can be learnt from individual ports, you can control the number of the MAC address entries the MAC address table

can dynamically maintain. When the number of the MAC address entries learnt from a port reaches the set value, the port stops learning MAC addresses.

Table 1-5 Set the maximum number of MAC addresses a port can learn

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the maximum number of MAC addresses the port can learn	**mac-address max-mac-count** *count*	Required By default, the number of the MAC addresses a port can learn is not limited.

1.3 Displaying and Maintaining MAC Address Table Configuration

To verify your configuration, you can display information about the MAC address table by executing the **display** command in any view.

Table 1-6 Display and maintain MAC address table configuration

Operation	Command	Description
Display information about the MAC address table	**display mac-address** [*display-option*]	The **display** command can be executed in any view.
Display the aging time of the dynamic MAC address entries in the MAC address table	**display mac-address aging-time**	

1.4 Configuration Example

I. Network requirements

- Log in to the switch through the Console port and enable address table configuration.
- Set the aging time of dynamic MAC address entries to 500 seconds.
- Add a static MAC address entry 000f-e235-dc71 for Ethernet1/0/2 port (assuming that the port belongs to VLAN 1)

II. Network diagram

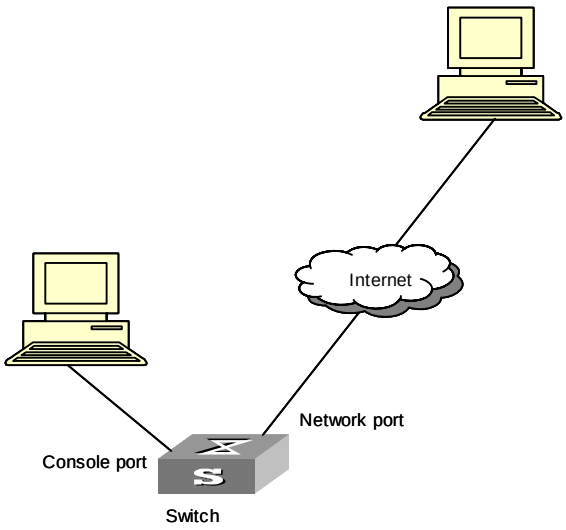


Figure 1-2 Network diagram for MAC address table configuration

III. Configuration procedure

Enter system view.

```
<H3C> system-view
[H3C]
```

Add a MAC address, with the VLAN, ports, and states specified.

```
[H3C] mac-address static 000f-e235-dc71 interface Ethernet 1/0/2 vlan 1
```

Set the aging time of dynamic MAC addresses to 500 seconds.

```
[H3C] mac-address timer aging 500
```

Display the information about the MAC address entries in system view.

```
[H3C] display mac-address interface Ethernet 1/0/2
MAC ADDR          VLAN ID  STATE    PORT INDEX       AGING TIME(s)
000f-e235-dc71    1        Static   Ethernet1/0/2    NOAGED
000f-e217-a7d6    1        Learned  Ethernet1/0/2    AGING
000f-e25e-b1fb    1        Learned  Ethernet1/0/2    AGING
000f-e255-f116    1        Learned  Ethernet1/0/2    AGING
---  4 mac address(es) found on port Ethernet1/0/2 ---
```

Table of Contents

Chapter 1 Auto Detect Configuration 1-1
1.1 Introduction to the Auto Detect Function 1-1
1.1.1 Configuring the Auto Detect Function 1-1
1.1.2 Displaying Auto Detect Configuration 1-1
1.1.3 Auto Detect Configuration Example 1-2
Chapter 2 Auto Detect Implementation 2-1
2.1 Introduction 2-1
2.2 Auto Detect Implementation in Static Routing 2-1
2.2.1 Configuring the Auto Detect Function for a Static Route 2-1
2.2.2 Configuration Example 2-2
2.3 Auto Detect Implementation in VRRP 2-3
2.3.1 Configuring the Auto Detect Function for VRRP 2-3
2.3.2 Configuration Example 2-4
2.4 Auto Detect Implementation in VLAN Interface Backup 2-5
2.4.1 Configuring the Auto Detect Function for VLAN Interface Backup 2-6
2.4.2 Configuration Example 2-6

Chapter 1 Auto Detect Configuration

1.1 Introduction to the Auto Detect Function

The auto detect function uses ICMP request/reply packets to test the connectivity of a network regularly.

The auto detect function is carried out through detecting groups. A detecting group comprises of a group of the IP addresses to be detected. As the states of detecting groups indicate network state, they can be used to locate network problems in time and trigger network devices to take proper measures against network problems.

1.1.1 Configuring the Auto Detect Function

Table 1-1 Configure the auto detect function

Operation	Command	Description
Enter system view	**system-view**	—
Create a detecting group and enter detecting group view	**detect-group** *group-number*	Required
Add an IP address to be detected to the detecting group	**detect-list** *list-number* **ip address** *ip-address* [**nexthop** *ip-address*]	Required
Specify how the detecting result is generated	**option** [**and** | **or**]	Optional By default, the **and** keyword is specified.
Set the detecting interval	**timer loop** *seconds*	Optional By default, the detecting interval is 15 seconds.
Set the maximum number of retries during a detecting operation	**retry** *retry-times*	Optional By default, the maximum number of retries is 2.
Set the detecting timeout time	**timer wait** *seconds*	Optional By default, the detecting timeout time is 2 seconds.

1.1.2 Displaying Auto Detect Configuration

After the above-mentioned configuration, you can use the **display** command in any view to view the auto detect configuration, so as to verify configuration result.

Table 1-2 Display auto detect configuration

Operation	Command	Description
Display the configuration of a detecting group	**display detect-group** [*group-number*]	The **display** command can be executed in any view.

1.1.3 Auto Detect Configuration Example

I. Network requirements

- Create detecting group 10 on Switch A and add two IP addresses, 10.1.1.4 and 192.168.2.2, to it to test the reachability to the two IP addresses.
- Specify to return **reachable** as the detecting result if one of the two IP addresses is reachable, that is, specify the **or** keyword for the **option** command.
- Set the detecting interval to 60 seconds; the maximum number of retries to 3, and the timeout time to 3 seconds.

II. Network diagram

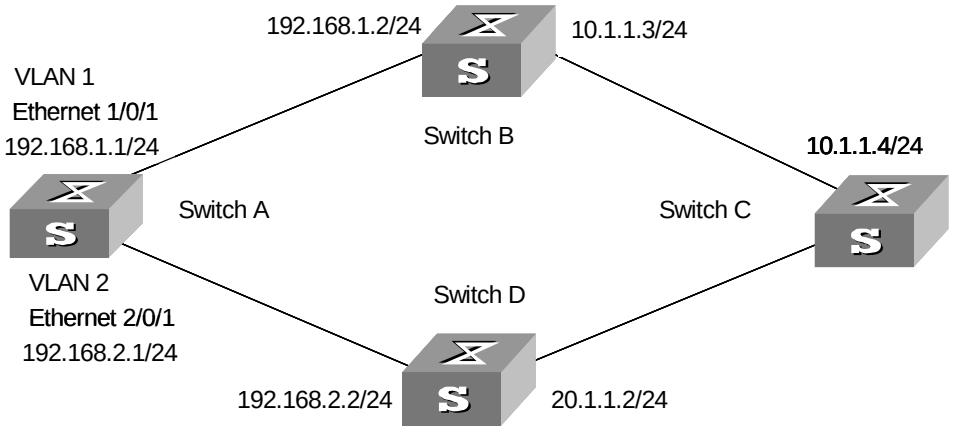


Figure 1-1 Network diagram for auto detect configuration

III. Configuration procedure

Enter system view.

```
<H3C> system-view
```

Create detecting group 10.

```
[H3C] detect-group 10
```

Specify to detect the IP address of 10.1.1.4, taking the IP address of 192.168.1.2 as the next hop and setting the detecting number to 1.

```
[H3C-detect-group-10] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
```

Specify to detect the IP address of 192.168.2.2, setting the detecting number to 2.

```
[H3C-detect-group-10] detect-list 2 ip address 192.168.2.2
```

Specify to return **reachable** as the detecting result if one of the two IP addresses is reachable.

```
[H3C-detect-group-10] option or
```

Set the detecting interval to 60 seconds.

```
[H3C-detect-group-10] timer loop 60
```

Set the maximum number of retries during a detecting operation to 3.

```
[H3C-detect-group-10] retry 3
```

The IP addresses in the detecting group are detected after 3 seconds the last detecting operation is performed.

```
[H3C-detect-group-10] timer wait 3
[H3C-detect-group-10] quit
[H3C]
```

Chapter 2 Auto Detect Implementation

2.1 Introduction

The results of auto detect operations (reachable or unreachable) can be used to trigger other functions, such as:

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

You can utilize a single detecting group simultaneously in multiple implementations mentioned above.

🕮 **Note:**

- Refer to the Routing Protocol chapter of this manual for information about static routing.
- Refer to the VRRP chapter of this manual for information about VRRP.

2.2 Auto Detect Implementation in Static Routing

By binding a detecting group to a static route, you can control the validity of a static route according to auto detect results as follows:

- Enable the static route when the result of the detecting group is **reachable**.
- Disable the static route when the result of the detecting group is **unreachable**.

2.2.1 Configuring the Auto Detect Function for a Static Route

---

🕮 **Note:**

You need to create the detecting group before performing the following operations.

Table 2-1 Configure the auto detect function for a static route

Operation	Command	Description
Enter system view	**system-view**	—
Bind a detecting group to a static route	**ip route-static** *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *next-hop* } [**preference** *preference-value*] [**reject** | **blackhole**] **detect-group** *group-number*	Required

2.2.2 Configuration Example

I. Network requirements

- Create detecting group 8 on Switch A. to detect the reachability of the IP address 10.1.1.4/24, with 192.168.1.2/24 as the next hop, and the detecting number set to 1.
- Configure a static route between Switch A and Switch B.
- Enable the static route when the result of detecting group 8 is **reachable**.

II. Network diagram

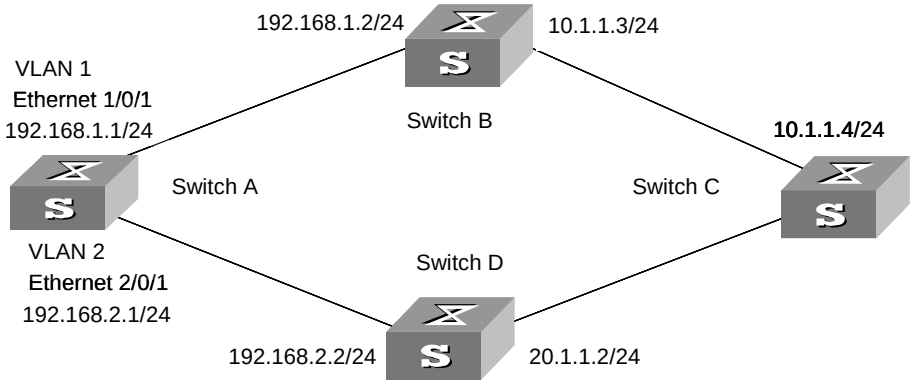


Figure 2-1 Network diagram for implementing the auto detect function in static routing

III. Configuration procedure

- Configure Switch A.

Enter system view.

```
<H3C> system-view
```

Create detecting group 8.

```
[H3C] detect-group 8
```

Detect the reachability of 10.1.1.4/24, with 192.168.1.2/24 as the next hop, and the detecting number set to 1.

```
[H3C-detect-group-8] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
[H3C-detect-group-8] quit
```

Enable the static route when the detecting group is reachable. Disable the static route when the detecting group is unreachable.

```
[H3C] ip route-static 10.1.1.4 24 192.168.1.2 detect-group 8
```

2.3 Auto Detect Implementation in VRRP

Note:

Currently, auto detect implementation in VRRP is only supported on S3600-EI series switches.

You can control the priorities of VRRP backup groups according to auto detect results to enable automatic switch between the master and the backup switch as follows:

- Decrease the priority of a VRRP backup group when the result of the detecting group is **unreachable**.
- Resume the priority of a VRRP backup group when the result of the detecting group is **reachable**.

2.3.1 Configuring the Auto Detect Function for VRRP

Note:

You need to create the detecting group and perform VRRP-related configurations before the following operations.

Table 2-2 Configure the auto detect function for VRRP

Operation	Command	Description
Enter system view	**system-view**	—
Enter VLAN interface view	**interface vlan-interface** *vlan-id*	—
Enable the auto detect function for VRRP	**Vrrp vrid** *virtual-router-id* **track detect-group** *group-number* [**reduced** *value-reduced*]	Required

2.3.2 Configuration Example

I. Network requirements

- Switch B and switch D form VRRP backup group 1, whose virtual IP address is 192.168.1.10.
- Packets sourced from Switch A and destined for Switch C is forwarded by Switch B under normal situations.
- When the connection between Switch B and Switch C fails, Switch D becomes the Master in backup group 1 automatically and the link from Switch D to Switch C, the secondary link, is enabled.

II. Network diagram

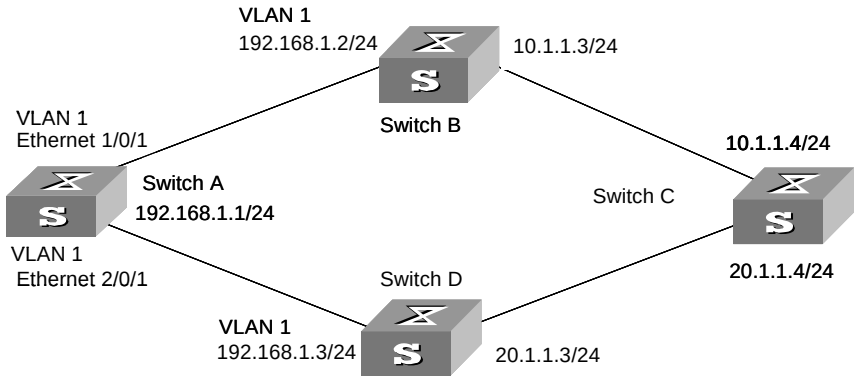


Figure 2-2 Network diagram for implementing the auto detect function in VRRP

III. Configuration procedure

- Configure Switch B.

Create detecting group 9.

```
<H3C> system-view
[H3C] detect-group 9
```

Specify to detect the reachability of the IP address 10.1.1.4/24, setting the detect number to 1.

```
[H3C-detect-group-9] detect-list 1 ip address 10.1.1.4
[H3C-detect-group-9] quit
```

Assign an IP address to VLAN 1 interface.

```
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 192.168.1.2 24
```

Enable VRRP on VLAN 1 interface and assign a virtual IP address to the backup group.

```
[H3C-Vlan-interface1] vrrp vrid 1 virtual-ip 192.168.1.10
```

Set the backup group priority of switch B to 110, and specify to decrease the priority by 20 when the result of detecting group 9 is **unreachable**.

```
[H3C-Vlan-interface1] vrrp vrid 1 priority 110
[H3C-Vlan-interface1] vrrp vrid 1 track detect-group 9 reduced 20
```

- Configure Switch D.

Assign an IP address to VLAN 1 interface.

```
<H3C> system-view
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 192.168.1.3 24
```

Enable VRRP on VLAN 1 interface and assign a virtual IP address to the backup group.

```
[H3C-Vlan-interface1] vrrp vrid 1 virtual-ip 192.168.1.10
```

Set the backup group priority of Switch D to 100.

```
[H3C-Vlan-interface1] vrrp vrid 1 priority 100
```

2.4 Auto Detect Implementation in VLAN Interface Backup

The interface backup function is used to back up VLAN interfaces by using the auto detect function. For two VLAN interfaces configured with the same destination device, you can configure them to be the primary interface and the secondary interface. The latter is enabled automatically when the primary fails, so as to ensure the connectivity. In this case, the auto detect function is implemented as follows:

- In normal situations (that is, when the result of the detecting group is **reachable**), the secondary VLAN interface is down and packets are transmitted through the primary VLAN interface.
- When the link between the primary VLAN interface and the destination operates improperly (that is, the result of the detecting group is **unreachable**), the system shuts down the primary VLAN interface and enables the secondary VLAN interface.
- When the link between the primary VLAN interface and the destination recovers (that is, the result of the detecting group becomes **reachable** again), the system enables the primary VLAN interface and shuts down the secondary VLAN interface again.

2.4.1 Configuring the Auto Detect Function for VLAN Interface Backup

Note:

You need to create the detecting group and perform configurations concerning VLAN interfaces before the following operations.

Table 2-3 Configure the auto detect function for VLAN interface backup

Operation	Command	Description
Enter system view	**system-view**	—
Enter VLAN interface view	**interface vlan-interface** *vlan_id*	—
Enable the auto detect function to implement VLAN interface backup	**standby detect-group** *group-number*	Required This operation is only needed on the secondary VLAN interface.

2.4.2 Configuration Example

I. Network requirements

- Configure a static route between Switch C and Switch A.
- Create detecting group 10 on Switch A to detect the connectivity between Switch B and Switch C.
- Configure VLAN 1 interface to be the primary interface, which is enabled when the result of detecting group 10 is **reachable**.
- Configure VLAN 2 interface to be the secondary interface, which is enabled when the result of the detecting group 10 is **unreachable**.
- Make sure the routes between Switch A, Switch B, and Switch C are reachable; and those between Switch A, Switch D, and Switch C are also reachable.

II. Network diagram

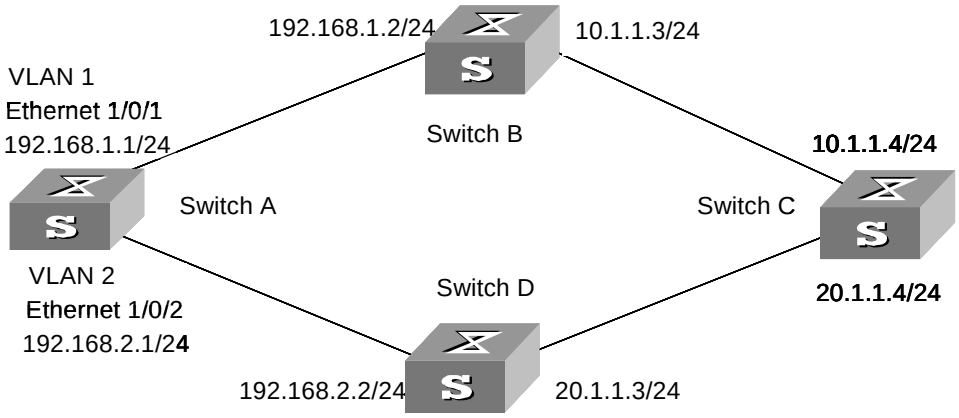


Figure 2-3 Network diagram for VLAN interface backup

III. Configuration procedure

- Configure Switch C.

Enter system view.

```
<H3C> system-view
```

Configure a static route to VLAN interface 1 on Switch A as the primary route, with the IP address of 10.1.1.3/24 as the next hop.

```
[H3C] ip route-static 192.168.1.1 24 10.1.1.3
```

Configure a static route to VLAN interface 2 on Switch A as the secondary route, with the IP address of 20.1.1.3/24 as the next hop.

```
[H3C] ip route-static 192.168.2.1 24 20.1.1.3
```

- Configure Switch A.

Enter system view.

```
<H3C> system-view
```

Assign an IP address to VLAN 1 interface.

```
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 192.168.1.1 24
[H3C-Vlan-interface1] quit
```

Add port Ethernet1/0/2 to VLAN 2.

```
[H3C] vlan 2
[H3C-vlan2] port ethernet1/0/2
[H3C-vlan2] quit
```

Assign an IP address to VLAN 2 interface.

```
[H3C] interface vlan-interface 2
[H3C-Vlan-interface2] ip address 192.168.2.1 24
```

```
[H3C-Vlan-interface2] quit
```

Create auto detecting group 10.

```
[H3C] detect-group 10
```

Add the IP address of 10.1.1.4 to detecting group 10 to detect the reachability of the IP address, with the IP address of 192.168.1.2 as the next hop, and the detecting number set to 1.

```
[H3C-detect-group-10] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
[H3C-detect-group-10] quit
```

Specify to enable VLAN 2 interface when the result of detecting group 10 is **unreachable**.

```
[H3C] interface vlan-interface 2
[H3C-Vlan-interface2] standby detect-group 10
```

Table of Contents

Chapter 1 MSTP Configuration 1-1
1.1 MSTP Overview 1-1
1.1.1 MSTP Protocol Data Unit 1-1
1.1.2 Basic MSTP Terminologies 1-2
1.1.3 Principle of MSTP 1-5
1.1.4 MSTP Implementation on Switches 1-7
1.2 Configuring Root Bridge 1-7
1.2.1 Configuration Prerequisites 1-8
1.2.2 Configuring the MST Region 1-9
1.2.3 Specifying the Current Switch as a Root Bridge/Secondary Root Bridge 1-10
1.2.4 Configuring the Bridge Priority of the Current Switch 1-12
1.2.5 Configuring the MSTP Packet Format 1-13
1.2.6 Configuring the MSTP Operation Mode 1-14
1.2.7 Configuring the Maximum Hops of MST Region 1-15
1.2.8 Configuring the Network Diameter of the Switched Network 1-16
1.2.9 Configuring the MSTP Time-related Parameters 1-16
1.2.10 Configuring the Timeout Time Factor 1-18
1.2.11 Configuring the Maximum Transmitting Speed on the Current Port 1-19
1.2.12 Configuring the Current Port as an Edge Port 1-21
1.2.13 Specifying Whether the Link Connected to a Port Is Point-to-point Link 1-22
1.2.14 Enabling the MSTP Feature 1-24
1.3 Configuring Leaf Nodes 1-25
1.3.1 Configuration Prerequisites 1-26
1.3.2 Configuring the MST Region 1-26
1.3.3 Configuring the MSTP Operation Mode 1-27
1.3.4 Configuring the Timeout Time Factor 1-27
1.3.5 Configuring the Maximum Transmitting Speed 1-27
1.3.6 Configuring a Port as an Edge 1-27
1.3.7 Configuring the Path Cost for a Port 1-27
1.3.8 Configuring Port Priority 1-30
1.3.9 Specifying Whether the Link Connected to a Port Is a Point-to-point Link 1-31
1.3.10 Enabling the MSTP Feature 1-31
1.4 Performing mCheck 1-31
1.4.1 Configuration Prerequisites 1-32
1.4.2 Configuration Procedure 1-32
1.4.3 Configuration Example 1-32
1.5 Configuring Protection Function 1-33
1.5.1 Introduction 1-33

1.5.2 Configuration Prerequisites 1-35
1.5.3 Configuring BPDU Protection 1-35
1.5.4 Configuring Root Protection 1-35
1.5.5 Configuring Loop Prevention 1-36
1.5.6 Configuring TC-BPDU Attack Prevention 1-37
1.5.7 Configuring the Function of Dropping BPDU Packets 1-37
1.6 Configuring Digest Snooping 1-38
1.6.1 Introduction 1-38
1.6.2 Configuring Digest Snooping 1-38
1.7 Configuring Rapid Transition 1-40
1.7.1 Introduction 1-40
1.7.2 Configuring Rapid Transition 1-41
1.8 Configuring VLAN-VPN Tunnel 1-43
1.8.1 Introduction 1-43
1.8.2 Configuring VLAN-VPN tunnel 1-44
1.9 Displaying and Maintaining MSTP 1-44
1.10 MSTP Configuration Example 1-45
1.11 VLAN-VPN tunnel Configuration Example 1-47

Chapter 1 MSTP Configuration

1.1 MSTP Overview

Spanning tree protocol (STP) cannot enable Ethernet ports to transit their states rapidly. It costs two times of the forward delay for a port to turn to the forwarding state even if the port is on a point-to-point link or the port is an edge port.

Rapid spanning tree protocol (RSTP) enables the spanning tree to converge rapidly, but it suffers from the same drawback as STP: all bridges in a LAN share one spanning tree; packets of all VLANs are forwarded along the same spanning tree, and therefore redundant links cannot be blocked based on VLANs.

As well as the two protocols above, multiple spanning tree protocol (MSTP) can disbranch a ring network to form a tree-topological ring-free network to prevent packets from being duplicated and forwarded endlessly in the ring network. Additionally, MSTP can also provide multiple redundant paths for packet forwarding to implement VLAN-based load balancing.

MSTP is compatible with both STP and RSTP. It overcomes the drawback of STP and RSTP. It not only enables spanning trees to converge rapidly, but also enables packets of different VLANs to be forwarded along their respective paths to provide a better load balancing mechanism for redundant links.

1.1.1 MSTP Protocol Data Unit

Bridge protocol data unit (BPDU), which is also called configuration message, is the protocol data unit (PDU) that STP and RSTP use.

The switches in a network transfer BPDUs between each other to determine the topology of the network. BPDUs carry enough information needed for spanning tree calculation.

BPDUs used in STP fall into the following two categories:

- Configuration BPDUs: BPDUs of this type are used to maintain the spanning tree topology.
- Topology change notification BPDU (TCN BPDN): BPDUs of this type are used to notify the switches of network changes.

Similar to STP and RSTP, MSTP uses BPDUs for spanning tree calculation too. Besides, the BPDUs of MSTP carry MSTP configuration information of the switches.

1.1.2 Basic MSTP Terminologies

Figure 1-1 illustrates basic MSTP terms (assuming that MSTP is enabled on each switch in this figure).

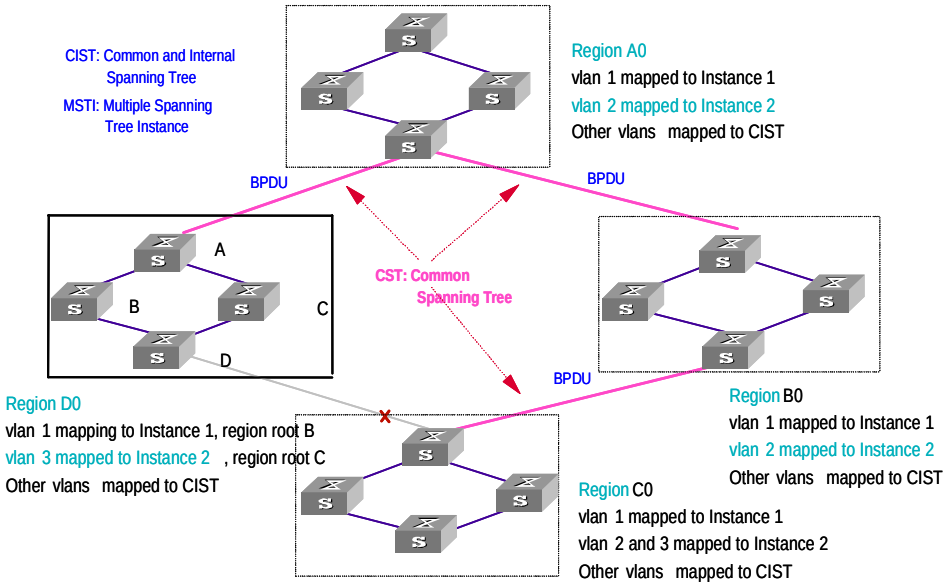


Figure 1-1 Basic MSTP terminologies

I. MST region

A multiple spanning tree region (MST region) comprises multiple physically-interconnected MSTP-enabled switches and the corresponding network segments connected to these switches. These switches have the same region name, the same VLAN-to-MSTI mapping configuration and the same MSTP revision level.

A switched network can contain multiple MST regions. You can group multiple switches into one MST region by using the corresponding MSTP configuration commands. For example, all switches in region A0 shown in Figure 1-1 have the same MST region configuration: the same region name, the same VLAN-to-MSTI mappings (that is, VLAN 1 is mapped to spanning tree instance 1, VLAN 2 is mapped to spanning tree instance 2, and other VLANs are mapped to CIST), and the same MSTP revision level (not shown in Figure 1-1).

II. MSTI

A multiple spanning tree instance (MSTI) refers to a spanning tree in an MST region.

Multiple spanning trees can be established in one MST region. These spanning trees are independent of each other. For example, each region in Figure 1-1 contains multiple spanning trees known as MSTIs. Each of these spanning trees corresponds to a VLAN.

III. VLAN mapping table

A VLAN mapping table is a property of an MST region. It contains information about how VLANs are mapped to MSTIs. For example, in Figure 1-1, the VLAN mapping table of region A0 is: VLAN 1 is mapped to MSTI 1; VLAN 2 is mapped to MSTI 2; and other VLANs are mapped to CIST. In an MST region, load balancing is implemented according to the VLAN mapping table.

IV. IST

An internal spanning tree (IST) is a spanning tree in an MST region.

ISTs together with the common spanning tree (CST) form the common and internal spanning tree (CIST) of the entire switched network. An IST is a special MSTI; it is a branch of CIST in the MST region. In Figure 1-1, each MST region has an IST, which is a branch of the CIST.

V. CST

A CST is a single spanning tree in a switched network that connects all MST regions in the network. If you regard each MST region in the network as a switch, then the CST is the spanning tree generated by STP or RSTP running on the "switches". In Figure 1-1, the lines in red depict the CST.

VI. CIST

A CIST is the spanning tree in a switched network that connects all switches in the network. It comprises the ISTs and the CST. In Figure 1-1, the ISTs in the MST regions and the CST connecting the MST regions form the CIST.

VII. Region root

A region root is the root of the IST or an MSTI in an MST region. Different spanning trees in an MST region may have different topologies and thus have different region roots. In region D0 shown in Figure 1-1, the region root of MSTI 1 is switch B, and the region root of MSTI 2 is switch C.

VIII. Common root bridge

The common root bridge is the root of the CIST. The common root bridge of the network shown in Figure 1-1 is a switch in region A0.

IX. Port role

During MSTP calculation, the following port roles exist: root port, designated port, master port, region edge port, alternate port, and backup port.

- A root port is used to forward packets to the root.
- A designated port is used to forward packets to a downstream network segment or switch.

- A master port connects an MST region to the common root. The path from the master port to the common root is the shortest path between the MST region and the common root.
- A region edge port is located on the edge of an MST region and is used to connect one MST region to another MST region, an STP-enabled region or an RSTP-enabled region
- An alternate port is a backup port of a master port. It becomes the master port if the existing master port is blocked.
- A loop occurs when two ports of a switch are connected to each other. In this case, the switch blocks one of the two ports. The blocked port is a backup port.

In Figure 1-2, switch A, switch B, switch C, and switch D form an MST region. Port 1 and port 2 on switch A connect upstream to the common root. Port 5 and port 6 on switch C form a loop. Port 3 and port 4 on switch D connect downstream to other MST regions. This figure shows the roles these ports play.

Note:

- A port can play different roles in different MSTIs.
- The role a region edge port plays is consistent with the role it plays in the CIST. For example, port 1 on switch A in Figure 1-2 is a region edge port, and it is a master port in the CIST. So it is a master port in all MSTIs in the region.

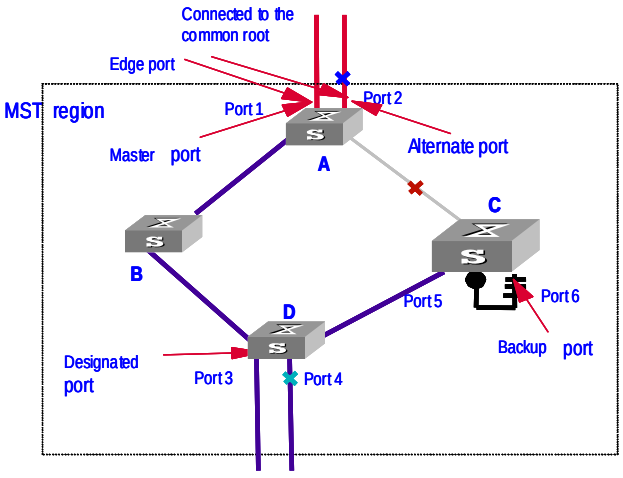


Figure 1-2 Port roles

X. Port state

Ports can be in one of the following three states:

- Forwarding state: Ports in this state can forward user packets and receive/send BPDU packets.
- Learning state: Ports in this state can receive/send BPDU packets.
- Discarding state: Ports in this state can only receive BPDU packets.

Port roles and port states are not mutually dependent. Table 1-1 lists possible combinations of port states and port roles.

Table 1-1 Combinations of port states and port roles

Port role / Port state	Root/ port/Master port	Designated port	Region edge port	Alternate port	Backup port
Forwarding	√	√	√	—	—
Learning	√	√	√	—	—
Discarding	√	√	√	√	√

1.1.3 Principle of MSTP

MSTP divides a Layer 2 network into multiple MST regions. The CSTs are generated between these MST regions, and multiple spanning trees (also called MSTIs) can be generated in each MST region. As well as RSTP, MSTP uses configuration BPDUs for spanning tree calculation. The only difference is that the configuration BPDUs for MSTP carry the MSTP configuration information on the switches.

I. Calculate the CIST

Through comparing configuration BPDUs, the switch of the highest priority in the network is selected as the root of the CIST. In each MST region, an IST is calculated by MSTP. At the same time, MSTP regards each MST region as a switch to calculate the CSTs of the network. The CSTs, together with the ISTs, form the CIST of the network.

II. Calculate an MSTI

In an MST region, different MSTIs are generated for different VLANs based on the VLAN-to-MSTI mappings. Each spanning tree is calculated independently, in the same way as how STP/RSTP is calculated.

III. Implement STP algorithm

In the beginning, each switch regards itself as the root, and generates a configuration BPDU for each port on it as a root, with the root path cost being 0, the ID of the designated bridge being that of the switch, and the designated port being itself.

1) Each switch sends out its configuration BPDUs and operates in the following way when receiving a configuration BPDU on one of its ports from another switch:

- If the priority of the configuration BPDU is lower than that of the configuration BPDU of the port itself, the switch discards the BPDU and does not change the configuration BPDU of the port.
- If the priority of the configuration BPDU is higher than that of the configuration BPDU of the port itself, the switch replaces the configuration BPDU of the port with the received one and compares it with those of other ports on the switch to obtain the one with the highest priority.

2) Configuration BPDUs are compared as follows:

- The smaller the root ID of the configuration BPDU is, the higher the priority of the configuration BPDU is.
- For configuration BPDUs with the same root IDs, the path costs are compared. Suppose S is the sum of the root path costs and the corresponding path cost of the port. The less the S value is, the higher the priority of the configuration BPDU is.
- For configuration BPDUs with both the same root ID and the same root path cost, the designated bridge ID, designated port ID, the ID of the receiving port are compared in turn.

3) A spanning tree is calculated as follows:

- Determining the root bridge

Root bridges are selected by configuration BPDU comparing. The switch with the smallest root ID is chosen as the root bridge.

- Determining the root port

For each switch in a network, the port on which the configuration BPDU with the highest priority is received is chosen as the root port of the switch.

- Determining the designated port

First, the switch calculates a designated port configuration BPDU for each of its ports using the root port configuration BPDU and the root port path cost, with the root ID being replaced with that of the root port configuration BPDU, root path cost being replaced with the sum of the root path cost of the root port configuration BPDU and the path cost of the root port, the ID of the designated bridge being replaced with that of the switch, and the ID of the designated port being replaced with that of the port.

The switch then compares the calculated configuration BPDU with the original configuration BPDU received from the corresponding port on another switch. If the latter takes precedence over the former, the switch blocks the local port and keeps the port's configuration BPDU unchanged, so that the port can only receive configuration messages and cannot forward packets. Otherwise, the switch sets the local port to the designated port, replaces the original configuration BPDU of the port with the calculated one and advertises it regularly.

1.1.4 MSTP Implementation on Switches

MSTP is compatible with both STP and RSTP. That is, MSTP-enabled switches can recognize the protocol packets of STP and RSTP and use them for spanning tree calculation. In addition to the basic MSTP functions, H3C series switches also provide the following functions for the convenience of users to manage their switches:

- Root bridge hold
- Root bridge backup
- Root protection
- BPDU protection
- Loop prevention

1.2 Configuring Root Bridge

Table 1-2 lists MSTP-related configurations about root bridges.

Table 1-2 Configure root bridge

Operation	Description	Related section
Enable the MSTP feature	Required To prevent network topology jitter caused by other related configurations, you are recommended to enable the MSTP feature after other related configurations are performed.	Section 1.2.14 “Enabling the MSTP Feature”
Configure the MST region	Required	Section 1.2.2 “Configuring the MST Region”
Specify the current switch as a root bridge/secondary root bridge	Required	Section 1.2.3 “Specifying the Current Switch as a Root Bridge/Secondary Root Bridge”
Configure the bridge priority of the current switch	Optional The priority of a switch cannot be changed after the switch is specified as the root bridge or a secondary root bridge.	Section 1.2.4 “Configuring the Bridge Priority of the Current Switch”
Configure the MSTP packet format	Optional	Section 1.2.5 “Configuring the MSTP Packet Format”

Operation	Description	Related section
Configure the MSTP operation mode	Optional	Section 1.2.6 “Configuring the MSTP Operation Mode”
Configure the maximum hops of MST region	Optional	Section 1.2.7 “Configuring the Maximum Hops of MST Region”
Configure the network diameter of the switched network	Optional The default value is recommended.	Section 1.2.8 “Configuring the Network Diameter of the Switched Network”
Configure the MSTP time-related parameters	Optional The default values are recommended.	Section 1.2.9 “Configuring the MSTP Time-related Parameters”
Configure the timeout time factor	Optional	Section 1.2.10 “Configuring the Timeout Time Factor”
Configure the maximum transmitting speed on the current port	Optional The default value is recommended.	Section 1.2.11 “Configuring the Maximum Transmitting Speed on the Current Port”
Configure the current port as an edge port	Optional	Section 1.2.12 “Configuring the Current Port as an Edge Port”
Specify whether the link connected to a port is a point-to-point link	Optional	Section 1.2.13 “Specifying Whether the Link Connected to a Port Is Point-to-point Link”

Note:

In a network containing switches with both GVRP and MSTP enabled, GVRP packets are forwarded along the CIST. If you want to advertise packets of a specific VLAN through GVRP, be sure to map the VLAN to the CIST when configuring the MSTP VLAN mapping table (the CIST of a network is spanning tree instance 0).

1.2.1 Configuration Prerequisites

The role (root, branch, or leaf) of each switch in each spanning tree instance is determined.

1.2.2 Configuring the MST Region

I. Configuration procedure

Table 1-3 Configure an MST region

Operation	Command	Description
Enter system view	**system-view**	—
Enter MST region view	**stp region-configuration**	—
Configure the name of the MST region	**region-name** *name*	Required The default MST region name of a switch is its MAC address.
Configure the VLAN mapping table for the MST region	**instance** *instance-id* **vlan** *vlan-list*	Required Both commands can be used to configure VLAN mapping tables. By default, all VLANs in an MST region are mapped to spanning tree instance 0.
	vlan-mapping modulo *modulo*	
Configure the MSTP revision level for the MST region	**revision-level** *level*	Required The default revision level of an MST region is level 0.
Activate the configuration of the MST region manually	**active region-configuration**	Required
Display the configuration of the current MST region	**check region-configuration**	Optional
Display the currently valid configuration of the MST region	**display stp region-configuration**	You can execute this command in any view.

Configuring MST region-related parameters (especially the VLAN mapping table) results in spanning tree recalculation and network topology jitter. To reduce network topology jitter caused by the configuration, MSTP does not recalculate spanning trees immediately after the configuration; it does this only after you perform one of the following operations, and then the configuration can really takes effect:

- Activate the new MST region-related settings by using the **active region-configuration** command
- Enable MSTP by using the **stp enable** command

Note:

Switches belong to the same MST region only when they have the same MST region name, VLAN mapping table, and MSTP revision level.

II. Configuration example

Configure an MST region, with the name being “info”, the MSTP revision level being level 1, VLAN 2 through VLAN 10 being mapped to spanning tree instance 1, and VLAN 20 through VLAN 30 being mapped to spanning tree 2.

```
<H3C> system-view
[H3C] stp region-configuration
[H3C-mst-region] region-name info
[H3C-mst-region] instance 1 vlan 2 to 10
[H3C-mst-region] instance 2 vlan 20 to 30
[H3C-mst-region] revision-level 1
[H3C-mst-region] active region-configuration
```

Verify the above configuration.

```
[H3C-mst-region] check region-configuration
Admin configuration
   Format selector    :0
   Region name        :info
   Revision level     :1

   Instance   Vlans Mapped
      0       11 to 19, 31 to 4094
      1       1 to 10
      2       20 to 30
```

1.2.3 Specifying the Current Switch as a Root Bridge/Secondary Root Bridge

MSTP can automatically choose a switch as a root bridge through calculation. You can also manually specify the current switch as a root bridge by using the corresponding commands.

I. Specify the current switch as the root bridge of a specified spanning tree

Table 1-4 Specify the current switch as the root bridge of a specified spanning tree

Operation	Command	Description
Enter system view	**system-view**	—

Operation	Command	Description
Specify the current switch as the root bridge of a specified spanning tree	**stp** [**instance** *instance-id*] **root primary** [**bridge-diameter** *bridgenumber*] [**hello-time** *centi-seconds*]	Required

II. Specify the current switch as the secondary root bridge of a specified spanning tree

Table 1-5 Specify the current switch as the secondary root bridge of a specified spanning tree

Operation	Command	Description
Enter system view	**system-view**	—
Specify the current switch as the secondary root bridge of a specified spanning tree	**stp** [**instance** *instance-id*] **root secondary** [**bridge-diameter** *bridgenumber*] [**hello-time** *centi-seconds*]	Required

Using the **stp root primary**/**stp root secondary** command, you can specify the current switch as the root bridge or the secondary root bridge of the spanning tree instance identified by the *instance-id* argument. If the value of the *instance-id* argument is set to 0, the **stp root primary**/**stp root secondary** command specify the current switch as the root bridge or the secondary root bridge of the CIST.

A switch can play different roles in different spanning tree instances. That is, it can be the root bridges in a spanning tree instance and be a secondary root bridge in another spanning tree instance at the same time. But in the same spanning tree instance, a switch cannot be the root bridge and the secondary root bridge simultaneously.

When the root bridge fails or is turned off, the secondary root bridge becomes the root bridge if no new root bridge is configured. If you configure multiple secondary root bridges for a spanning tree instance, the one with the smallest MAC address replaces the root bridge when the latter fails.

You can specify the network diameter and the hello time parameters while configuring a root bridge/secondary root bridge. Refer to section 1.2.8 “Configuring the Network Diameter of the Switched Network” and 1.2.9 “Configuring the MSTP Time-related Parameters” for information about the network diameter parameter and the hello time parameter.

Note:

- You can configure a switch as the root bridges of multiple spanning tree instances. But you cannot configure two or more root bridges for one spanning tree instance. So, do not configure root bridges for the same spanning tree instance on two or more switches using the **stp root primary** command.
- You can configure multiple secondary root bridges for one spanning tree instance. That is, you can configure secondary root bridges for the same spanning tree instance on two or more switches using the **stp root secondary** command.
- You can also configure the current switch as the root bridge by setting the priority of the switch to 0. Note that once a switch is configured as the root bridge or a secondary root bridge, its priority cannot be modified.

III. Configuration example

Configure the current switch as the root bridge of spanning tree instance 1 and a secondary root bridge of spanning tree instance 2.

```
<H3C> system-view
[H3C] stp instance 1 root primary
[H3C] stp instance 2 root secondary
```

1.2.4 Configuring the Bridge Priority of the Current Switch

Root bridges are selected according to the bridge priorities of switches. You can make a specific switch be selected as a root bridge by setting a lower bridge priority for the switch. An MSTP-enabled switch can have different bridge priorities in different spanning tree instances.

I. Configuration procedure

Table 1-6 Configure the bridge priority of the current switch

Operation	Command	Description
Enter system view	**system-view**	—
Set the bridge priority for the current switch	**stp** [**instance** *instance-id*] **priority** *priority*	Required The default bridge priority of a switch is 32,768.

Caution:

- Once you specify a switch as the root bridge or a secondary root bridge by using the **stp root primary** or **stp root secondary** command, the bridge priority of the switch cannot be configured any more.
- During the selection of the root bridge, if multiple switches have the same bridge priority, the one with the smallest MAC address becomes the root bridge.

II. Configuration example

Set the bridge priority of the current switch to 4,096 in spanning tree instance 1.

```
<H3C> system-view
[H3C] stp instance 1 priority 4096
```

1.2.5 Configuring the MSTP Packet Format

You can set the MSTP packet format to the following three formats for a port: **auto**, **legacy**, and **dot1s** (802.1s).

- With the MSTP packet format set to **auto**, the port automatically determines the format of the received MSTP packets (**legacy** or **dot1s**) and then decides the format of packets to be transmitted, thus implementing communication with the peer device. If the format of the received packets from the peer device changes repeatedly, MSTP will shut down the corresponding port to prevent network storm. A port shut down in this way can only be enabled again by the network administrator after login.
- With the MSTP packet format set to **legacy**, the port processes and transmits only MSTP packets in **legacy** format, thus implementing communication with the peer device sending packets in **legacy** format. If packets in **dot1s** format are received, the corresponding ports are set to the discarding state to prevent network storm.
- With the MSTP packet format set to **dot1s**, the port processes and transmits only MSTP packets in **dot1s** format, thus implementing communication with the peer device sending packets in **dot1s** format. If packets in **legacy** format are received, the corresponding ports are set to the discarding state to prevent network storm.
- All the ports in an aggregation group use the same MSTP packet format.

I. Configuration procedure

Table 1-7 Configure MSTP packet format for the port

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure MSTP packet format for the port	**stp compliance** { **auto** | **dot1s** | **legacy** }	Required By default, an MSTP packet is in **legacy** format.

II. Configuration example

Configure the MSTP packet format as **dot1s** (802.1s).

```
<H3C> system-view
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] stp compliance dot1s
```

Restore the MSTP packet format to the default value.

```
[H3C-Ethernet1/0/1] undo stp compliance
```

1.2.6 Configuring the MSTP Operation Mode

A MSTP-enabled switch can operate in one of the following operation modes:

- STP-compatible mode: In this mode, all ports of the switches send STP packets. If the switched network contains STP-enabled switches, you can configure the current MSTP-enabled switch to operate in this mode by using the **stp mode stp** command.
- RSTP-compatible mode: In this mode, all ports of the switches send RSTP packets. If the switched network contains RSTP-enabled switches, you can configure the current MSTP-enabled switch to operate in this mode by using the **stp mode rstp** command.
- MSTP mode: In this mode, all the ports of the switches send MSTP packets or STP packets (if the port is connected to an STP-enabled switch). In this case, the multiple spanning tree function is enabled as well.

I. Configuration procedure

Table 1-8 Configure the MSTP operation mode

Operation	Command	Description
Enter system view	**system-view**	—
Configure the MSTP operation mode	**stp mode** { **stp** | **rstp** | **mstp** }	Required An MSTP-enabled switch operates in the MSTP mode by default.

II. Configuration example

Configure the current MSTP-enabled switch to operate in the STP-compatible mode.

```
<H3C> system-view
[H3C] stp mode stp
```

1.2.7 Configuring the Maximum Hops of MST Region

The maximum hops configured on the region root is also the maximum hops of an MST region. The value of the maximum hops limits the size of the MST region.

A configuration BPDU contains a field that maintains the remaining hops of the configuration BPDU. And a switch discards the configuration BPDUs whose remaining hops are 0. After a configuration BPDU reaches a root bridge of a spanning tree in an MST region, the value of the remaining hops field in the configuration BPDU is decreased by 1 every time the configuration BPDU passes one switch. Such a mechanism disables the switches that are beyond the maximum hops from participating in spanning tree calculation, and thus limits the size of an MST region.

With such a mechanism, the maximum hops configured on the switch operating as the root bridge of the CIST or an MSTI in an MST region becomes the network diameter of the spanning tree, which limits the size of the spanning tree in the current MST region. The switches that are not root bridges in the MST region adopt the maximum hop settings of their root bridges.

I. Configuration procedure

Table 1-9 Configure the maximum hops for an MST region

Operation	Command	Description
Enter system view	**system-view**	—
Configure the maximum hops of the MST region	**stp max-hops** *hops*	Required By default, the maximum hops of an MST region are 20.

The bigger the maximum hops are in an MST region, the larger the MST region is. Note that only the maximum hop settings on the switch operating as a region root can limit the size of the MST region.

II. Configuration example

Configure the maximum hops of the MST region to be 30.

```
<H3C> system-view
[H3C] stp max-hops 30
```

1.2.8 Configuring the Network Diameter of the Switched Network

In a switched network, any two switches can communicate with each other through a specific path made up of multiple switches. The network diameter of a network is measured by the number of switches; it equals the number of the switches on the longest path (that is, the path containing the maximum number of switches).

I. Configuration procedure

Table 1-10 Configure the network diameter of the switched network

Operation	Command	Description
Enter system view	**system-view**	—
Configure the network diameter of the switched network	**stp bridge-diameter** *bridgenumber*	Required The default network diameter of a network is 7.

The network diameter parameter indicates the size of a network. The bigger the network diameter is, the larger the network size is.

After you configure the network diameter of a switched network, an MSTP-enabled switch adjusts its hello time, forward delay, and max age settings accordingly to better values.

The network diameter setting only applies to only CIST; it is invalid for MSTIs.

II. Configuration example

Configure the network diameter of the switched network to 6.

```
<H3C> system-view
[H3C] stp bridge-diameter 6
```

1.2.9 Configuring the MSTP Time-related Parameters

You can configure three MSTP time-related parameters for a switch: forward delay, hello time, and max age.

- The forward delay parameter sets the delay of state transition.

Link failures in a network result in the spanning tree recalculation and spanning tree structure change. As the newly calculated configuration BPDUs cannot be advertised across the entire network immediately when the new spanning trees are calculated, temporary loops may occur if the new root ports and designated ports begin to forward packets immediately.

This problem can be solved by adopting a state transition mechanism. With this mechanism, newly selected root ports and designated ports undergo an intermediate state before they begin to forward packets. That is, it costs these ports a period (specified by the forward delay parameter) for them to turn to the forwarding state. In the period, the newly calculated configuration BPDUs are advertised across the entire network.

- The hello time parameter is used for testing link failures.

A switch regularly sends hello packets to other switches at the interval specified by the hello time parameter to test whether the links fail.

- The max age parameter is used to judge whether or not a configuration BPDU times out. The configuration BPDUs which time out will be discarded.

I. Configuration procedure

Table 1-11 Configure MSTP time-related parameters

Operation	Command	Description
Enter system view	**system-view**	—
Configure the forward delay parameter	**stp timer forward-delay** *centiseconds*	Required The forward delay parameter defaults to 1,500 centiseconds (namely, 15 seconds).
Configure the hello time parameter	**stp timer hello** *centiseconds*	Required The hello time parameter defaults to 200 centiseconds (namely, 2 seconds).
Configure the max age parameter	**stp timer max-age** *centiseconds*	Required The max age parameter defaults to 2,000 centiseconds (namely, 20 seconds).

All switches in a switched network adopt the three time-related parameters configured on the CIST root bridge.

Caution:

- The forward delay parameter and the network diameter are correlated. Normally, a large network diameter corresponds to a large forward delay. A too small forward delay parameter may result in temporary redundant paths. And a too large forward delay parameter may cause a network unable to resume the normal state in time after changes occurred to the network. The default value is recommended.
- An adequate hello time parameter enables a switch to detect link failures in time without occupying too many network resources. And a too small hello time parameter may result in duplicated configuration BPDUs being sent frequently, which increases the work load of the switches and wastes network resources. The default value is recommended.
- As for the max age parameter, if it is too small, network congestion may be falsely regarded as link failures, which results in frequent spanning tree recalculation. If it is too large, link problems may be unable to be detected in time, which prevents spanning trees being recalculated in time and makes the network less adaptive. The default value is recommended.

As for the configuration of the three time-related parameters (that is, the hello time, forward delay, and max age parameters), the following formulas must be met to prevent frequent network jitter.

2 x (forward delay – 1 second) >= max age

Max age >= 2 x (hello time + 1 second)

You are recommended to specify the network diameter of the switched network and the hello time by using the **stp root primary** or **stp root secondary** command. After that, the three proper time-related parameters are determined automatically.

II. Configuration example

Configure the forward delay parameter to be 1,600 centiseconds, the hello time parameter to be 300 centiseconds, and the max age parameter to be 2,100 centiseconds (assuming that the current switch operates as the CIST root bridge).

```
<H3C> system-view
[H3C] stp timer forward-delay 1600
[H3C] stp timer hello 300
[H3C] stp timer max-age 2100
```

1.2.10 Configuring the Timeout Time Factor

A switch regularly sends protocol packets to its neighboring devices at the interval specified by the hello time parameter to test the link failures. Normally, a switch regards

its upstream switch faulty if the former does not receive any protocol packets from the latter in a period three times of the hello time and then initiates the spanning tree recalculation process.

Spanning trees may be recalculated even in a steady network if an upstream switch continues to be busy. You can configure the timeout time factor to a larger number to avoid such cases. Normally, the timeout time can be four or more times of the hello time. For a steady network, the timeout time can be five to seven times of the hello time.

I. Configuration procedure

Table 1-12 Configure the timeout time factor

Operation	Command	Description
Enter system view	**system-view**	—
Configure the timeout time factor for the switch	**stp timer-factor** *number*	Required The timeout time factor defaults to 3.

For a steady network, the timeout time can be five to seven times of the hello time.

II. Configuration example

Configure the timeout time factor to be 6.

```
<H3C> system-view
[H3C] stp timer-factor 6
```

1.2.11 Configuring the Maximum Transmitting Speed on the Current Port

The maximum transmitting speed of a port specifies the maximum number of configuration BPDUs a port can transmit in a period specified by the hello time parameter. It depends on the physical state of the port and network structure. You can configure this parameter according to the network.

I. Configure the maximum transmitting speed for specified ports in system view

Table 1-13 Configure the maximum transmitting speed for specified ports in system view

Operation	Command	Description
Enter system view	**system-view**	—
Configure the maximum transmitting speed for specified ports	**stp interface** *interface-list* **transmit-limit** *packetnum*	Required The maximum transmitting speed of all Ethernet ports on a switch defaults to 10.

II. Configure the maximum transmitting speed in Ethernet port view

Table 1-14 Configure the maximum transmitting speed in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the maximum transmitting speed	**stp transmit-limit** *packetnum*	Required The maximum transmitting speed of all Ethernet ports on a switch defaults to 10.

As the maximum transmitting speed parameter determines the number of the configuration BPDUs transmitted in each hello time, set it to a proper value to prevent MSTP from occupying too many network resources. The default value is recommended.

III. Configuration example

Set the maximum transmitting speed of Ethernet1/0/1 to 15.

1) Configure the maximum transmitting speed in system view.

```
<H3C> system-view
[H3C] stp interface Ethernet1/0/1 transmit-limit 15
```

2) Configure the maximum transmitting speed in Ethernet port view.

```
<H3C> system-view
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] stp transmit-limit 15
```

1.2.12 Configuring the Current Port as an Edge Port

Edge ports are ports that neither directly connects to other switches nor indirectly connects to other switches through network segments. After a port is configured as an edge port, the rapid transition mechanism is applicable to the port. That is, when the port changes from the blocking state to the forwarding state, it does not have to wait for a delay.

You can configure a port as an edge port in one of the following two ways.

I. Configure a port as an edge port in system view

Table 1-15 Configure a port as an edge port in system view

Operation	Command	Description
Enter system view	**system-view**	—
Configure the specified ports as edge ports	**stp interface** *interface-list* **edged-port enable**	Required By default, all the Ethernet ports of a switch are non-edge ports.

II. Configure a port as an edge port in Ethernet port view

Table 1-16 Configure a port as an edge port in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the port as an edge port	**stp edged-port enable**	Required By default, all the Ethernet ports of a switch are non-edge ports.

On a switch with BPDU protection disabled, an edge port becomes a non-edge port again once it receives a BPDU from another port.

Note:

You are recommended to configure the Ethernet ports connected directly to terminals as edge ports and enable the BPDU protection function at the same time. This not only enables these ports to turn to the forwarding state rapidly but also secures your network.

III. Configuration example

Configure Ethernet1/0/1 as an edge port.

1) Configure Ethernet1/0/1 as an edge port in system view.

```
<H3C> system-view
[H3C] stp interface Ethernet1/0/1 edged-port enable
```

2) Configure Ethernet1/0/1 as an edge port in Ethernet port view.

```
<H3C> system-view
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] stp edged-port enable
```

1.2.13 Specifying Whether the Link Connected to a Port Is Point-to-point Link

A point-to-point link directly connects two switches. If the roles of the two ports at the two ends of a point-to-point link meet certain criteria, the two ports can turn to the forwarding state rapidly by exchanging synchronization packets, thus reducing the forward delay.

You can determine whether or not the link connected to a port is a point-to-point link in one of the following two ways.

I. Specify whether the link connected to a port is point-to-point link in system view

Table 1-17 Specify whether the link connected to a port is point-to-point link in system view

Operation	Command	Description
Enter system view	**system-view**	—
Specify whether the link connected to a port is point-to-point link	**stp interface** *interface-list* **point-to-point** { **force-true** | **force-false** | **auto** }	Required The **auto** keyword is adopted by default. The **force-true** keyword specifies that the links connected to the specified ports are point-to-point links. The **force-false** keyword specifies that the links connected to the specified ports are not point-to-point links. The **auto** keyword specifies to automatically determine whether or not the links connected to the specified ports are point-to-point links.

II. Specify whether the link connected to a port is point-to-point link in Ethernet port view

Table 1-18 Specify whether the link connected to a port is point-to-point link in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Specify whether the link connected to a port is a point-to-point link	**stp point-to-point** { **force-true** | **force-false** | **auto** }	Required The **auto** keyword is adopted by default. The **force-true** keyword specifies that the link connected to the port is a point-to-point link. The **force-false** keyword specifies that the link connected to the port is not a point-to-point link. The **auto** keyword specifies to automatically determine whether or not the link connected to the port is a point-to-point link.

Note:

- Among aggregated ports, you can only configure the links of master ports as point-to-point links.
- If an auto-negotiating port operates in full duplex mode after negotiation, you can configure the link of the port as a point-to-point link.

After you configure the link of a port as a point-to-point link, the configuration applies to all spanning tree instances. If the actual physical link of a port is not a point-to-point link and you forcibly configure the link as a point-to-point link, temporary loops may be incurred.

III. Configuration example

Configure the link connected to Ethernet1/0/1 as a point-to-point link.

1) Perform this configuration in system view.

```
<H3C> system-view
```

```
[H3C] stp interface Ethernet1/0/1 point-to-point force-true
```

2) Perform this configuration in Ethernet port view.

```
<H3C> system-view
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] stp point-to-point force-true
```

1.2.14 Enabling the MSTP Feature

I. Configuration procedure

Table 1-19 Enable the MSTP feature in system view

Operation	Command	Description
Enter system view	**system-view**	—
Enable the MSTP feature	**stp enable**	Required MSTP is disabled by default.
Disable the MSTP feature on specified ports	**stp interface** *interface-list* **disable**	Optional By default, the MSTP feature is enabled on all ports after you enable the MSTP feature in system view. To enable a switch to operate more flexibly, you can disable MSTP on specific ports. As MSTP-disabled ports do not participate in spanning tree calculation, this operation saves CPU resources of the switch.

Table 1-20 Enable the MSTP feature in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enable the MSTP feature	**stp enable**	Required MSTP is disabled by default.
Enter Ethernet port view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Disable the MSTP feature on the port	**stp disable**	Optional By default, MSTP is enabled on all ports after you enable MSTP in system view. To enable a switch to operate more flexibly, you can disable MSTP on specific ports. As MSTP-disabled ports do not participate in spanning tree calculation, this operation saves CPU resources of the switch.

Other MSTP-related settings can take effect only after MSTP is enabled on the switch.

II. Configuration example

Enable MSTP on the switch and disable MSTP on Ethernet1/0/1.

1) Perform this configuration in system view.

```
<H3C> system-view
[H3C] stp enable
[H3C] stp interface Ethernet1/0/1 disable
```

2) Perform this configuration in Ethernet port view.

```
<H3C> system-view
[H3C] stp enable
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] stp disable
```

1.3 Configuring Leaf Nodes

Table 1-21 lists MSTP-related configurations about leaf nodes.

Table 1-21 Configure leaf nodes

Operation	Description	Related section
Enable the MSTP feature	Required To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after performing other configurations.	Section 1.2.14 “Enabling the MSTP Feature”

Operation	Description	Related section
Configure the MST region	Required	Section 1.2.2 “Configuring the MST Region”
Configure the MSTP operation mode	Optional	Section 1.2.5 “Configuring the MSTP Packet Format”
Configure the timeout time factor	Optional	Section 1.2.10 “Configuring the Timeout Time Factor”
Configure the maximum transmitting speed on the current port	Optional The default value is recommended.	Section 1.2.11 “Configuring the Maximum Transmitting Speed on the Current Port”
Configure the current port as an edge port	Optional	Section 1.2.12 “Configuring the Current Port as an Edge Port”
Configure the path cost for a port	Optional	Section 1.3.7 “Configuring the Path Cost for a Port”
Configure the port priority	Optional	Section 1.3.8 “Configuring Port Priority”
Specify whether the link connected to a port is point-to-point link	Optional	Section 1.2.13 “Specifying Whether the Link Connected to a Port Is Point-to-point Link”

Note:

In a network containing switches with both GVRP and MSTP enabled, GVRP packets are forwarded along the CIST. In this case, if you want to broadcast packets of a specific VLAN through GVRP, be sure to map the VLAN to the CIST when configuring the MSTP VLAN mapping table (the CIST of a network is spanning tree instance 0).

1.3.1 Configuration Prerequisites

The role (root, branch, or leaf) of each switch in each spanning tree instance is determined.

1.3.2 Configuring the MST Region

Refer to section 1.2.2 “Configuring the MST Region”.

1.3.3 Configuring the MSTP Operation Mode

Refer to section 1.2.6 “Configuring the MSTP Operation Mode”.

1.3.4 Configuring the Timeout Time Factor

Refer to section 1.2.10 “Configuring the Timeout Time Factor”.

1.3.5 Configuring the Maximum Transmitting Speed

Refer to section 1.2.11 “Configuring the Maximum Transmitting Speed on the Current Port”.

1.3.6 Configuring a Port as an Edge

Refer to section 1.2.12 “Configuring the Current Port as an Edge Port”.

1.3.7 Configuring the Path Cost for a Port

The path cost parameter reflects the rate of the link connected to the port. For a port on an MSTP-enabled switch, the path cost may be different in different spanning tree instances. You can enable flows of different VLANs to travel along different physical links by configuring appropriate path costs on ports, so that VLAN-based load balancing can be implemented.

Path cost of a port can be determined by the switch or through manual configuration.

I. Standards for calculating path costs of ports

Currently, a switch can calculate the path costs of ports based on one of the following standards:

- **dot1d-1998**: Adopts the IEEE 802.1D-1998 standard to calculate the default path costs of ports.
- **dot1t**: Adopts the IEEE 802.1t standard to calculate the default path costs of ports.
- **legacy**: Adopts the proprietary standard to calculate the default path costs of ports.

Table 1-22 Specify the standard for calculating path costs

Operation	Command	Description
Enter system view	**system-view**	—
Specify the standard for calculating the default path costs of the links connected to the ports of the switch	**stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }	Optional By default, the legacy standard is used to calculate the default path costs of ports.

Table 1-23 Transmission speeds and the corresponding path costs

Transmission speed	Operation mode (half-/full-duplex)	802.1D-1998	IEEE 802.1t	Proprietary standard
0	—	65,535	200,000,000	200,000
10 Mbps	Half-duplex/Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	100 95 95 95	200,000 1,000,000 666,666 500,000	2,000 1,800 1,600 1,400
100 Mbps	Half-duplex/Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	19 15 15 15	200,000 100,000 66,666 50,000	200 180 160 140
1,000 Mbps	Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	4 3 3 3	200,000 10,000 6,666 5,000	20 18 16 14
10 Gbps	Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	2 1 1 1	200,000 1,000 666 500	2 1 1 1

Normally, the path cost of a port operating in full-duplex mode is slightly less than that of the port operating in half-duplex mode.

When calculating the path cost of an aggregated link, the 802.1D-1998 standard does not take the number of the ports on the aggregated link into account, whereas the 802.1T standard does. The following formula is used to calculate the path cost of an aggregated link:

Path cost = 200,000/ link transmission speed.

In this formula, the link transmission speed is the sum of the speeds of all the unblocked ports on the aggregated link, which is measured in 100 Kbps.

II. Configure the path costs of ports

Table 1-24 Configure the path cost for specified ports in system view

Operation	Command	Description
Enter system view	**system-view**	—
Configure the path cost for specified ports	**stp interface** *interface-list* [**instance** *instance-id*] **cost** *cost*	Required An MSTP-enabled switch can calculate path costs for all its ports automatically.

Table 1-25 Configure the path cost for a port in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the path cost for the port	**stp** [**instance** *instance-id*] **cost** *cost*	Required A MSTP-enabled switch can calculate path costs for all its ports automatically.

Changing the path cost of a port may change the role of the port and put it in state transition. Executing the **stp cost** command with the *instance-id* argument being 0 sets the path cost on the CIST for the port.

III. Configuration example (A)

Configure the path cost of Ethernet1/0/1 in spanning tree instance 1 to be 2,000.

1) Perform this configuration in system view.

```
<H3C> system-view
[H3C] stp interface Ethernet1/0/1 instance 1 cost 2000
```

2) Perform this configuration in Ethernet port view.

```
<H3C> system-view
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] stp instance 1 cost 2000
```

IV. Configuration example (B)

Configure the path cost of Ethernet1/0/1 in spanning tree instance 1 to be calculated by the MSTP-enabled switch according to the IEEE 802.1D-1998 standard.

1) Perform this configuration in system view.

```
<H3C> system-view
[H3C] undo stp interface Ethernet1/0/1 instance 1 cost
[H3C] stp pathcost-standard dot1d-1998
```

2) Perform this configuration in Ethernet port view.

```
<H3C> system-view
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] undo stp instance 1 cost
[H3C-Ethernet1/0/1] quit
[H3C] stp pathcost-standard dot1d-1998
```

1.3.8 Configuring Port Priority

Port priority is an important criterion on determining the root port. In the same condition, the port with the smallest port priority value becomes the root port.

A port on an MSTP-enabled switch can have different port priorities and play different roles in different spanning tree instances. This enables packets of different VLANs to be forwarded along different physical paths, so that VLAN-based load balancing can be implemented.

You can configure port priority in one of the following two ways.

I. Configure port priority in system view

Table 1-26 Configure port priority in system view

Operation	Command	Description
Enter system view	**system-view**	—
Configure port priority for specified ports	**stp interface** *interface-list* **instance** *instance-id* **port priority** *priority*	Required The default port priority is 128.

II. Configure port priority in Ethernet port view

Table 1-27 Configure port priority in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Configure port priority for the port	**stp** [**instance** *instance-id*] **port priority** *priority*	Required. The default port priority is 128.

Changing port priority of a port may change the role of the port and put the port into state transition.

A smaller port priority value indicates a higher possibility for the port to become the root port. If all the ports of a switch have the same port priority value, the port priorities are determined by the port indexes. Changing the priority of a port will cause spanning tree recalculation.

You can configure port priorities according to actual networking requirements.

III. Configuration example

Configure the port priority of Ethernet1/0/1 in spanning tree instance 1 to be 16.

1) Perform this configuration in system view.

```
<H3C> system-view
[H3C] stp interface Ethernet1/0/1 instance 1 port priority 16
```

2) Perform this configuration in Ethernet port view.

```
<H3C> system-view
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] stp instance 1 port priority 16
```

1.3.9 Specifying Whether the Link Connected to a Port Is a Point-to-point Link

Refer to section 1.2.13 “Specifying Whether the Link Connected to a Port Is Point-to-point Link”.

1.3.10 Enabling the MSTP Feature

Refer to section 1.2.14 “Enabling the MSTP Feature”.

1.4 Performing mCheck

Ports on an MSTP-enabled switch can operate in three modes: STP-compatible, RSTP-compatible, and MSTP.

A port on an MSTP-enabled switch operating as an upstream switch transits to the STP-compatible mode when it has an STP-enabled switch connected to it. When the STP-enabled downstream switch is then replaced by an MSTP-enabled switch, the port cannot automatically transit to the MSTP mode. It remains in the STP-compatible

mode. In this case, you can force the port to transit to the MSTP mode by performing the mCheck operation on the port.

Similarly, a port on an RSTP-enabled switch operating as an upstream switch turns to the STP-compatible mode when it has an STP-enabled switch connected to it. When the STP enabled downstream switch is then replaced by an MSTP-enabled switch, the port cannot automatically transit to the MSTP-compatible mode. It remains in the STP-compatible mode. In this case, you can force the port to transit to the MSTP-compatible mode by performing the mCheck operation on the port.

1.4.1 Configuration Prerequisites

MSTP runs normally on the switch.

1.4.2 Configuration Procedure

Perform the mCheck operation in the following two ways.

I. Perform the mCheck operation in system view

Table 1-28 Perform the mCheck operation in system view

Operation	Command	Description
Enter system view	**system-view**	—
Perform the mCheck operation	**stp** [**interface** *interface-list*] **mcheck**	Required

II. Perform the mCheck operation in Ethernet port view

Table 1-29 Perform the mCheck operation in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Perform the mCheck operation	**stp mcheck**	Required

1.4.3 Configuration Example

Perform the mCheck operation on Ethernet1/0/1.

1) Perform this configuration in system view.

```
<H3C> system-view
[H3C] stp interface Ethernet1/0/1 mcheck
```

2) Perform this configuration in Ethernet port view.

```
<H3C> system-view
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] stp mcheck
```

1.5 Configuring Protection Function

1.5.1 Introduction

The following protection functions are available on an MSTP-enabled switch: BPDU protection, root protection, loop prevention, and TC-BPDU attack prevention.

I. BPDU protection

Normally, the access ports of the devices operating on the access layer are directly connected to terminals (such as PCs) or file servers. These ports are usually configured as edge ports to achieve rapid transition. But they resume non-edge ports automatically upon receiving configuration BPDUs, which causes spanning tree recalculation and network topology jitter.

Normally, no configuration BPDU will reach edge ports. But malicious users can attack a network by sending configuration BPDUs deliberately to edge ports to cause network jitter. You can prevent this type of attacks by utilizing the BPDU protection function. With this function enabled on a switch, the switch shuts down the edge ports that receive configuration BPDUs and then reports these cases to the administrator. If a port is shut down, only the administrator can restore it.

II. Root protection

A root bridge and its secondary root bridges must reside in the same region. The root bridge of the CIST and its secondary root bridges are usually located in the high-bandwidth core region. Configuration errors or attacks may result in configuration BPDUs with their priorities higher than that of a root bridge, which causes a new root bridge to be elected and network topology jitter to occur. In this case, flows that should travel along high-speed links may be led to low-speed links, and network congestion may occur.

You can avoid this problem by utilizing the root protection function. Ports with this function enabled can only be kept as designated ports in all spanning tree instances. When a port of this type receives configuration BPDUs with higher priorities, it turns to the discarding state (rather than become a non-designated port) and stops forwarding packets (as if it is disconnected from the link). It resumes the normal state if it does not receive any configuration BPDUs with higher priorities for a specified period.

III. Loop prevention

A switch maintains the states of the root port and other blocked ports by receiving and processing BPDUs from the upstream switch. These BPDUs may get lost because of network congestions or unidirectional link failures. If a switch does not receive BPDUs from the upstream switch for certain period, the switch selects a new root port; the original root port becomes a designated port; and the blocked ports turns to the forwarding state. This may cause loops in the network.

The loop prevention function suppresses loops. With this function enabled, if link congestions or unidirectional link failures occur, both the root port and the blocked ports become designated ports and turn to the discarding state. In this case, they stop forwarding packets, and thereby loops can be prevented.

IV. TC-BPDU attack prevention

A switch removes MAC address entries and ARP entries upon receiving TC-BPDUs. If a malicious user sends a large amount of TC-BPDUs to a switch in a short period, the switch may be busy in removing MAC address entries and ARP entries, which may decrease the performance of the switch and affect the stability of the network.

With the TC-BPDU prevention function enabled, the switch performs only one removing operation in a specified period (it is 10 seconds by default) after it receives a TC-BPDU. The switch also checks to see whether other TC-BPDUs arrive in this period and performs another removing operation in the next period if a TC-BPDU is received. Such a mechanism prevents a switch from busying itself in performing removing operations.

Caution:

Among loop prevention function, root protection function, and edge port setting, only one can be valid on a port at one time.

V. BPDU packet drop

In a STP-enabled network, some users may send BPDU packets to the switch continuously in order to destroy the network. When a switch receives the BPDU packets, it will forward them to other switches. As a result, STP calculation is performed continuously, which may occupy too much CPU of the switches or cause errors in the protocol state of the BPDU packets.

In order to avoid this problem, you can enable the function of dropping BPDU packets on the Ethernet ports. Once the function is enabled on a port, the port will not receive

and forward any BPDU packets. In this way, the switch is protected again the BPDU packet attack so that the STP calculation is assured to be right.

1.5.2 Configuration Prerequisites

MSTP runs normally on the switch.

1.5.3 Configuring BPDU Protection

I. Configuration procedure

Table 1-30 Configure BPDU protection

Operation	Command	Description
Enter system view	**system-view**	—
Enable the BPDU protection function	**stp bpdu-protection**	Required The BPDU protection function is disabled by default.

II. Configuration example

Enable the BPDU protection function.

```
<H3C> system-view
[H3C] stp bpdu-protection
```

Caution:

As Gigabit ports of an S3600 Ethernet switch cannot be shut down, the BPDU protection function is not applicable to these ports even if you enable the BPDU protection function and specify these ports to be MSTP edge ports.

1.5.4 Configuring Root Protection

I. Configuration procedure

Table 1-31 Configure the root protection function in system view

Operation	Command	Description
Enter system view	**system-view**	—

Operation	Command	Description
Enable the root protection function on specified ports	**stp interface** *interface-list* **root-protection**	Required The root protection function is disabled by default.

Table 1-32 Enable the root protection function in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**Interface** *interface-type interface-number*	—
Enable the root protection function on the current port	**stp root-protection**	Required The root protection function is disabled by default.

II. Configuration example

Enable the root protection function on Ethernet1/0/1.

1) Perform this configuration in system view.

```
<H3C> system-view
[H3C] stp interface Ethernet1/0/1 root-protection
```

2) Perform this configuration in Ethernet port view.

```
<H3C> system-view
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] stp root-protection
```

1.5.5 Configuring Loop Prevention

I. Configuration procedure

Table 1-33 Configure loop prevention

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the loop prevention function on the current port	**stp loop-protection**	Required The loop prevention function is disabled by default.

II. Configuration example

Enable the loop prevention function on Ethernet1/0/1.

```
<H3C> system-view
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] stp loop-protection
```

1.5.6 Configuring TC-BPDU Attack Prevention

I. Configuration procedure

Table 1-34 Configure the TC-BPDU attack prevention function

Operation	Command	Description
Enter system view	**system-view**	—
Enable the TC-BPDU attack prevention function	**stp tc-protection enable**	Required The TC-BPDU attack prevention function is disabled by default.

II. Configuration example

Enable the TC-BPDU attack prevention function

```
<H3C> system-view
[H3C] stp tc-protection enable
```

1.5.7 Configuring the Function of Dropping BPDU Packets

Table 1-35 Configure the function of dropping BPDU Packets

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-name*	—
Enable the function of dropping BPDU packets in Ethernet port view	**bpdu-drop any**	Required

Enable the function of dropping BPDU packets on Ethernet1/0/1.

```
<H3C>system-view
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] bpdu-drop any
```

1.6 Configuring Digest Snooping

1.6.1 Introduction

According to IEEE 802.1s, two interconnected switches can interwork with each other through MSTIs in an MST region only when the two switches have the same MST region-related configuration. Interconnected MSTP-enabled switches determine whether or not they are in the same MST region by checking the configuration IDs of the BPDUs between them. (A configuration ID contains information such as region ID and configuration digest.)

As some other manufacturers' switches adopt proprietary spanning tree protocols, they cannot interwork with the other switches in an MST region even if they are configured with the same MST region-related settings as the other switches in the MST region.

This problem can be overcome by implementing the digest snooping feature. If a port on an S3600 Ethernet switch is connected to another manufacturer's switch that has the same MST region-related configuration as its own but adopts a proprietary spanning tree protocol, you can enable digest snooping on the port. Then the S3600 Ethernet switch regards another manufacturer's switch as in the same region; it records the configuration digests carried in the BPDUs received from another manufacturer's switch, and put them in the BPDUs to be sent to the another manufacturer's switch. In this way, the S3600 Ethernet switch can interwork with another manufacturer’s switches in the same MST region.

⚠ **Caution:**

The digest snooping function is not applicable to edge ports.

1.6.2 Configuring Digest Snooping

Configure the digest snooping feature on a switch to enable it to interwork with other switches adopting proprietary protocols to calculate configuration digests in the same MST region through MSTIs.

I. Configuration prerequisites

The switch to be configured is connected to another manufacturer's switch adopting a proprietary spanning tree protocol. The MSTP and the network operate normally.

II. Configuration procedure

Table 1-36 Configure digest snooping

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the digest snooping feature	**stp config-digest-snooping**	Required The digest snooping feature is disabled on the port by default.
Return to system view	**quit**	—
Enable the digest snooping feature globally	**stp config-digest-snooping**	Required The digest snooping feature is disabled globally by default.
Display the configuration	**display current-configuration**	You can execute this command in any view.

Note:

- When the digest snooping feature is enabled on a port, the port state turns to the discarding state. That is, the port will not send BPDU packets. The port is not involved in the STP calculation until it receives BPDU packets from the peer port.
- The digest snooping feature is needed only when your switch is connected to another manufacturer's switches adopting proprietary spanning tree protocols.
- To enable the digest snooping feature successfully, you must first enable it on all the ports of your switch that are connected to another manufacturer's switches adopting proprietary spanning tree protocols and then enable it globally.
- To enable the digest snooping feature, the interconnected switches and another manufacturer's switch adopting proprietary spanning tree protocols must be configured with exactly the same MST region-related configurations (including region name, revision level, and VLAN-to-MSTI mapping).
- The digest snooping feature must be enabled on all the ports of your S3600 Ethernet switches connected to another manufacturer's switches adopting proprietary spanning tree protocols in the same MST region.
- When the digest snooping feature is enabled globally, the VLAN-to-MSTI mapping table cannot be modified.
- The digest snooping feature is not applicable to edge ports in an MST region.

1.7 Configuring Rapid Transition

1.7.1 Introduction

Designated ports of RSTP-enabled or MSTP-enabled switches use the following two types of packets to implement rapid transition:

- Proposal packets: Packets sent by designated ports to request rapid transition
- Agreement packets: Packets used to acknowledge rapid transition requests

Both RSTP and MSTP specify that the upstream switch can perform rapid transition operation on the designated port only when the port receives an agreement packet from the downstream switch. The difference between RSTP and MSTP are:

- For MSTP, the upstream switch sends agreement packets to the downstream switch; and the downstream switch sends agreement packets to the upstream switch only after it receives agreement packets from the upstream switch.
- For RSTP, the upstream switch does not send agreement packets to the downstream switch.

Figure 1-3 and Figure 1-4 illustrate the rapid transition mechanisms on designated ports in RSTP and MSTP.

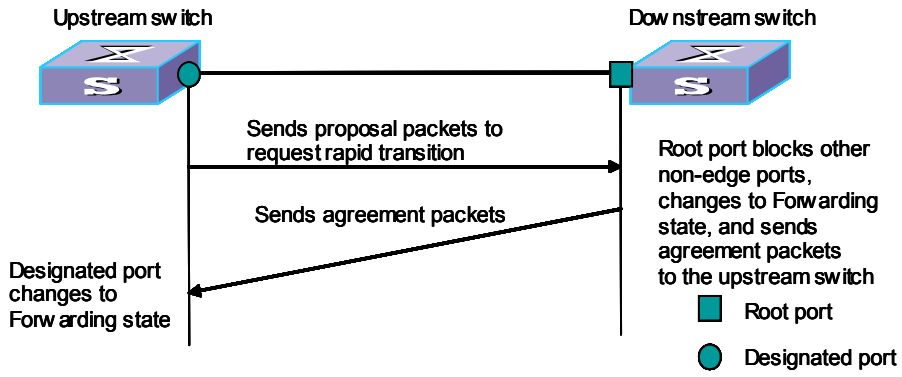


Figure 1-3 The RSTP rapid transition mechanism

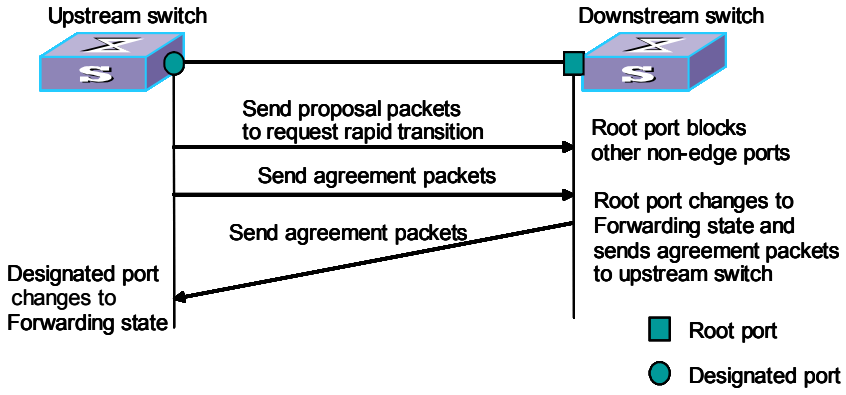


Figure 1-4 The MSTP rapid transition mechanism

The cooperation between MSTP and RSTP is limited in the process of rapid transition. For example, when the upstream switch adopts RSTP, the downstream switch adopts MSTP and the downstream switch does not support RSTP-compatible mode, the root port on the downstream switch receives no agreement packet from the upstream switch and thus sends no agreement packets to the upstream switch. As a result, the designated port of the upstream switch fails to transit rapidly and can only turn to the forwarding state after a period twice the forward delay.

Some other manufacturers' switches adopt proprietary spanning tree protocols that are similar to RSTP in the way to implement rapid transition on designated ports. When a switch of this kind operating as the upstream switch connects with a H3C series switch running MSTP, the upstream designated port fails to change its state rapidly.

The rapid transition feature is developed to resolve this problem. When a H3C series switch running MSTP is connected in the upstream direction to another manufacturer's switch running proprietary spanning tree protocols, you can enable the rapid transition feature on the ports of the H3C series switch operating as the downstream switch. Among these ports, those operating as the root ports will then send agreement packets to their upstream ports after they receive proposal packets from the upstream designated ports, instead of waiting for agreement packets from the upstream switch. This enables designated ports of the upstream switch to change their states rapidly.

1.7.2 Configuring Rapid Transition

I. Configuration prerequisites

As shown in Figure 1-5, a H3C series switch is connected to another manufacturer's switch. The former operates as the downstream switch, and the latter operates as the upstream switch. The network operates normally.

The upstream switch is running a proprietary spanning tree protocol that is similar to RSTP in the way to implement rapid transition on designated ports. Port 1 is the designated port.

The downstream switch is running MSTP. Port 2 is the root port.

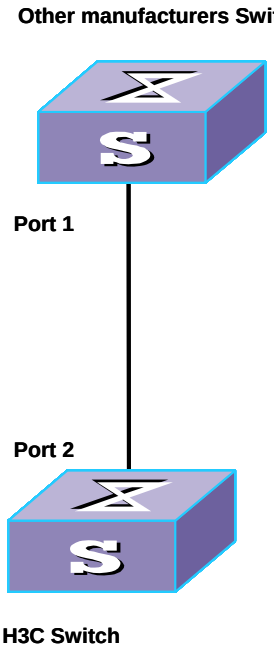


Figure 1-5 Network diagram for rapid transition configuration

II. Configuration procedure

1) Configure the rapid transition feature in system view

Table 1-37 Configure the rapid transition feature in system view

Operation	Command	Description
Enter system view	**system-view**	—
Enable the rapid transition feature	**stp interface** *interface-type interface-number* **no-agreement-check**	Required By default, the rapid transition feature is disabled on a port.

2) Configure the rapid transition feature in Ethernet port view

Table 1-38 Configure the rapid transition feature in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the rapid transition feature	**stp no-agreement-check**	Required By default, the rapid transition feature is disabled on a port.

Note:

- The rapid transition feature can be enabled on only root ports or alternate ports.
- If you configure the rapid transition feature on a designated port, the feature does not take effect on the port.

1.8 Configuring VLAN-VPN Tunnel

1.8.1 Introduction

The VLAN-VPN Tunnel function enables STP packets to be transparently transmitted between geographically dispersed user networks through specified VLAN VPNs in operator's networks, through which spanning trees can be generated across these user networks and are independent of those of the operator's network.

As shown in Figure 1-6, the upper part is the operator's network, and the lower part is the user's network. The operator's network comprises packet ingress/egress devices, and the user's network has networks A and B. On the operator's network, configure the arriving STP packets at the ingress to have MAC addresses in a special format, and reconvert them back to their original formats at the egress. This is how transparent transmission is implemented over the operator's network.

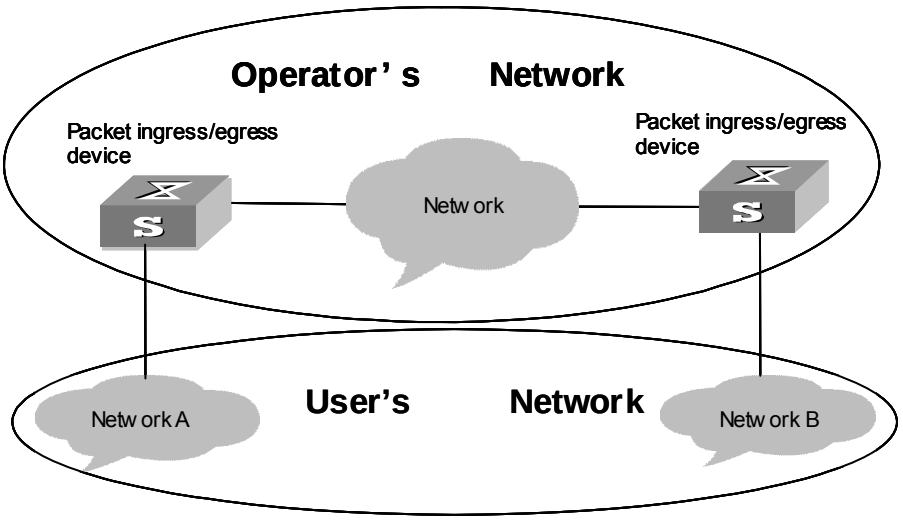


Figure 1-6 VLAN-VPN tunnel network hierarchy

1.8.2 Configuring VLAN-VPN tunnel

Table 1-39 Configure VLAN-VPN tunnel

Operation	Command	Description
Enter system view	**system-view**	—
Enable MSTP globally	**stp enable**	—
Enable the VLAN-VPN tunnel function globally	**vlan-vpn tunnel**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	Make sure that you enter the Ethernet port view of the port for which you want to enable the VLAN-VPN tunnel function.
Disable MSTP for the port	**stp disable**	—
Enable the VLAN VPN function for the Ethernet port	**vlan-vpn enable**	Required By default, the VLAN VPN function is disabled on all ports.

Note:

- The VLAN-VPN tunnel function can be enabled on only STP-enabled devices.
- To enable the VLAN-VPN tunnel function, make sure the links between operator's networks are trunk links.
- If a fabric port exists on a switch, you cannot enable the VLAN VPN function on any port of the switch.

1.9 Displaying and Maintaining MSTP

You can verify the above configurations by executing the **display** commands in any view.

Execute the **reset** command in user view to clear statistics about MSTP.

Table 1-40 Display and maintain MSTP

Operation	Command
Display the state and statistics information about spanning trees of the current device	**display stp** [**instance** *instance-id*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]
Display region configuration	**display stp region-configuration**
Clear statistics about MSTP	**reset stp** [**interface** *interface-list*]

1.10 MSTP Configuration Example

I. Network requirements

Implement MSTP in the network shown in Figure 1-7 to enable packets of different VLANs to be forwarded along different spanning tree instances. The detailed configurations are as follows:

- All switches in the network belong to the same MST region.
- Packets of VLAN 10, VLAN 30, VLAN 40, and VLAN 20 are forwarded along spanning tree instance 1, instance 3, instance 4, and instance 0 respectively.

In this network, Switch A and Switch B operate on the convergence layer; Switch C and Switch D operate on the access layer. VLAN 10 and VLAN 30 are limited in the convergence layer and VLAN 40 is limited in the access layer. Switch A and Switch B are configured as the root bridges of spanning tree instance 1 and spanning tree instance 3 respectively. Switch C is configured as the root bridge of spanning tree instance 4.

II. Network diagram

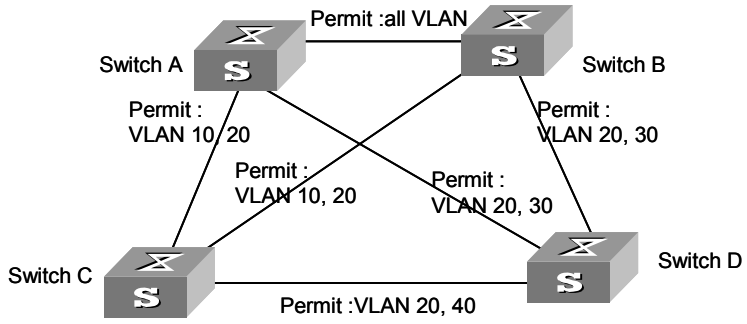


Figure 1-7 Network diagram for MSTP configuration

Note:

The word “permit” shown in Figure 1-7 means the corresponding link permits packets of specific VLANs.

III. Configuration procedure

1) Configure Switch A

Enter MST region view.

```
<H3C> system-view
[H3C] stp region-configuration
```

Configure the MST region.

```
[H3C-mst-region] region-name example
[H3C-mst-region] instance 1 vlan 10
[H3C-mst-region] instance 3 vlan 30
[H3C-mst-region] instance 4 vlan 40
[H3C-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[H3C-mst-region] active region-configuration
```

Specify Switch A as the root bridge of spanning tree instance 1.

```
[H3C] stp instance 1 root primary
```

2) Configure Switch B

Enter MST region view.

```
<H3C> system-view
[H3C] stp region-configuration
```

Configure the MST region.

```
[H3C-mst-region] region-name example
[H3C-mst-region] instance 1 vlan 10
[H3C-mst-region] instance 3 vlan 30
[H3C-mst-region] instance 4 vlan 40
[H3C-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[H3C-mst-region] active region-configuration
```

Specify Switch B as the root bridge of spanning tree instance 3.

```
[H3C] stp instance 3 root primary
```

3) Configure Switch C.

Enter MST region view.

```
<H3C> system-view
[H3C] stp region-configuration
```

Configure the MST region.

```
[H3C-mst-region] region-name example
[H3C-mst-region] instance 1 vlan 10
[H3C-mst-region] instance 3 vlan 30
[H3C-mst-region] instance 4 vlan 40
[H3C-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[H3C-mst-region] active region-configuration
```

Specify Switch C as the root bridge of spanning tree instance 4.

```
[H3C] stp instance 4 root primary
```

4) Configure Switch D

Enter MST region view.

```
<H3C> system-view
[H3C] stp region-configuration
```

Configure the MST region.

```
[H3C-mst-region] region-name example
[H3C-mst-region] instance 1 vlan 10
[H3C-mst-region] instance 3 vlan 30
[H3C-mst-region] instance 4 vlan 40
[H3C-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[H3C-mst-region] active region-configuration
```

1.11 VLAN-VPN tunnel Configuration Example

I. Network requirements

- S3600 series Ethernet switches operate as the access devices of the operator's network, that is, Switch C and Switch D in the network diagram.
- S3100 series switches operate as the access devices of the user's network, that is, Switch A and Switch B in the network diagram.
- Switch C and Switch D are connected to each other through the configured trunk ports of the switches. The VLAN-VPN tunnel function is enabled in system view, thus implementing transparent transmission between the user's network and the operator's network.

II. Network diagram

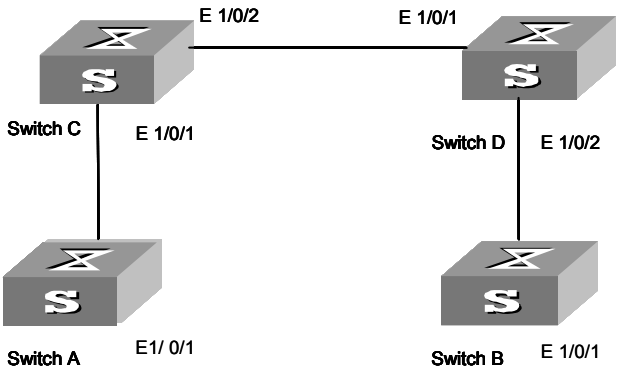


Figure 1-8 Network diagram for VLAN-VPN tunnel configuration

III. Configuration procedure

1) Configure Switch A

Enable MSTP.

```
<H3C> system-view
[H3C] stp enable
```

Add Ethernet 1/0/1 to VLAN 10.

```
[H3C] vlan 10
[H3C-Vlan10] port Ethernet 1/0/1
```

2) Configure Switch B

Enable MSTP.

```
<H3C> system-view
[H3C] stp enable
```

Add Ethernet 1/0/1 to VLAN 10.

```
[H3C] vlan 10
[H3C-Vlan10] port Ethernet 1/0/1
```

3) Configure Switch C

Enable MSTP.

```
<H3C> system-view
[H3C] stp enable
```

Enable the VLAN-VPN tunnel function.

```
[H3C] vlan-vpn tunnel
```

Add Ethernet1/0/1 to VLAN 10.

```
[H3C] vlan 10
[H3C-Vlan10] port Ethernet 1/0/1
[H3C-Vlan10] quit
```

Disable the STP feature on Ethernet1/0/1 and then enable the VLAN VPN function on it.

```
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] port access vlan 10
[H3C-Ethernet1/0/1] stp disable
[H3C-Ethernet1/0/1] vlan-vpn enable
[H3C-Ethernet1/0/1] quit
```

Configure Ethernet1/0/2 as a trunk port.

```
[H3C] interface Ethernet 1/0/2
[H3C-Ethernet1/0/2] port link-type trunk
```

Add the trunk port to all VLANs.

```
[H3C-Ethernet1/0/2] port trunk permit vlan all
```

4) Configure Switch D

Enable MSTP.

```
<H3C> system-view
[H3C] stp enable
```

Enable the VLAN-VPN tunnel function.

```
[H3C] vlan-vpn tunnel
```

Add Ethernet1/0/2 to VLAN 10.

```
[H3C] vlan 10
[H3C-Vlan10] port Ethernet 1/0/2
```

Disable STP on Ethernet1/0/2 and then enable the VLAN VPN function on it.

```
[H3C] interface Ethernet 1/0/2
[H3C-Ethernet1/0/2] port access vlan 10
[H3C-Ethernet1/0/2] stp disable
[H3C-Ethernet1/0/2] vlan-vpn enable
[H3C-Ethernet1/0/2] quit
```

Configure Ethernet1/0/1 as a trunk port.

```
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] port link-type trunk
```

Add the trunk port to all VLANs.

```
[H3C-Ethernet1/0/1] port trunk permit vlan all
```

Table of Contents

Chapter 1 IP Routing Protocol Overview 1-1
1.1 Introduction to IP Route and Routing Table 1-1
1.1.1 IP Route and Route Segment 1-1
1.1.2 Route Selection through the Routing Table 1-2
1.2 Routing Management Policy 1-4
1.2.1 Routing Protocols and Preferences 1-4
1.2.2 Traffic Sharing and Route Backup 1-5
1.2.3 Routes Shared Between Routing Protocols 1-6
Chapter 2 Static Route Configuration 2-1
2.1 Introduction to Static Route 2-1
2.1.1 Static Route 2-1
2.1.2 Default Route 2-2
2.2 Static Route Configuration 2-2
2.2.1 Configuration Prerequisites 2-2
2.2.2 Configuring a Static Route 2-2
2.3 Displaying the Routing Table 2-3
2.4 Static Route Configuration Example 2-4
2.5 Troubleshooting a Static Route 2-5
Chapter 3 RIP Configuration 3-1
3.1 RIP Overview 3-1
3.1.1 Basic Concepts 3-1
3.1.2 RIP Startup and Operation 3-2
3.2 RIP Configuration Tasks 3-3
3.3 Basic RIP Configuration 3-4
3.3.1 Configuration Prerequisites 3-4
3.3.2 Configuring Basic RIP Functions 3-4
3.4 RIP Route Control 3-6
3.4.1 Configuration Prerequisites 3-6
3.4.2 Configuring RIP Route Control 3-6
3.5 RIP Network Adjustment and Optimization 3-10
3.5.1 Configuration Prerequisites 3-10
3.5.2 Configuration Tasks 3-10
3.6 Displaying and Maintaining RIP Configuration 3-13
3.7 RIP Configuration Example 3-13
3.8 Troubleshooting RIP Configuration 3-14
Chapter 4 OSPF Configuration 4-1
4.1 OSPF Overview 4-1

4.1.1 Introduction to OSPF 4-1
4.1.2 OSPF Route Calculation 4-2
4.1.3 Basic OSPF Concepts 4-2
4.1.4 OSPF Network Type 4-4
4.1.5 OSPF Packets 4-6
4.1.6 LSA Types 4-7
4.1.7 OSPF Features 4-8
4.2 OSPF Configuration Tasks 4-9
4.3 Basic OSPF Configuration 4-10
4.3.1 Configuration Prerequisites 4-10
4.3.2 Basic OSPF Configuration 4-10
4.4 OSPF Area Attribute Configuration 4-12
4.4.1 Configuration Prerequisites 4-12
4.4.2 Configuring OSPF Area Attributes 4-13
4.5 OSPF Network Type Configuration 4-13
4.5.1 Configuration Prerequisites 4-14
4.5.2 Configuring the Network Type of an OSPF Interface 4-14
4.5.3 Configuring an NBMA Neighbor 4-15
4.5.4 Configuring the DR Priority on an OSPF Interface 4-15
4.6 OSPF Route Control 4-16
4.6.1 Configuration Prerequisites 4-16
4.6.2 Configuring OSPF Route Summary 4-16
4.6.3 Configuring OSPF to Filter Received Routes 4-17
4.6.4 Configuring the Cost for Sending Packets on an OSPF Interface 4-18
4.6.5 Configuring OSPF Route Priority 4-18
4.6.6 Configuring the Maximum Number of OSPF Equal-Cost Routes 4-18
4.6.7 Configuring OSPF to Import External Routes 4-19
4.7 OSPF Network Adjustment and Optimization 4-20
4.7.1 Configuration Prerequisites 4-20
4.7.2 Configuring OSPF Timers 4-21
4.7.3 Configuring the LSA transmission delay 4-22
4.7.4 Configuring the SPF Calculation Interval 4-22
4.7.5 Disabling OSPF Packet Transmission on an Interface 4-23
4.7.6 Configuring OSPF Authentication 4-24
4.7.7 Configuring to Fill the MTU Field When an Interface Transmits DD Packets 4-24
4.7.8 Enabling OSPF Logging 4-25
4.7.9 Configuring OSPF Network Management System (NMS) 4-25
4.8 Displaying and Maintaining OSPF Configuration 4-26
4.9 OSPF Configuration Example 4-28
4.9.1 Configuring DR Election Based on OSPF Priority 4-28
4.9.2 Configuring OSPF Virtual Link 4-30
4.10 Troubleshooting OSPF Configuration 4-31

Chapter 5 IP Routing Policy Configuration 5-1
5.1 IP Routing Policy Overview 5-1
5.2 IP Routing Policy Configuration Tasks 5-2
5.3 Route-Policy Configuration 5-3
5.3.1 Configuration Prerequisites 5-3
5.3.2 Defining a Route-Policy 5-3
5.3.3 Defining if-match Clauses and apply Clauses 5-4
5.4 ip-prefix Configuration 5-5
5.4.1 Configuration Prerequisites 5-6
5.4.2 Configuring an ip-prefix list 5-6
5.5 Displaying IP Routing Policy 5-7
5.6 IP Routing Policy Configuration Example 5-7
5.6.1 Configuring to Filter Received Routing Information 5-7
5.7 Troubleshooting IP Routing Policy 5-9

Chapter 6 Route Capacity Configuration 6-1
6.1 Route Capacity Configuration Overview 6-1
6.1.1 Introduction 6-1
6.1.2 Route Capacity Limitation on the S3600 Series 6-1
6.2 Route Capacity Configuration 6-2
6.2.1 Configuring the Lower Limit and the Safety Value of the Switch Memory 6-2
6.2.2 Enabling/Disabling Automatic Protocol Recovery 6-2
6.3 Displaying Route Capacity Configuration 6-3

Chapter 1 IP Routing Protocol Overview

Note:

When running a routing protocol, the Ethernet switch also functions as a router. The word “router” and the router icons covered in the following text represent routers in common sense and Ethernet switches running a routing protocol.

This manual deals with the S3600-EI series switches. The **ospf**, **ospf-ase**, and **ospf-nssa** commands are supported by the S3600-EI series, but not supported by the S3600-SI series. This will not be mentioned again in this manual.

1.1 Introduction to IP Route and Routing Table

1.1.1 IP Route and Route Segment

Routers are used for route selection on the Internet. As a router receives a packet, it selects an appropriate route (through a network) according to the destination address of the packet and forwards the packet to the next router. The last router on the route is responsible for delivering the packet to the destination host.

A route segment is a common physical network interconnecting two nodes, which are deemed adjacent on the Internet. That is, two routers connected to the same physical network are adjacent to each other. The number of route segments between a router and any host on the local network is zero. In the following figure, the bold arrows represent route segments. A router is not concerned about which physical links compose a route segment. As shown in Figure 1-1, a packet sent from Host A to Host C travels through two routers over three route segments (along the broken line).

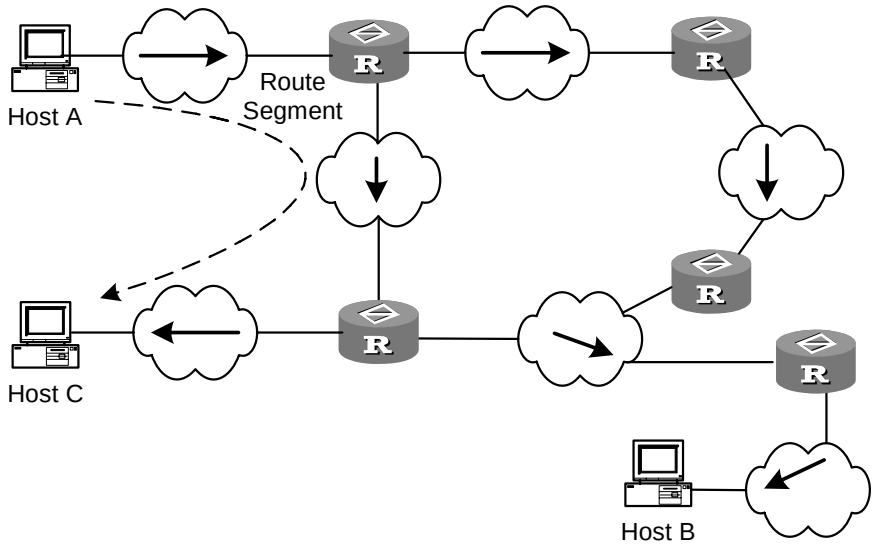


Figure 1-1 Route segment

The number of route segments on the path between a source and destination can be used to measure the "length" of the path. As the sizes of networks may differ greatly, the actual length of router segments may be different from each other. Therefore, you can put different weights to different route segments (so that, for example, a route segment can be considered as two segments if the weight is two). In this way, the length of the path can be measure by the number of weighted route segments.

If routers in networks are regarded as nodes in networks and route segments in the Internet are regarded as links in the Internet, routing in the Internet is similar to that in a conventional network.

Routing through the shortest route is not always the most ideal way. For example, routing across three high-speed LAN route segments may be much faster than routing across two low-speed WAN route segments.

1.1.2 Route Selection through the Routing Table

The key for a router to forward packets is the routing table. Each router maintains a routing table. Each entry in this table contains an IP address that represents a host/subnet and specifies which physical port on the router should be used to forward the packets destined for the host/subnet. And the router forwards those packets through this port to the next router or directly to the destination host if the host is on a network directly connected to the router.

Each entry in a routing table contains:

- Destination address: It identifies the address of the destination host or network of an IP packet.
- Network mask: Along with the destination address, it identifies the address of the network segment where the destination host or router resides. By performing

"logical AND" between destination address and network mask, you can get the address of the network segment where the destination host or router resides. For example, if the destination address is 129.102.8.10 and the mask is 255.255.0.0, the address of the network segment where the destination host or router resides is 129.102.0.0. A mask consists of some consecutive 1s, represented either in dotted decimal notation or by the number of the consecutive 1s in the mask.

- Output interface: It indicates through which interface IP packets should be forwarded to reach the destination.
- Next hop address: It indicates the next router that IP packets will pass through to reach the destination.
- Preference of the route added to the IP routing table: There may be multiple routes with different next hops to the same destination. These routes may be discovered by different routing protocols, or be manually configured static routes. The one with the highest preference (the smallest numerical value) will be selected as the current optimal route.

According to different destinations, routes fall into the following categories:

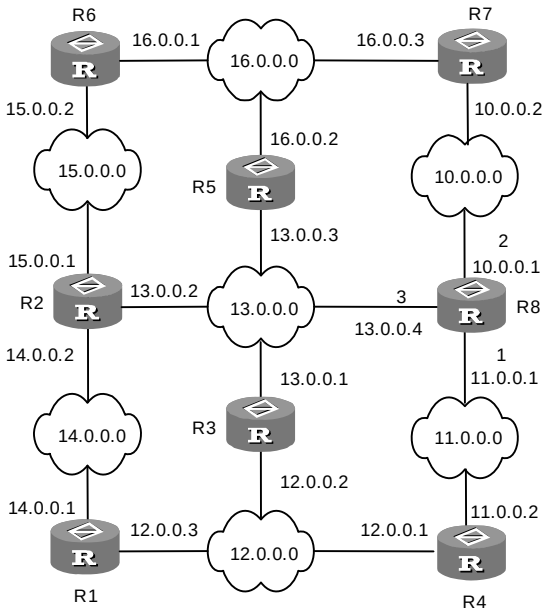
- Subnet route: The destination is a subnet.
- Host route: The destination is a host.

In addition, according to whether the network where the destination resides is directly connected to the router, routes fall into the following categories:

- 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 avoid an oversized routing table, you can set a default route. All the packets for which the router fails to find a matching entry in the routing table will be forwarded through this default route.

Figure 1-2 shows a relatively complicated internet environment, the number in each network cloud indicate the network address and "R" represents a router. The router R8 is connected to three networks, and so it has three IP addresses and three physical ports. Its routing table is shown in Figure 1-2.



Routing table of router R8

Destination network	Next hop	Interface
10.0.0.0	10.0.0.1	2
11.0.0.0	11.0.0.1	1
12.0.0.0	11.0.0.2	1
13.0.0.0	13.0.0.4	3
14.0.0.0	13.0.0.2	3
15.0.0.0	13.0.0.2	3
16.0.0.0	10.0.0.2	2

Figure 1-2 Routing table

The H3C S3600 Series Ethernet Switches (hereinafter referred to as S3600 series) support the configuration of static routes as well as a series of dynamic routing protocols such as RIP and OSPF. Moreover, the switches in operation can automatically obtain some direct routes according to interface status and user configuration.

1.2 Routing Management Policy

On an S3600 Ethernet switch, you can manually configure a static route to a certain destination, or configure a dynamic routing protocol to make the switch interact with other routers in the internetwork and find routes by routing algorithm. On an S3600 Ethernet switch, the static routes configured by the user and the dynamic routes discovered by routing protocols are managed uniformly. The static routes and the routes learned or configured by different routing protocols can also be shared among routing protocols.

1.2.1 Routing Protocols and Preferences

Different routing protocols may discover different routes to the same destination, but only one route among these routes and the static routes is optimal. In fact, at any given moment, only one routing protocol can determine the current route to a specific destination. Routing protocols (including static routing) are endowed with different preferences. 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 their default route preferences (the smaller the value is, the higher the preference is) are shown in Table 1-1.

In the table, “0” is used for directly connected routes, and “255” is used for routes from untrusted sources.

Table 1-1 Routing protocols and corresponding route preferences

Routing protocol or route type	Preference of the corresponding route
DIRECT	0
OSPF	10
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
UNKNOWN	255

Except for direct routing, you can manually configure the preferences of various dynamic routing protocols as required. In addition, you can configure different preferences for different static routes.

1.2.2 Traffic Sharing and Route Backup

I. Traffic sharing

The S3600 series support multi-route mode, allowing the configuration of multiple routes that reach the same destination and have the same preference. The same destination can be reached through multiple different routes, whose preferences are equal. When there is no route with a higher preference to the same destination, the multiple routes will be adopted. Then, the packets destined for the same destination will be forwarded through these routes in turn to implement traffic sharing.

II. Route backup

The S3600 series support route backup. When the primary route fails, the system automatically switches to a backup route to improve network reliability.

To achieve route backup, you can configure multiple routes to the same destination according to actual situation. One of the routes has the highest preference and is called primary route. The other routes have descending preferences and are called backup routes. Normally, the router sends data through the primary route. When line failure occurs on the primary route, the primary route will hide itself and the router will choose the one whose preference is the highest among the remaining backup routes as the path to send data. In this way, the switchover from the primary route to a

backup route is implemented. When the primary route recovers, the router will restore it and re-select a route. And, as the primary route has the highest preference, the router will choose the primary route to send data. This process is the automatic switchover from the backup route to the primary route.

1.2.3 Routes Shared Between Routing Protocols

As the algorithms of various routing protocols are different, different routing protocols may discover different routes. This brings about the problem of how to share the discovered routes between routing protocols. The S3600 series can import (with the **import-route** command) the routes discovered by one routing protocol to another routing protocol. Each protocol has its own route redistribution mechanism. For details, see section 3.4.2 VII. "Configuring RIP to import routes" and section 4.6.7 "Configuring OSPF to Import External Routes".

Chapter 2 Static Route Configuration

Note:

When running a routing protocol, the Ethernet switch also functions as a router. The word “router” and the router icons covered in the following text represent routers in common sense and Ethernet switches running a routing protocol.

2.1 Introduction to Static Route

2.1.1 Static Route

Static routes are special routes. They are manually configured by the administrator. By configuring static routes, you can build an interconnecting network. The problem for such configuration is when a fault occurs on the network, a static route cannot change automatically to steer away from the fault point without the help of the administrator.

In a relatively simple network, you only need to configure static routes to make routers work normally. Proper configuration and usage of static routes can improve network performance and ensure sufficient bandwidth for important applications.

Static routes are divided into three types:

- Reachable route: normal route. If a static route to a destination is of this type, the IP packets destined for this destination will be forwarded to the next hop. It is the most common type of static routes.
- Unreachable route: route with the "**reject**" attribute. If a static route to a destination has the "**reject**" attribute, all the IP packets destined for this destination will be discarded, and the source hosts will be informed of the unreachability of the destination.
- Blackhole route: route with “**blackhole**” attribute. If a static route destined for a destination has the “**blackhole**” attribute, the outgoing interface of this route is the Null 0 interface regardless of the next hop address, and all the IP packets addressed to this destination will be dropped without notifying the source hosts.

The attributes "**reject**" and "**blackhole**" are usually used to limit the range of the destinations this router can reach, and help troubleshoot the network.

2.1.2 Default Route

A default route is a special route. You can manually configure a default route by using a static route. Some dynamic routing protocols, such as OSPF, can automatically generate a default route.

Simply to say, a default route is a route used only when no matching entry is found in the routing table. That is, the default route is used only when there is no proper route. In a routing table, both the destination address and mask of the default route are 0.0.0.0. You can use the **display ip routing-table** command to view whether the default route has been set. If the destination address of a packet does not match any entry in the routing table, the router will select the default route for the packet; in this case, if there is no default route, the packet will be discarded, and an Internet control message protocol (ICMP) packet will be returned to inform the source host that the destination host or network is unreachable.

2.2 Static Route Configuration

2.2.1 Configuration Prerequisites

Before configuring a static route, perform the following tasks:

- Configuring the physical parameters of the related interface
- Configuring the link layer attributes of the related interface
- Configuring an IP address for the related interface

2.2.2 Configuring a Static Route

Table 2-1 Configure a static route

Operation	Command	Description
Enter system view	**system-view**	—
Add a static route	**ip route-static** *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *next-hop* } [**preference** *value*] [**reject** | **blackhole**] [**description** *text* | **detect-group** *group number*]*	Required By default, the system can obtain the route to the subnet directly connected to the router.
Delete all static routes	**delete static-routes all**	Optional This command deletes all static routes, including the default route.

Note:

- If the destination IP address and the mask of a route are both 0.0.0.0, the route is the default route. Any packet for which the router fails to find a matching entry in the routing table will be forwarded through the default route.
- Do not configure the next hop address of a static route to the address of an interface on the local switch.
- Different preferences can be configured to implement flexible route management policy.

2.3 Displaying the Routing Table

After the above configuration, use the **display** command in any view to display and verify the static route configuration.

Table 2-2 Display the routing table

Operation	Command	Description
Display routing table summary	**display ip routing-table**	You can execute the **display** command in any view.
Display routing table details	**display ip routing-table verbose**	
Display the detailed information of a specific route	**display ip routing-table** *ip-address* [*mask*] [**longer-match**] [**verbose**]	
Display the routes in a specified address range	**display ip routing-table** *ip-address1 mask1 ip-address2 mask2* [**verbose**]	
Display the routes discovered by a specified protocol	**display ip routing-table protocol** *protocol* [**inactive** | **verbose**]	
Display the tree-structured routing table information	**display ip routing-table radix**	
Display the statistics of the routing table	**display ip routing-table statistics**	

2.4 Static Route Configuration Example

I. Network requirements

As shown in Figure 2-1, the masks of all the IP addresses in the figure are 255.255.255.0. It is required that all the hosts/Ethernet switches in the figure can interconnect with each other by configuring static routes.

II. Network diagram

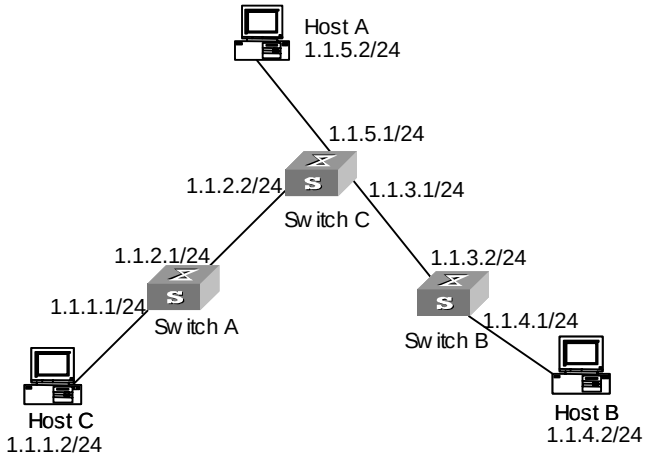


Figure 2-1 Static route configuration

III. Configuration procedure

Perform the following steps on the switch:

Configure static routes on SwitchA.

```
[SwitchA] ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[SwitchA] ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
[SwitchA] ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

Configure static routes on SwitchB.

```
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
[SwitchB] ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
[SwitchB] ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

Configure static routes on SwitchC.

```
[SwitchC] ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
[SwitchC] ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

Perform the following steps on the host:

Configure the default gateway of Host A to 1.1.5.1. Detailed configuration procedure is omitted.

Configure the default gateway of Host B to 1.1.4.1. Detailed configuration procedure is omitted.

Configure the default gateway of Host C to 1.1.1.1. Detailed configuration procedure is omitted.

Now, all the hosts/switches in the figure can interconnect with each other.

2.5 Troubleshooting a Static Route

Symptom: The switch is not configured with a dynamic routing protocol. Both the physical status and the link layer protocol status of an interface are UP, but IP packets cannot be normally forwarded on the interface.

Solution: Perform the following procedure.

Use the **display ip routing-table protocol static** command to view whether the corresponding static route is correctly configured.

Use the **display ip routing-table** command to view whether the static route is valid.

Chapter 3 RIP Configuration

Note:

When running a routing protocol, the Ethernet switch also functions as a router. The word “router” and the router icons covered in the following text represent routers in common sense and Ethernet switches running a routing protocol.

3.1 RIP Overview

Routing information protocol (RIP) is a simple interior gateway protocol (IGP) suitable for small-sized networks.

3.1.1 Basic Concepts

I. RIP

RIP is a distance-vector (D-V) algorithm-based protocol. It exchanges routing information through UDP packets.

RIP uses hop count (also called routing cost) to measure the distance to a destination address. In RIP, the hop count from a router to its directly connected network is 0, and that to a network which can be reached through another router is 1, and so on. To restrict the time to converge, RIP prescribes that the cost is an integer ranging from 0 and 15. The hop count equal to or exceeding 16 is defined as infinite; that is, the destination network or host is unreachable.

To improve performance and avoid routing loop, RIP supports split horizon. Besides, RIP can import routes from other routing protocols.

II. RIP routing database

Each router running RIP manages a routing database, which contains routing entries to all the reachable destinations in the internetwork. Each routing entry contains the following information:

- Destination address: IP address of a host or network.
- Next hop address: IP address of an interface on the adjacent router that IP packets should pass through to reach the destination.
- Interface: Interface on this router, through which IP packets should be forwarded to reach the destination.
- Cost: Cost for the router to reach the destination.

- Routing time: Time elapsed after the routing entry is updated last time. This time is reset to 0 whenever the routing entry is updated.

III. RIP timers

As defined in RFC 1058, RIP is controlled by three timers: Period update, Timeout, and Garbage-collection.

- Period update timer: This timer is used to periodically trigger routing information update so that the router can send all RIP routes to all the neighbors.
- Timeout timer: If a RIP route is not updated (that is, the switch does not receive any routing update packet from the neighbor) within the timeout time of this timer, the route is considered unreachable.
- Garbage-collection timer: An unreachable route will be completely deleted from the routing table if no update packet for the route is received from the neighbor before this timer times out.

3.1.2 RIP Startup and Operation

The whole process of RIP startup and operation is as follows:

- Once RIP is enabled on a router, the router broadcasts or multicasts a request packet to its neighbors. Upon receiving the packet, each neighbor running RIP answers a response packet containing its routing table information.
- When this router receives a response packet, it modifies its local routing table and sends an update triggering packet to the neighbor. Upon receiving the update triggering packet, the neighbor sends the packet to all its neighbors. After a series of update triggering processes, each router can get and keep the updated routing information.
- By default, RIP sends its routing table to its neighbors every 30 seconds. Upon receiving the packets, the neighbors maintain their own routing tables and select optimal routes, and then advertise update information to their respective neighbors so as to make the updated routes known globally. Furthermore, RIP uses the timeout mechanism to handle the timeout routes to ensure real-time and valid routes.

RIP is commonly used by most IP router suppliers. It can be used in most campus networks and the regional networks that are simple and less disperse. For larger and more complicated networks, RIP is not recommended.

3.2 RIP Configuration Tasks

Table 3-1 RIP configuration tasks

Configuration task		Description	Related section
Configuring basic RIP functions	Enabling RIP	Required	Section 3.3.2 I. “Enabling RIP globally and on the interface of a specified network segment”
	Setting the RIP operating status on an interface	Optional	Section 3.3.2 II. “Setting the RIP operating status on an interface”
	Specifying a RIP version	Optional	Section 3.3.2 III. “Specifying the RIP version on an interface”
Configuring RIP route control	Setting the additional routing metrics of an interface	Optional	Section 3.4.2 I. “Setting the additional routing metrics of an interface”
	Configuring RIP route summary	Optional	Section 3.4.2 II. “Configuring RIP route summary”
	Disabling the receiving of host routes	Optional	Section 3.4.2 III. “Disabling the receiving of host routes”
	Configuring RIP to filter incoming/outgoing routes	Optional	Section 3.4.2 IV. “Configuring RIP to filter incoming/outgoing routes”
	Setting RIP preference	Optional	Section 3.4.2 V. “Setting RIP preference”
	Enabling traffic to be forwarded along multiple equivalent RIP routes	Optional	Section3.4.2 VI. Enabling traffic to be forwarded along multiple equivalent RIP routes”
	Configuring RIP to import routes from another protocol	Optional	Section 3.4.2 VII. “Configuring RIP to import routes from another protocol”

Configuration task		Description	Related section
Adjusting and optimizing a RIP network	Configuring RIP timers	Optional	Section 3.5.2 I. “Configuring RIP timers”
	Configuring split horizon	Optional	Section 3.5.2 II. “Configuring split horizon”
	Configuring RIP-1 packet zero field check	Optional	Section 3.5.2 III. “Configuring RIP-1 packet zero field check”
	Setting RIP-2 packet authentication mode	Optional	Section 3.5.2 IV. “Setting RIP-2 packet authentication mode”
	Configuring a RIP neighbor	Optional	Section 3.5.2 V. “Configuring a RIP neighbor”
Displaying and debugging RIP		Optional	Section 3.6 “Displaying and Maintaining RIP Configuration”

3.3 Basic RIP Configuration

3.3.1 Configuration Prerequisites

Before configuring basic RIP functions, perform the following tasks:

- Configuring the link layer protocol
- Configuring the network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer

3.3.2 Configuring Basic RIP Functions

I. Enabling RIP globally and on the interface of a specified network segment

Table 3-2 Enable RIP globally and on the interface of a specified network segment

Operation	Command	Description
Enter system view	**system-view**	—
Enable RIP globally and enter RIP view	**rip**	Required
Enable RIP on the interface of a specified network segment	**network** *network-address*	Required By default, RIP is disabled on any interface.

Note:

- Related RIP commands configured in interface view can take effect only after RIP is enabled.
- RIP operates on the interface of a network segment only when it is enabled on the interface. When RIP is disabled on an interface, it does not operate on the interface, that is, it neither receives/sends routes on the interface nor forwards its interface route. Therefore, after RIP is enabled globally, you must also specify its operating network segments to enable it on the corresponding interfaces.

II. Setting the RIP operating status on an interface

Table 3-3 Setting the RIP operating status on an interface

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Enable the interface to receive RIP update packets	**rip input**	Optional By default, all interfaces are allowed to send and receive RIP packets.
Enable the interface to send RIP update packets	**rip output**	
Run RIP on the interface	**rip work**	

III. Specifying the RIP version on an interface

Table 3-4 Specify the RIP version on an interface

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Specify RIP version on the interface	**rip version** { **1** | **2** [**broadcast** | **multicast**] }	Optional By default, the interface can receive RIP-1 and RIP-2 broadcast packets but send only RIP-1 packets. When specifying the RIP version on an interface as RIP-2, you can also specify the mode (broadcast or multicast) to send RIP packets.

3.4 RIP Route Control

In actual implementation, it may be needed to control RIP routing information more accurately to accommodate complex network environments. By performing the configuration described in the following sections, you can:

- Control route selection by adjusting additional routing metrics on interfaces running RIP.
- Reduce the size of the routing table by setting route summary and disabling the receiving of host routes.
- Filter the received routes.
- Set the preference of RIP to change the preference order of routing protocols. This order makes sense when more than one route to the same destination is discovered by multiple routing protocols.
- Import external routes in an environment with multiple routing protocols and filter the advertised routes.

3.4.1 Configuration Prerequisites

Before configuring RIP route control, perform the following tasks:

- Configuring network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer
- Configuring basic RIP functions

3.4.2 Configuring RIP Route Control

I. Setting the additional routing metrics of an interface

Additional routing metric is the routing metric (hop count) added to the original metrics of RIP routes on an interface. It does not change the metric value of a RIP route in the routing table, but will be added for incoming or outgoing RIP routes on the interface.

Table 3-5 Set additional routing metric

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Set the additional routing metric to be added for incoming RIP routes on this interface	**rip metricin** *value*	Optional By default, the additional routing metric added for incoming routes on an interface is 0.

Operation	Command	Description
Set the additional routing metric to be added for outgoing RIP routes on this interface	**rip metricout** *value*	Optional By default, the additional routing metric added for outgoing routes on an interface is 1.

Note:

The **rip metricout** command takes effect only on the RIP routes learnt by the router and the RIP routes generated by the router itself, but the command is invalid for any route imported to RIP from other routing protocols.

II. Configuring RIP route summary

Route summary means that different subnet routes in the same natural network segment can be aggregated into one route with a natural mask for transmission to another network segment. This function is used to reduce the routing traffic on the network as well as to reduce the size of the routing table.

Route summary does not work for RIP-1. RIP-2 supports route summary. When it is needed to advertise all subnet routes, you can disable the function for RIP-2.

Table 3-6 Configure RIP route summary

Operation	Command	Description
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Enable RIP-2 automatic route summary	**summary**	Optional By default, RIP-2 automatic route summary is enabled.

III. Disabling the receiving of host routes

In some special cases, the router can receive a lot of host routes from the same segment, and these routes are of little help in route addressing but consume a lot of network resources. After host route receiving is disabled, a router can refuse any incoming host route.

Table 3-7 Disable the receiving of host route

Operation	Command	Description
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Disable the receiving of host routes	**undo host-route**	Optional By default, the router receives host routes.

IV. Configuring RIP to filter incoming/outgoing routes

The route filtering function provided by a router enables you to configure inbound/outbound filter policy by specifying an ACL or address prefix list to make RIP filter incoming/outgoing routes. Besides, you can configure RIP to receive only the RIP packets from a specific neighbor.

Table 3-8 Configure RIP to filter incoming/outgoing routes

Operation	Command	Description
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Configure RIP to filter incoming routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] | **route-policy** *route-policy-name* } **import**	Required By default, RIP does not filter any incoming route. The **gateway** keyword is used to filter the incoming routes advertised from a specified address.
	filter-policy gateway *ip-prefix-name* **import**	
Configure RIP to filter outgoing routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-protocol*]	Required By default, RIP does not filter any outgoing route.
	filter-policy route-policy *route-policy-name* **export**	

Note:

- The **filter-policy import** command filters the RIP routes received from neighbors, and the routes being filtered out will neither be added to the routing table nor be advertised to any neighbors.
- The **filter-policy export** command filters all the routes to be advertised, including the routes imported by using the **import-route** command as well as RIP routes learned from neighbors.
- The **filter-policy export** command without the *routing-protocol* argument filters all the routes to be advertised, including the routes imported by the **import-route** command.

V. Setting RIP preference

Table 3-9 Set RIP preference

Operation	Command	Description
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Set the RIP preference	**preference** *value*	Optional The default RIP preference is 100.

VI. Enabling traffic to be forwarded along multiple equivalent RIP routes

Table 3-10 Enable traffic to be forwarded along multiple equivalent RIP routes

Operation	Command	Description
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Enable traffic forwarded along multiple equivalent RIP routes	**traffic-share-across-interface**	Optional By default, **traffic-share-across-interface** is disabled

VII. Configuring RIP to import routes from another protocol

Table 3-11 Configure RIP to import routes from another protocol

Operation	Command	Description
Enter system view	**system-view**	—
Enter RIP view	**rip**	—

Operation	Command	Description
Set the default cost for RIP to import routes from other protocols	**default cost** *value*	Optional When you use the **import-route** command without specifying the cost of imported routes, the default cost you set here will be used.
Configure RIP to import routes from another protocol	**import-route** *protocol* [*process-id*] [**cost** *value* | **route-policy** *route-policy-name*]*	Optional The *process-id* parameter is used only for importing OSPF routes

3.5 RIP Network Adjustment and Optimization

In some special network environments, some RIP features need to be configured and RIP network performance needs to be adjusted and optimized. By performing the configuration mentioned in this section, the following can be implemented:

- Changing the convergence speed of RIP network by adjusting RIP timers,
- Avoiding routing loop by configuring split horizon,
- Packet validation in network environments with high security requirements, and
- Configuring RIP feature on an interface or link with special requirements.

3.5.1 Configuration Prerequisites

Before adjusting RIP, perform the following tasks:

- Configuring the network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer
- Configuring basic RIP functions

3.5.2 Configuration Tasks

I. Configuring RIP timers

Table 3-12 Configure RIP timers

Operation	Command	Description
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Set the values of RIP timers	**timers** { **update** *update-timer* | **timeout** *timeout-timer* } *	Optional By default, Update timer value is 30 seconds and Timeout timer value is 180 seconds.

Note:

When configuring the values of RIP timers, you should take network performance into consideration and perform consistent configuration on all routers running RIP to avoid unnecessary network traffic and network route oscillation.

II. Configuring split horizon

Table 3-13 Configure split horizon

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Enable split horizon	**rip split-horizon**	Optional By default, an interface uses split horizon to send RIP packets.

Note:

Split horizon cannot be disabled on a point-to-point link.

III. Configuring RIP-1 packet zero field check

Table 3-14 Configure RIP-1 packet zero field check

Operation	Command	Description
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Enable zero field check of RIP-1 packets	**checkzero**	Optional By default, zero field check is performed on RIP-1 packets.

Note:

Some fields in a RIP-1 packet must be 0, and they are known as zero fields. For RIP-1, zero field check is performed on incoming packets, those RIP-1 packets with nonzero value in a zero filed will not be processed further. As a RIP-2 packet has no zero fields, this configuration is invalid for RIP-2.

IV. Setting RIP-2 packet authentication mode

RIP-2 supports two authentication modes: simple authentication and MD5 authentication.

Simple authentication cannot provide complete security, because the authentication keys sent along with packets that are not encrypted. Therefore, simple authentication cannot be applied where high security is required.

Table 3-15 Set RIP-2 packet authentication mode

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Set RIP-2 packet authentication mode	**rip authentication-mode** { **simple** *password* | **md5** { **rfc2453** *key-string* | **rfc2082** *key-string key-id* } }	Required If you specify to use MD5 authentication, you must specify one of the following MD5 authentication types: rfc2453 (this type supports the packet format defined in RFC 2453) rfc2082 (this type supports the packet format defined in RFC 2082)

V. Configuring a RIP neighbor

Table 3-16 Configure a RIP neighbor

Operation	Command	Description
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Configure a RIP neighbor	**peer** *ip-address*	Required To make RIP to work on a link that does not support broadcast/multicast packets, you must manually configure the RIP neighbor. Normally, RIP uses broadcast or multicast addresses to send packets.

3.6 Displaying and Maintaining RIP Configuration

After the above configuration, you can use the **display** command in any view to display the running status of RIP and verify the RIP configuration. You can use the **reset** command in RIP view to reset the system configuration related to RIP.

Table 3-17 Display and debug RIP configuration

Operation	Command	Description
Display the current RIP running status and configuration information	**display rip**	You can execute the **display** command in any view.
Display RIP interface information	**display rip interface**	
Display RIP routing information	**display rip routing**	
Reset the system configuration related to RIP	**reset**	You can use this command in RIP view.

3.7 RIP Configuration Example

I. Network requirements

As shown in Figure 3-1, SwitchC is connected to subnet 117.102.0.0 through an Ethernet port. SwitchA and SwitchB are connected to networks 155.10.1.0 and 196.38.165.0 respectively through Ethernet ports. SwitchC, SwitchA and SwitchB are interconnected through Ethernet 110.11.2.0. It is required to configure RIP correctly to ensure the interworking between the networks connected to SwitchC, SwitchA and SwitchB.

II. Network diagram

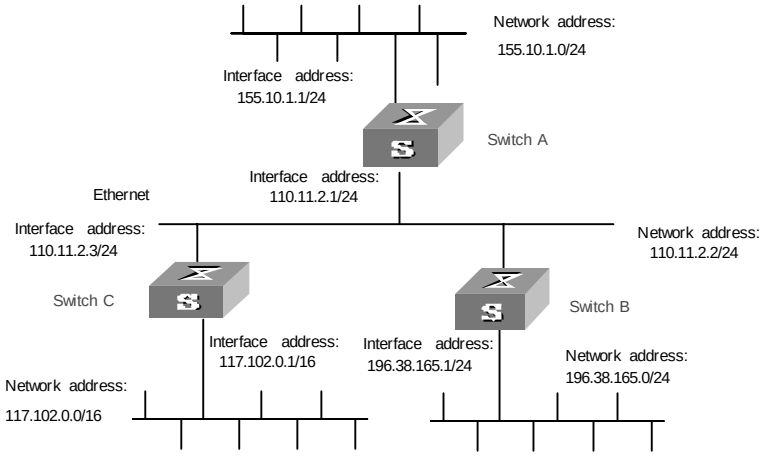


Figure 3-1 RIP configuration

III. Configuration procedure

Note:

Only the configuration related to RIP is listed below. Before the following configuration, make sure the Ethernet link layer works normally and the IP addresses of VLAN interfaces are configured correctly.

---

1) Configure SwitchA:

Configure RIP.

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip] network 110.11.2.0
[SwitchA-rip] network 155.10.1.0
```

2) Configure SwitchB:

Configure RIP.

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip] network 196.38.165.0
[SwitchB-rip] network 110.11.2.0
```

3) Configure SwitchC:

Configure RIP.

```
<SwitchC> system-view
[SwitchC-rip] network 117.102.0.0
[SwitchC-rip] network 110.11.2.0
```

3.8 Troubleshooting RIP Configuration

Symptom: The Ethernet switch cannot receive any RIP update packet when the physical connection between the switch and the peer routing device is normal.

Solution: RIP is not enabled on the corresponding interface (for example, the **undo rip work** command is executed on the interface) or RIP is not enabled by the **network** command on the interface. The peer routing device is configured to work in the multicast mode (for example, the **rip version 2 multicast** command is executed) but the multicast mode is not configured on the corresponding interface of this switch.

Chapter 4 OSPF Configuration

Note:

When running a routing protocol, the Ethernet switch also functions as a router. The words “router” and the router icons covered in the following text represent routers in common sense and Ethernet switches running a routing protocol.
Among S3600 series, only S3600-EI series support OSPF protocol.

4.1 OSPF Overview

4.1.1 Introduction to OSPF

Open shortest path first (OSPF) is a link state-based interior gateway protocol developed by IETF. At present, OSPF version 2 (RFC 2328) is used, which has the following features:

- High applicability: OSPF supports networks of various sizes and can support up to several hundred routers.
- Fast convergence: OSPF can transmit update packets immediately after the network topology changes so that the change can be synchronized in the autonomous system (AS).
- Loop-free: Since OSPF calculates routes with the shortest path tree algorithm according to the collected link states, it guarantees that no loop routes will be generated from the algorithm basis.
- Area partition: OSPF allows an autonomous system network to be divided into different areas for convenient management so that routing information transmitted between the areas is abstracted further, thereby reducing network bandwidth consumption.
- Equivalent route: OSPF supports multiple equivalent routes to the same destination.
- Routing hierarchy: OSPF has a four-level routing hierarchy. It prioritizes the routes as intra-area, inter-area, external type-1, and external type-2 routes.
- Authentication: OSPF supports interface-based packet authentication to guarantee the security of route calculation.
- Multicast transmission: OSPF supports transmitting protocol packets in multicast mode.

4.1.2 OSPF Route Calculation

Taking no account of area partition, 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). Routers on the network exchange LSAs with each other by transmitting protocol packets. Thus, each router receives the LSAs of other routers and all these LSAs form the LSDB of the router.
- An LSA describes the network topology around a router, whereas an LSDB describes the network topology of the whole network. Routers can easily transform the LSDB to a weighted directed map, which actually reflects the topology of the whole network. Obviously, all routers get exactly the same map.
- A router uses the shortest path first (SPF) algorithm to calculate the shortest path tree with itself as the root. The tree shows the routes to the nodes in the autonomous system. External routes are leaf nodes, which are marked with the routers from which they are advertised to record information outside the AS. Obviously, the routing tables obtained by different routers are different.

Furthermore, to enable individual routers to broadcast their local status information (such as available interface information and reachable neighbor information) to the whole AS, routers in the AS should establish neighboring relationship among them. In this case, the route changes on any router will result in multiple transmissions, which are unnecessary and waste the precious bandwidth resources. To solve this problem, designated router (DR) and backup designated router (BDR) are defined in OSPF. For details about DR and BDR, see section 4.1.4 III. "DR and BDR".

OSPF supports interface-based packet authentication to guarantee the security of route calculation. In addition, it transmits and receives packets in multicast (224.0.0.5 and 224.0.0.6).

4.1.3 Basic OSPF Concepts

I. Router ID

To run OSPF, a router must have a router ID. A router ID can be configured manually. If no router ID is configured, the system will automatically select an IP address from the IP addresses of the interfaces as the router ID. A router ID is selected in the following way: if loopback interface addresses are configured, the system chooses the latest configured IP address as the router ID; if no loopback interface is configured, the first configured IP address among the IP addresses of other interfaces will be the router ID.

II. Area

If all the routers on an ever-growing huge network run OSPF, the large number of routers will result in an enormous LSDB, which will consume an enormous storage space, complicate the running of SPF algorithm, and increase CPU load. Furthermore, as a network grows larger, it is more potential to have changes in the network topology. Hence, the network will often be in “flapping”, and a great number of OSPF packets will be generated and transmitted in the network. This will lower the network bandwidth utilization. In addition, each change will cause all the routers on the network re-perform route calculation.

OSPF solves the above-mentioned problem by dividing an AS into multiple areas. Areas group routers logically. A router on the border of an area belongs to more than one area. A router connecting the backbone area to a non-backbone area is called an area border router (ABR). An ABR can connect to the backbone area physically or logically.

Area partition in OSPF reduces the number of LSAs in the network and enhances OSPF scalability. To further reduce routing table size and the number of LSAs in some non-backbone areas on the edge of the AS, you can configure these areas as stub areas.

A stub area cannot import any external route. For this reason the concept NSSA area (not-so-stubby area) is introduced. In an NSSA area, type 7 LSAs are allowed to be propagated. A type 7 LSA is generated by an ASBR (autonomous system boundary router) in a NSSA area. A type 7 LSA reaching an ABR in the NSSA area is transformed into an AS-external LSA, which is then advertised to other areas.

III. Backbone area and virtual link

Backbone Area

With OSPF area partition, not all areas are equal. One of the areas is different from any other area. Its area ID is 0 and it is usually called the backbone area.

Virtual link

Since all areas must be connected to the backbone area, the concept virtual link is introduced to maintain logical connectivity between the backbone area and any other area physically separated from the backbone area.

IV. Route summary

After an AS is divided into different areas that are interconnected through OSPF ABRs, The routing information between areas can be reduced through route summary. This reduces the size of routing tables and improves the calculation speed of routers.

After an ABR in an area calculates the intra-area routes in the area, the ABR aggregates multiple OSPF routes into one LSA (based on the summary configuration) and sends the LSA outside the area.

For example, in Figure 4-1, there are three intra-area routes in Area 19: 19.1.1.0/24, 19.1.2.0/24, and 19.1.3.0/24. If route summary is configured, the three routes are aggregated into one route 19.1.0.0/16, and only one corresponding LSA, which describes the route after summary, is generated on RTA.

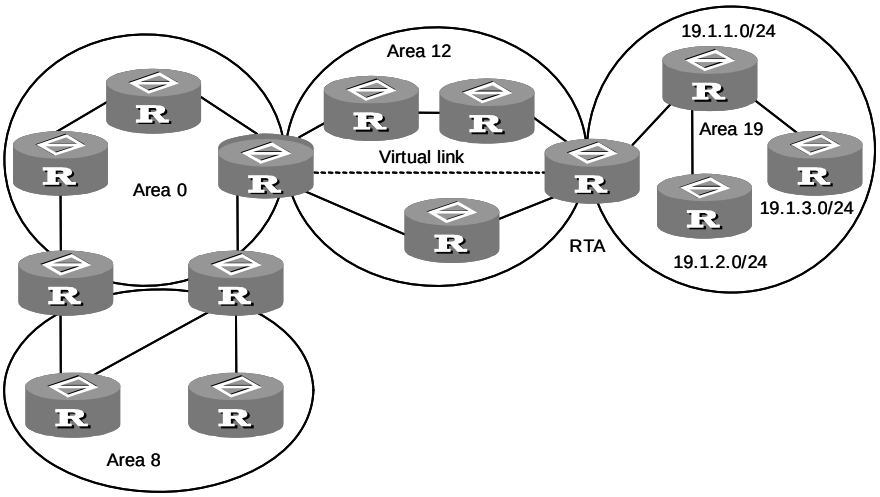


Figure 4-1 Area partition and route aggregation

4.1.4 OSPF Network Type

I. Four OSPF network types

OSPF divides networks into four types by link layer protocols:

- Broadcast: If Ethernet or FDDI is adopted, OSPF defaults the network type to broadcast. In a broadcast network, protocol packets are sent in multicast (224.0.0.5 and 224.0.0.6) by default.
- Non-broadcast multi-access (NBMA): If Frame Relay, ATM, or X.25 is adopted, OSPF defaults the network type to NBMA. In an NBMA network, protocol packets are sent in unicast.
- Point-to-multipoint (P2MP): OSPF will not default the network type of any link layer protocol to P2MP. A P2MP network must be compulsorily changed from another network type. The common practice is to change an NBMA network into a P2MP network. In a P2MP network, protocol packets are sent in multicast (224.0.0.5).
- Point-to-point (P2P): If PPP or HDLC is adopted, OSPF defaults the network type to P2P. In a P2P network, protocol packets are sent in multicast (224.0.0.5).

II. Principles for configuring an NBMA network

An NBMA network is a non-broadcast and multi-accessible network. ATM and frame relay networks are typical NBMA networks.

Some special configurations need to be done on an NBMA network. In an NBMA network, an OSPF router cannot discover an adjacent router by broadcasting Hello packets. Therefore, you must manually specify an IP address for the adjacent router and whether the adjacent router has the right to vote for a DR.

An NBMA network must be fully connected. That is, any two routers in the network must be directly reachable to each other through a virtual circuit. If two routers in the network are not directly reachable to each other, you must configure the corresponding interface type to P2MP. If a router in the network has only one peer, you can change the corresponding interface type to P2P.

The differences between NBMA and P2MP are as follows:

- An NBMA network is fully connected, non-broadcast, and multi-accessible, whereas a P2MP network is not necessarily fully connected.
- DR and BDR are required to be elected on an NBMA network but not on a P2MP network.
- NBMA is a default network type. A P2MP network, however, must be compulsorily changed from another network type. The more common practice is to change an NBMA network into a P2MP network.
- NBMA sends protocol packets in unicast and neighbors should be configured manually, while P2MP sends protocol packets in multicast.

III. DR and BDR

In a broadcast network or an NBMA network, routing information needs to be transmitted between any two routers. If there are n routers in the network, n x (n-1)/2 adjacencies need to be established. In this case, the route changes on any router will result in multiple transmissions, which waste bandwidth. To solve this problem, DR is defined in OSPF so that all routers send information to the DR only and the DR broadcasts the network link states in the network.

If the DR fails, a new DR must be elected and synchronized with the other routers on the network. The process takes quite a long time; in the process, route calculation is incorrect. To shorten the process, BDR is introduced in OSPF.

In fact, a BDR provides backup for a DR. DR and BDR are elected at the same time. Adjacencies are also established between the BDR and all the other routers on the segment, and routing information is also exchanged between them. Once the DR becomes invalid, the BDR becomes a DR. Since no re-election is needed and the adjacencies already exist, the switchover process is very short. Now, a new BDR should be elected. Although this election process will also take quite a long time, route calculation will not be affected.

Neither neighboring relationship is established nor routing information is exchanged between DR Others (routers other than DR and BDR). This reduces the number of adjacencies among routers on the broadcast or NBMA network.

In Figure 4-2, the solid lines represent physical Ethernet connections and the dotted lines represent adjacencies established. The figure shows that, with the DR/BDR mechanism adopted, seven adjacencies suffice among the five routers.

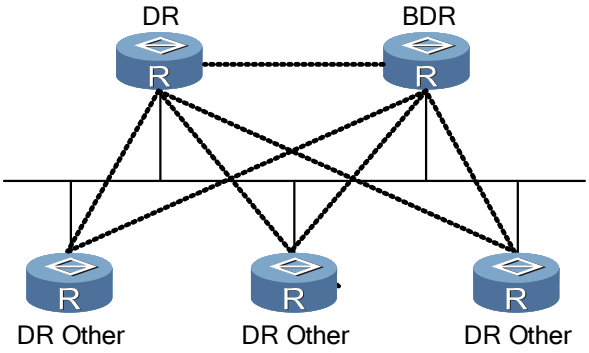


Figure 4-2 DR and BDR

IV. DR/BDR election

Instead of being manually configured, DR and BDR are elected by all the routers on the current network segment. The priority of a router interface determines the qualification of the interface in DR/BDR election. All the routers with DR priorities greater than 0 in the current network segment are eligible "candidates".

Hello packets serve as the "votes" in the election. Each router writes the DR it selects to the Hello packet and sends the packet to each router running OSPF in the network segment. If two routers on the same network segment declare themselves to be the DR, the one with the highest DR priority will be preferred. If their priorities are the same, the one with greater router ID will be preferred. A router whose DR priority is 0 can neither be elected as the DR nor be elected as the BDR.

Note the following points:

- DR election is required for broadcast or NBMA interfaces but is not required for P2P or P2MP interfaces.
- DR is based on the router interfaces in a certain segment. A router may be a DR on an interface and a BDR or DR Other on another interface.
- If a new router is added after DR and BDR election, the router does not become the DR immediately even if it has the highest DR priority.
- The DR on a network segment is not necessarily the router with the highest priority. Likewise, the BDR is not necessarily the router with the second-highest priority.

4.1.5 OSPF Packets

OSPF uses five types of packets:

I. Hello packet:

Hello packets are most commonly used OSPF packets, which are periodically sent by a router to its neighbors. A Hello packet contains the values of some timers, the DR, the BDR and the known peers.

II. DD packet:

When two routers synchronize their databases, they use database description (DD) packets to describe their own LSDBs, including the digest of each LSA. The digest refers to the HEAD of an LSA which uniquely identifies the LSA. This reduces the size of traffic transmitted between the routers because the HEAD of an LSA only occupies a small portion of the LSA. With the HEAD, the peer router can judge whether it has the LSA or not.

III. LSR packet:

After exchanging DD packets, the two routers know which LSAs of the peer router are lacked in the local LSDB, and send link state request (LSR) packets requesting for the lacked LSAs to the peer. These LSR packets contain the digest of the needed LSAs.

IV. LSU packet:

Link state update (LSU) packets are used to transmit the needed LSAs to the peer router. An LSU packet is a collection of multiple LSAs (complete LSAs, not LSA digest).

V. LSAck packet

Link state acknowledgment (LSAck) packets are used to acknowledge received LSU packets. An LSAck contains the HEAD(s) of LSA(s) to be acknowledged (one LSAck packet can acknowledge multiple LSAs).

4.1.6 LSA Types

I. Five basic LSA types

As described in the preceding sections, LSAs are the primary source for OSPF to calculate and maintain routes. RFC 2328 defines five types of LSAs:

- Router-LSA: Type-1 LSAs, generated by every router to describe the router's link states and costs and advertised only in the area where the router resides.
- Network-LSA: Type-2 LSAs, generated by the DRs of broadcast or NBMA network to describe the link states of the current network segment and are advertised only in the area where the DRs reside.
- Summary-LSA: Type-3 and Type-4 LSAs, generated by ABRs and advertised in the areas associated with the LSAs. Each Summary-LSA describes a route to a destination in another area of the AS (also called inter-area route).Type-3

Summary-LSAs are for routes to networks (that is, their destinations are segments), while Type-4 Summary-LSAs are for routes to ASBRs.

- AS-external-LSA: Type-5 LSA, also called ASE LSA, generated by ASBRs to describe the routes to other ASs and advertised to the whole AS (excluding stub areas). The default AS route can also be described by AS-external-LSAs.

II. Type-7 LSAs

In RFC 1587 (OSPF NSSA Option), Type-7 LSA, a new LSA type, is added.

As described in RFC 1587, Type-7 LSAs and Type-5 LSAs mainly differ in the following two ways:

- Type-7 LSAs are generated and advertised in an NSSA, where Type-5 LSAs will not be generated or advertised.
- Type-7 LSAs can only be advertised in an NSSA area. When Type-7 LSAs reach an ABR, the ABR can convert part of the routing information carried in the Type-7 LSAs into Type-5 LSAs and advertise the Type-5 LSAs. Type-7 LSAs are not directly advertised to other areas (including the backbone area).

4.1.7 OSPF Features

S3600 series support the following OSPF features:

- Stub area: Stub area is defined to reduce the cost for the routers in the area to receive ASE routes.
- NSSA area: NSSA area is defined to remove the limit on the topology in a stub area.
- OSPF multi-process: Multiple OSPF processes can be run on a router.
- Sharing discovered routing information with other dynamic routing protocols: At present, OSPF supports importing the routes of other dynamic routing protocols (such as RIP), and static routes as OSPF external routes into the AS to which the router belongs. In addition, OSPF supports advertising the routing information it discovered to other routing protocols.
- Authentication key: OSPF supports the authentication of the packets between neighboring routers in the same area by using one of the two methods: plain text authentication key and MD5 authentication key.
- Flexible configuration of router interface parameters: For a router interface, you can configure the following OSPF parameters: output cost, Hello interval, retransmission interval, interface transmission delay, route priority, dead time for a neighboring router, and packet authentication mode and authentication key.
- Virtual link: Virtual links can be configured.

4.2 OSPF Configuration Tasks

Table 4-1 OSPF configuration tasks

Configuration task		Description	Related section
Basic OSPF configuration		Required	4.3
OSPF area attribute configuration		Optional	4.4
OSPF network type configuration	Configuring the network type of an OSPF interface	Optional	4.5.2
	Configuring an NBMA neighbor	Optional	4.5.3
	Configuring the DR priority on an OSPF interface	Optional	4.5.4
OSPF route control	Configuring OSPF route summary	Optional	4.6.2
	Configuring OSPF to filter received routes	Optional	4.6.3
	Configuring the cost for sending packets on an OSPF interface	Optional	4.6.4
	Configuring OSPF route priority	Optional	4.6.5
	Configuring the maximum number of OSPF equal-cost routes	Optional	4.6.6
	Configuring OSPF to import external routes	Optional	4.6.7

Configuration task		Description	Related section
OSPF network adjustment and optimization	Configuring OSPF timers	Optional	4.7.2
	Configuring the LSA transmission delay	Optional	4.7.3
	Configuring the SPF calculation interval	Optional	4.7.4
	Disabling OSPF packet transmission on an interface	Optional	4.7.5
	Configuring OSPF authentication	Optional	4.7.6
	Configuring to fill the MTU field when an interface transmits DD packets	Optional	4.7.7
	Enabling OSPF logging	Optional	4.7.8
	Configuring OSPF network management system (NMS)	Optional	4.7.9
Displaying and maintaining OSPF configuration		—	4.8

4.3 Basic OSPF Configuration

Before you can configure other OSPF features, you must first enable OSPF and specify the interface and area ID.

4.3.1 Configuration Prerequisites

Before configuring OSPF, perform the following tasks:

- Configuring the link layer protocol
- Configuring the network layer addresses of interfaces so that the adjacent nodes are reachable to each other at the network layer

4.3.2 Basic OSPF Configuration

Basic OSPF configuration includes:

- Configuring router ID

To ensure stable OSPF operation, you should determine the division of router IDs and manually configure them when implementing network planning. When you configure router IDs manually, make sure each router ID is uniquely used by one router in the

AS. A common practice is to set the router ID to the IP address of an interface on the router.

- Enabling OSPF

Comware supports multiple OSPF processes. To enable multiple OSPF processes on a router, you need to specify different process IDs. OSPF process ID is only locally significant; it does not affect the packet exchange between an OSPF process and other routers. Therefore, packets can be exchanged between routers with different OSPF processes IDs.

- Configuring an area and the network segments in the area. You need to plan areas in an AS before performing the corresponding configurations on each router.

When configuring the routers in the same area, please note that most configurations should be uniformly made based on the area. Wrong configuration may disable information transmission between neighboring routers and even lead to congestion or self-loop of routing information.

Table 4-2 Basic OSPF configuration

Operation	Command	Description
Enter system view	**system-view**	—
Configure the router ID	**router id** *router-id*	Optional If multiple OSPF processes run on a router, you are recommended to use the **router-id** keyword in the **ospf** command to specify different router IDs for different processes.
Enable OSPF and enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required Enter OSPF view.
Enter OSPF area view	**area** *area-id*	Required
Configure the network segments in the area	**network** *address wildcard-mask*	Required By default, an interface does not belong to any area.

Note:

- In router ID selection, the priorities of the router IDs configured with the **ospf** [*process-id* [**router-id** *router-id*]] command, the **router id** command, and the priorities of the router IDs automatically selected are in a descending order.
- Router IDs can be re-selected. A re-selected router ID takes effect only after the OSPF process is restarted.
- The **ospf** [*process-id* [**router-id** *router-id*]] command is recommended for configuring router IDs manually.
- The ID of an OSPF process or OSPF multi-instance is unique. That is, the ID of OSPF multi-instance must be different from any in-use process ID.
- One segment can belong to only one area and you must specify each OSPF interface to belong to a particular area.

4.4 OSPF Area Attribute Configuration

Area partition in OSPF reduces the number of LSAs in the network and enhances OSPF scalability. To further reduce routing table size and the number of LSAs in some non-backbone areas on the edge of the AS, you can configure these areas as stub areas.

A stub area cannot import any external route. For this reason the concept of NSSA area is introduced. Type7 LSAs can be advertised in an NSSA area. Type7 LSAs are generated by ASBRs of the NSSA area, and will be transformed into AS-external LSAs whey reaching ABRs in the NSSA area, which will then be advertised to other areas.

After area partition, the OSPF route updates between non-backbone areas are exchanged by way of the backbone area. Therefore, OSPF requires that all the non-backbone areas should keep connectivity with the backbone area and the backbone area must keep connectivity in itself.

If the physical connectivity cannot be ensured due to various restrictions, you can configure OSPF virtual links to satisfy this requirement.

4.4.1 Configuration Prerequisites

Before configuring OSPF area attributes, perform the following tasks:

- Configuring the network layer addresses of interfaces so that the adjacent nodes are reachable to each other at the network layer
- Performing basic OSPF configuration

4.4.2 Configuring OSPF Area Attributes

Table 4-3 Configure OSPF area attributes

Operation	Command	Description
Enter system view	**system-view**	—
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	—
Enter OSPF area view	**area** *area-id*	—
Configure the current area to be a stub area	**stub** [**no-summary**]	Optional By default, no area is configured as a stub area.
Configure the current area to be an NSSA area	**nssa** [**default-route-advertise** | **no-import-route** | **no-summary**]*	Optional By default, no area is configured as an NSSA area.
Configure the cost of the default route transmitted by OSPF to a stub or NSSA area	**default-cost** *cost*	Optional This can be configured on an ABR only. By default, the cost of the default route to a stub or NSSA area is 1.
Create and configure a virtual link	**vlink-peer** *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** *password* | **md5** *keyid key*]*	Optional For a virtual link to take effect, you need to use this command at both ends of the virtual link and ensure consistent configurations of the **hello**, **dead**, and other parameters at both ends.

Note:

- You must use the **stub** command on all the routers connected to a stub area to configure the area with the stub attribute.
- You must use the **nssa** command on all the routers connected to an NSSA area to configure the area with the NSSA attribute.

4.5 OSPF Network Type Configuration

OSPF divides networks into four types by link layer protocol. See section 4.1.4 "OSPF Network Type". An NBMA network must be fully connected. That is, any two routers in the network must be directly reachable to each other through a virtual circuit.

However, in many cases, this cannot be implemented and you need to use a command to change the network type forcibly.

Configure the interface type as P2MP if not all the routers are directly accessible on an NBMA network. Change the interface type to P2P if the router has only one peer on the NBMA network.

In addition, when configuring a broadcast network or NBMA network, you can also specify DR priority for each interface to control the DR/BDR selection in the network. Thus, the router with higher performance and reliability can be selected as a DR or BDR.

4.5.1 Configuration Prerequisites

Before configuring the network type of an OSPF interface, perform the following tasks:

- Configuring the network layer address of the interface so that the adjacent node is reachable at network layer
- Performing basic OSPF configuration

4.5.2 Configuring the Network Type of an OSPF Interface

Table 4-4 Configure the network type of an OSPF interface

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Configure the network type of the OSPF interface	**ospf network-type** { **broadcast** | **nbma** | **p2mp** | **p2p** }	Optional By default, the network type of an interface depends on the physical interface.

Note:

- After an interface has been configured with a new network type, the original network type of the interface is removed automatically.
- Note that, neighboring relationship can be established between two interfaces configured as broadcast, NBMA, or P2MP only if the interfaces are on the same network segment.

4.5.3 Configuring an NBMA Neighbor

Some special configurations need to be done on an NBMA network. Since an NBMA interface cannot discover the adjacent router by broadcasting Hello packets, you must manually specify the IP address of the adjacent router for the interface and whether the adjacent router has the right to vote.

Table 4-5 Configure NBMA neighbor

Operation	Command	Description
Enter system view	**system-view**	—
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required
Configure an NBMA neighbor	**peer** *ip-address* [**dr-priority** *dr-priority*]	Required By default, the priority for the neighbor of an NBMA interface is 1.

4.5.4 Configuring the DR Priority on an OSPF Interface

You can control the DR/BDR election on a broadcast or NBMA network by configuring the DR priorities of interfaces.

Table 4-6 Configure the DR priority on an OSPF interface

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the DR priority on the OSPF interface	**ospf dr-priority** *priority*	Optional The default DR priority is 1.

Note:

The DR priorities configured by the **ospf dr-priority** command and the **peer** command have different purpose:

- The priority set with the **ospf dr-priority** command is used for actual DR election.
- The priority set with the **peer** command is used to indicate if a neighbor has the right to vote. If you specify the priority to 0 when configuring a neighbor, the local router will believe that the neighbor has no right to vote and sends no Hello packet to it. This configuration can reduce the number of Hello packets on the network during the election of DR and BDR. However, if the local router is already a DR or BDR, it will send Hello packets to the neighbor whose DR priority is 0 to establish the neighboring relationship.

4.6 OSPF Route Control

Perform the following configurations to control the advertisement and reception of the routing information discovered by OSPF and import routing information discovered by other protocols.

4.6.1 Configuration Prerequisites

Before configuring OSPF route control, perform the following tasks:

- Configuring the network layer addresses of interfaces so that the adjacent nodes are reachable to each other at the network layer
- Completing basic OSPF configuration
- Configuring filter list to filter routing information

4.6.2 Configuring OSPF Route Summary

The configuration of OSPF route summary includes:

- Configuring ABR route summary,
- Configuring ASBR route summary for imported routes.

Table 4-7 Configure ABR route summary

Operation	Command	Description
Enter system view	**system-view**	—
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required
Enter area view	**area** *area-id*	Required

Operation	Command	Description
Enable ABR route summary	**abr-summary** *ip-address mask* [**advertise** | **not-advertise**]	Required This command takes effect only when it is configured on an ABR. By default, this function is disabled on an ABR.

Table 4-8 Configure ASBR route summary

Operation	Command	Description
Enter system view	**system-view**	—
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required
Enable ASBR route summary	**asbr-summary** *ip-address mask* [**not-advertise** | **tag** *value*]	Required This command takes effect only when it is configured on an ASBR. By default, summary of imported routes is disabled.

4.6.3 Configuring OSPF to Filter Received Routes

Table 4-9 Configure OSPF to filter received routes

Operation	Command	Description
Enter system view	**system-view**	—
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required
Configure to filter the received routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**	Required By default, OSPF does not filter received routing information.

Note:

OSPF is a dynamic routing protocol based on link state, with routing information hidden in LSAs. Therefore, OSPF cannot filter any advertised or received LSA. In fact, the **filter-policy import** command filters the routes calculated by OSPF; only the routes passing the filter can be added to the routing table.

4.6.4 Configuring the Cost for Sending Packets on an OSPF Interface

Table 4-10 Configure the cost for sending packets on an OSPF interface

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the cost for sending packets on an OSPF interface	**ospf cost** *value*	Optional By default, OSPF calculates the cost for sending packets on an interface according to the current baud rate on the interface. For a VLAN interface on the switch, this value is fixed at 10.

4.6.5 Configuring OSPF Route Priority

Since multiple dynamic routing protocols may be running on one router, the problem of route sharing and selection between various routing protocols arises. The system sets a priority for each routing protocol (which you can change manually), and when more than one route to the same destination is discovered by different protocols, the route with the highest priority will take preference over other routes.

Table 4-11 Configure OSPF route priority

Operation	Command	Description
Enter system view	**system-view**	—
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required
Configure OSPF route priority	**preference** [**ase**] *value*	Optional By default, the OSPF route priority is 10 and the priority of OSPF ASE is 150.

4.6.6 Configuring the Maximum Number of OSPF Equal-Cost Routes

Table 4-12 Configure the maximum number of OSPF equal-cost routes

Operation	Command	Description
Enter system view	**system-view**	—

Operation	Command	Description
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required
Configure the maximum number of OSPF equal-cost routes	**multi-path-number** *value*	Optional

4.6.7 Configuring OSPF to Import External Routes

Table 4-13 Configure OSPF to import external routes

Operation	Command	Description
Enter system view	**system-view**	—
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required
Enable OSPF to import routes of other protocols	**import-route** *protocol* [**cost** *value* | **type** *value* | **tag** *value* | **route-policy** *route-policy-name*]*	Required By default, OSPF does not import the routing information of other protocols.
Enable OSPF to filter advertised routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-protocol*]	Optional By default, OSPF does not filter advertised routes.
Enable OSPF to import the default route	**default-route-advertise** [**always** | **cost** *value* | **type** *type-value* | **route-policy** *route-policy-name*]*	Optional By default, OSPF does not import the default route.
Configure the default cost for OSPF to import external routes	**default cost** *value*	Optional By default, the cost for OSPF to import external routes is 1.
Configure the default maximum number of external routes imported by OSPF per unit time.	**default limit** *routes*	Optional By default, a maximum of 1000 routes can be imported.
Configure the default tag for OSPF to import external routes	**default tag** *tag*	Optional The default tag is 1 if it is not set by using this command.

Operation	Command	Description
Configure the default type of external routes that OSPF will import	**default type** { **1** | **2** }	Optional By default, the type of imported external routes is Type-2.

Note:

- The **import-route** command cannot import the default route. To import the default route, you must use the **default-route-advertise** command.
- The filtering of advertised routes by OSPF means that OSPF only converts the external routes meeting the filter criteria into Type-5 or Type-7 LSAs and advertises them.
- When enabling OSPF to import external routes, you can also configure the defaults of some additional parameters, such as cost, number of routes, tag, and type. A route tag can be used to identify protocol-related information.

4.7 OSPF Network Adjustment and Optimization

You can adjust and optimize an OSPF network in the following aspects:

- By changing the OSPF packet timers, you can adjust the convergence speed of the OSPF network and the network load brought by OSPF packets. On some low-speed links, you need to consider the delay experienced when the interfaces transmit LSAs.
- By Adjusting SPF calculation interval, you can mitigate resource consumption caused by frequent network changes.
- In a network with high security requirements, you can enable OSPF authentication to enhance OSPF network security.
- In addition, OSPF supports network management. You can configure the binding of the OSPF MIB with an OSPF process and configure the Trap message transmission and logging functions.

4.7.1 Configuration Prerequisites

Before adjusting and optimizing an OSPF network, perform the following tasks:

- Configuring the network layer addresses of interfaces so that the adjacent nodes are reachable to each other at the network layer
- Configuring basic OSPF functions

4.7.2 Configuring OSPF Timers

The Hello intervals for OSPF neighbors must be consistent. The value of Hello interval is in inverse proportion to route convergence speed and network load.

The dead time on an interface must be at least four times of the Hello interval on the same interface.

After a router sends an LSA to a neighbor, it waits for an acknowledgement packet from the neighbor. If the router receives no acknowledgement packet from the neighbor within the retransmission interval, it retransmits the LSA to the neighbor.

Table 4-14 Configure OSPF timers

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the hello interval on the interface	**ospf timer hello** *seconds*	Optional By default, **p2p** and **broadcast** interfaces send Hello packets every 10 seconds; while **p2mp** and **NBMA** interfaces send Hello packets every 30 seconds.
Configure the poll interval on the NBMA interface	**ospf timer poll** *seconds*	Optional By default, poll packets are sent every 40 seconds.
Configure the dead time of the neighboring router on the interface	**ospf timer dead** *seconds*	Optional By default, the dead time for the OSPF neighboring router on a **p2p** or **broadcast** interface is 40 seconds and that for the OSPF neighboring router on a **p2mp** or **NBMA** interface is 120 seconds.
Configure the interval at which the router retransmits an LSA to the neighboring router on the interface	**ospf timer retransmit** *interval*	Optional By default, this interval is five seconds.

Note:

- Default Hello and Dead timer values will be restored once the network type is changed.
- Do not set an LSA retransmission interval that is too short. Otherwise, unnecessary retransmission will occur. LSA retransmission interval must be greater than the round trip time of a packet between two routers.

4.7.3 Configuring the LSA transmission delay

Table 4-15 Configure the LSA transmission delay

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the LSA transmission delay	**ospf trans-delay** *seconds*	Optional By default, the LSA transmission delay is one second.

Note:

The transmission of OSPF packets on a link also takes time. Therefore, a transmission delay should be added to the aging time of LSAs before the LSAs are transmitted. For a low-speed link, pay close attention on this configuration.

4.7.4 Configuring the SPF Calculation Interval

Whenever the LSDB of OSPF is changed, the shortest paths need to be recalculated. When the network changes frequently, calculating the shortest paths immediately after LSDB changes will consume enormous resources and affect the operation efficiency of the router. By adjusting the minimum SPF calculation interval, you can lighten the negative affection caused by frequent network changes.

Table 4-16 Configure the SPF calculation interval

Operation	Command	Description
Enter system view	**system-view**	—
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required

Operation	Command	Description
Configure the SPF calculation interval	**spf-schedule-interval** *interval*	Optional By default, the SPF calculation interval is five seconds.

4.7.5 Disabling OSPF Packet Transmission on an Interface

To prevent OSPF routing information from being acquired by the routers on a certain network, use the **silent-interface** command to disable OSPF packet transmission on the corresponding interface.

Table 4-17 Disable OSPF packet transmission through an interface

Operation	Command	Description
Enter system view	**system-view**	—
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required
Disable OSPF packet transmission on a specified interface	**silent-interface** *silent-interface-type silent-interface-number*	Optional By default, all the interfaces are allowed to transmit OSPF packets.

Note:

- On the same interface, you can disable multiple OSPF processes from transmitting OSPF packets. The **silent-interface** command, however, only applies to the OSPF interface where the specified process has been enabled, without affecting the interface for any other process.
- After an OSPF interface is set to be in silent status, the interface can still advertise its direct route. However, the Hello packets from the interface will be blocked, and no neighboring relationship can be established on the interface. This enhances OSPF networking adaptability, thus reducing the consumption of system resources.

4.7.6 Configuring OSPF Authentication

Table 4-18 Configure OSPF authentication

Operation	Command	Description
Enter system view	**system-view**	—
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required
Enter OSPF area view	**area** *area-id*	Required
Configure the authentication mode of the OSPF area	**authentication-mode** { **simple** | **md5** }	Required By default, no authentication mode is configured for an area.
Return to OSPF view	**quit**	—
Return to system view	**quit**	—
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the authentication mode of the OSPF interface	**ospf authentication-mode** { **simple** *password* | **md5** *key-id key* }	Optional By default, OSPF packets are not authenticated on an interface.

Note:

- OSPF supports packet authentication and receives only those packets that are successfully authenticated. If packet authentication fails, no neighboring relationship will be established.
- The authentication modes for all routers in an area must be consistent. The authentication passwords for all routers on a network segment must also be consistent.

4.7.7 Configuring to Fill the MTU Field When an Interface Transmits DD Packets

By default, an interface uses value 0 instead of its actual MTU value when transmitting DD packets. After the following configuration, the actual MTU value of the interface is filled in the Interface MTU field of the DD packets.

Table 4-19 Configure to fill the MTU field when an interface transmits DD packets

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet interface view	**interface** *interface-type interface-number*	Required
Enable the interface to fill in the MTU field when transmitting DD packets	**ospf mtu-enable**	Optional By default, the MTU value is 0 when an interface transmits DD packets. That is, the actual MTU value of the interface is not filled in.

4.7.8 Enabling OSPF Logging

Table 4-20 Enable OSPF logging

Operation	Command	Description
Enter system view	**system-view**	—
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	—
Enable the logging of neighbor status changes	**log-peer-change**	Optional Log neighbor status changes.

4.7.9 Configuring OSPF Network Management System (NMS)

Table 4-21 Configure OSPF MIB binding

Operation	Command	Description
Enter system view	**system-view**	—
Configure OSPF MIB binding	**ospf mib-binding** *process-id*	Optional By default, MIB is bound to the first enabled OSPF process. When multiple OSPF processes are enabled, you can configure to which OSPF process the MIB is bound.

Operation	Command	Description
Enable OSPF Trap	**snmp-agent trap enable ospf** [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifauthfail** | **vifcfgerror** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**]*	Optional You can configure OSPF to send diversified SNMP TRAP messages and specify a certain OSPF process to send SNMP TRAP messages by process ID.

4.8 Displaying and Maintaining OSPF Configuration

After the above configuration, you can use the **display** command in any view to display and verify the OSPF configuration.

You can use the **reset** command in user view to reset the OSPF counter or connection.

Table 4-22 Display and maintain configuration

Operation	Command	Description
Display brief information about one or all OSPF processes	**display ospf** [*process-id*] **brief**	You can execute the **display** command in any view.
Display OSPF statistics	**display ospf** [*process-id*] **cumulative**	
Display OSPF LSDB information	**display ospf** [*process-id* [*area-id*]] **lsdb** [**brief** | [[**asbr** | **ase** | **network** | **nssa** | **router** | **summary**] [*ip-address*]] [**originate-router** *ip-address* | **self-originate**]]	
Display OSPF peer information	**display ospf** [*process-id*] **peer** [**brief** | **statistics**]	
Display OSPF next hop information	**display ospf** [*process-id*] **nexthop**	
Display OSPF routing table	**display ospf** [*process-id*] **routing**	
Display OSPF virtual links	**display ospf** [*process-id*] **vlink**	
Display OSPF request list	**display ospf** [*process-id*] **request-queue**	
Display OSPF retransmission list	**display ospf** [*process-id*] **retrans-queue**	
Display the information about OSPF ABR and ASBR	**display ospf** [*process-id*] **abr-asbr**	
Display OSPF interface information	**display ospf** [*process-id*] **interface** *interface-type interface-number*	
Display OSPF errors	**display ospf** [*process-id*] **error**	
Display OSPF ASBR summary information	**display ospf** [*process-id*] **asbr-summary** [*ip-address mask*]	
Reset one or all OSPF processes	**reset ospf** [**statistics**] { **all** | *process-id* }	Use the **reset** command in user view.

4.9 OSPF Configuration Example

4.9.1 Configuring DR Election Based on OSPF Priority

I. Network requirements

Four S3600 switches, SwitchA, SwitchB, SwitchC, and SwitchD, which run OSPF, are on the same segment, as shown in Figure 4-3. Perform proper configurations to make SwitchA and SwitchC become DR and BDR respectively. Set the priority of SwitchA to 100 (the highest on the network) so that SwitchA is elected as the DR. Set the priority of SwitchC to 2 (the second highest priority) so that SwitchC is elected as the BDR. Set the priority of SwitchB to 0 so that SwitchB cannot be elected as the DR. No priority is set for SwitchD so it has a default priority of 1.

II. Network diagram

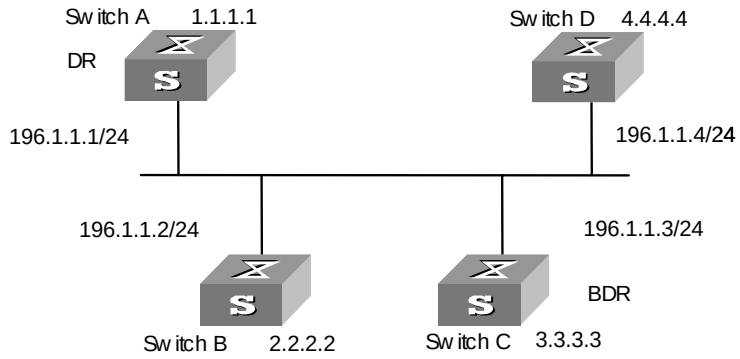


Figure 4-3 DR election based on OSPF priority

III. Configuration procedure

Configure SwitchA.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 196.1.1.1 255.255.255.0
[SwitchA-Vlan-interface1] ospf dr-priority 100
[SwitchA-Vlan-interface1] quit
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

Configure SwitchB.

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ip address 196.1.1.2 255.255.255.0
[SwitchB-Vlan-interface1] ospf dr-priority 0
```

```
[SwitchB-Vlan-interface1] quit
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

Configure SwitchC.

```
<SwitchC> system-view
[SwitchC] interface Vlan-interface 1
[SwitchC-Vlan-interface1] ip address 196.1.1.3 255.255.255.0
[SwitchC-Vlan-interface1] ospf dr-priority 2
[SwitchC-Vlan-interface1] quit
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

Configure SwitchD.

```
<SwitchD> system-view
[SwitchD] interface Vlan-interface 1
[SwitchD-Vlan-interface1] ip address 196.1.1.4 255.255.255.0
[SwitchD-Vlan-interface1] quit
[SwitchD] router id 4.4.4.4
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

On SwitchA, run the **display ospf peer** command to display its OSPF peers. Note that SwitchA has three peers.

The state of each peer is full, which means that adjacency is established between SwitchA and each peer. SwitchA and SwitchC must establish adjacencies with all the switches on the network so that they can serve as the DR and BDR respectively on the network. SwitchA is DR, while SwitchC is BDR on the network. All the other neighbors are DR others (This means that they are neither DRs nor BDRs).

Change the priority of SwitchB to 200.

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ospf dr-priority 200
```

On SwitchA, run the **display ospf peer** command to display its OSPF peers. Note that the priority of SwitchB has been changed to 200, but it is still not the DR.

The DR is changed only when the current DR turn offline. Shut down SwitchA, and run the **display ospf peer** command on SwitchD to display its peers. Note that the original BDR (SwitchC) becomes the DR and SwitchB becomes BDR now.

If all Ethernet Switches on the network are removed from and then added to the network again, SwitchB will be elected as the DR (with a priority of 200), and SwitchA will be the BDR (with a priority of 100). Shutting down and restarting all of the switches will bring about a new round of DR/BDR selection.

4.9.2 Configuring OSPF Virtual Link

I. Network requirements

As shown in Figure 4-4, Area 2 and Area 0 are not directly interconnected. It is required to use Area 1 as a transition area for interconnecting Area 2 and Area 0. Correctly configure a virtual link between SwitchB and SwitchC in Area 1.

II. Network diagram

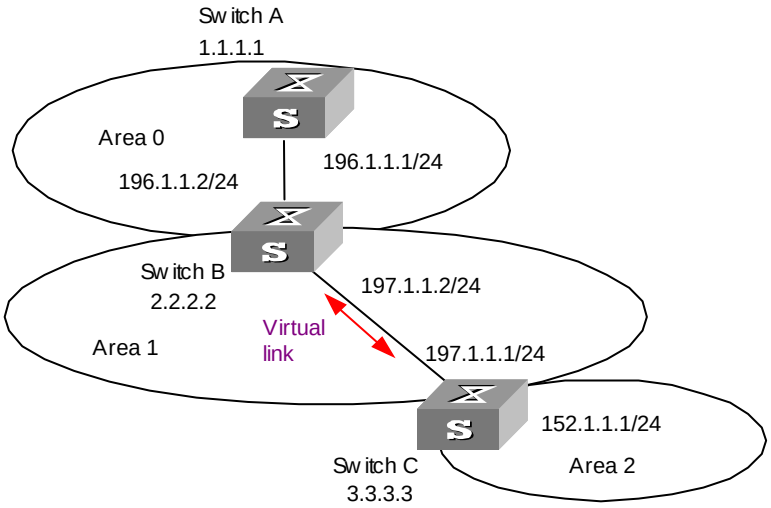


Figure 4-4 OSPF virtual link configuration

III. Configuration procedure

Configure SwitchA.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 196.1.1.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

Configure SwitchB.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
```

```
[SwitchB-Vlan-interface1] ip address 196.1.1.2 255.255.255.0
[SwitchB-Vlan-interface1] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 197.1.1.2 255.255.255.0
[SwitchB-Vlan-interface2] quit
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] network 197.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3
```

Configure SwitchC.

```
<SwitchC> system-view
[SwitchC] interface Vlan-interface 1
[SwitchC-Vlan-interface1] ip address 152.1.1.1 255.255.255.0
[SwitchC-Vlan-interface1] quit
[SwitchC] interface Vlan-interface 2
[SwitchC-Vlan-interface2] ip address 197.1.1.1 255.255.255.0
[SwitchC-Vlan-interface2] quit
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 197.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] area 2
[SwitchC-ospf-1-area-0.0.0.2] network 152.1.1.0 0.0.0.255
```

4.10 Troubleshooting OSPF Configuration

Symptom 1: OSPF has been configured in accordance with the above-mentioned steps, but OSPF does not run normally on the switch.

Solution: Perform the following procedure.

Local fault removal: Firstly, check whether the protocol works normally between two directly connected routers. The normal sign is that the peer state machine between the two routers reaches the FULL state. Note: On a broadcast or NBMA network, if the interfaces between two routers are in DROther state, the peer state machine between 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.

- Use the **display ospf peer** command to view peers.

- Use the **display ospf interface** command to view the OSPF information on an interface.
- Check whether the physical connection is correct and the lower layer protocol operates normally. You can use the **ping** command to test. If the local router cannot ping through the peer router, it indicates that faults exist on the physical link and the lower level protocol.
- If the physical connection and the lower layer protocol are normal, check the OSPF parameters configured on the interface. Verify that these parameter configurations are consistent with those on the peer interface. The area IDs must be the same, and the network segments and the masks must also be consistent (**p2p** or virtually linked segments can have different segments and masks).
- Ensure that the dead timer value is at least four times of the hello timer value on the same interface.
- If the network type is NBMA, you must use the **peer ip-address** command to manually specify a peer.
- If the network type is broadcast or NBMA, ensure that there is at least one interface with a priority greater than zero.
- If an area is set to a stub area, ensure that the area is set to a stub area for all the routers connected to this area.
- Ensure that the interface types of two neighboring routers are consistent.
- If two or more areas are configured, ensure that at least one area is configured as the backbone area; that is, the area ID of an area is 0.
- Ensure that the backbone area is connected to all the other areas.
- Ensure that no virtual link passes through a stub area.

Global fault removal: If OSPF still cannot discover the remote routes after the above procedure is performed, check the following configurations:

- If two or more areas are configured on a router, at least one area should be configured to be connected to the backbone area.

As shown in Figure 4-5, RTA and RTD are configured to belong to only one area, whereas RTB (Area 0 and Area 1) and RTC (Area 1 and Area 2) are configured to belong to two areas. RTB also belongs to area 0, which meets the requirement. However, none of the areas of RTC is Area 0. Therefore, a virtual link should be set up between RTC and RTB. Ensure that Area 2 and Area 0 (backbone area) are interconnected.

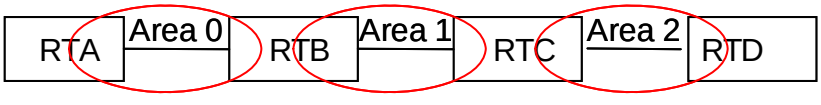


Figure 4-5 OSPF area

- A virtual link cannot pass through a stub area. The backbone area (Area 0) cannot be configured as a stub area. So, if a virtual link has been set up between RTB and RTC, neither Area 1 nor Area 0 can be configured as a stub area. In Figure 4-5, only Area 2 can be configured as a stub area.
- A router in a stub area cannot receive external routes.

The backbone area must guarantee the connectivity between various nodes.

Chapter 5 IP Routing Policy Configuration

Note:

When running a routing protocol, the Ethernet switch also functions as a router. The words “router” and the router icons covered in the following text represent routers in common sense and Ethernet switches running a routing protocol.

5.1 IP Routing Policy Overview

When a router distributes or receives routing information, it may need to implement some policies to filter the routing information, so as to receive or distribute only the routing information meeting given conditions. A routing protocol (RIP, for example) may need to import the routing information discovered by other protocols to enrich its routing knowledge. While importing routing information from another protocol, it possibly only needs to import the routes meeting given conditions and set some attributes of the imported routes to make the routes meet the requirements of this protocol.

For the implementation of a routing policy, you need to 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 as destination address and source address of the information. The matching rules can be set in advance and then used in the routing policies to advertise, receive, and import routes.

The S3600 series provide three kinds of filters (Route-policy, ACL, and ip-prefix), which can be referenced by routing protocols. The following sections introduce these filters.

I. Route-policy

A route policy is used to match some attributes with given routing information and the attributes of the information will be set if the conditions are satisfied.

A route policy can comprise multiple nodes. Each node is a unit for matching test, and the nodes will be matched in the order of their node numbers. Each node comprises a set of **if-match** and **apply** clauses. The **if-match** clauses define the matching rules. The matching objects are some attributes of routing information. The relationship among the **if-match** clauses for a node is “AND”. As a result, a matching test against a node is successful only when all the matching conditions specified by the **if-match** clauses in the node are satisfied. The **apply** clauses specify the actions performed

after a matching test against the node is successful, and the actions can be the attribute settings of routing information.

The relationships among different nodes in a route-policy are “OR”. As a result, the system examines the nodes in the route-policy in sequence, and once the route passes a node in the route-policy, it will pass the matching test of the route-policy without entering the test of the next node.

II. ACL

The S3600 series support four types of ACLs: advanced, basic, user-defined, and layer 2 ACLs.

Normally, a basic ACL is used to filter routing information. You can specify a range of IP addresses or subnets when defining a basic ACL so as to match the destination network segment addresses or next-hop addresses of routing information. If an advanced ACL is used, the specified range of source addresses will be used for matching.

For ACL configuration, see the QoS/ACL configuration section of this manual.

III. ip-prefix

ip-prefix plays a role similar to ACL. But it is more flexible than ACL and easier to understand. When ip-prefix is applied to filtering routing information, its matching object is the destination address information field of routing information. Moreover, with ip-prefix, you can use the **gateway** option to specify that only routing information advertised by certain routers will be received.

An ip-prefix is identified by its ip-prefix name. Each ip-prefix can include multiple items, and each item, identified by an index-number, can independently specify the match range in network prefix form. An index-number specifies the matching sequence in the ip-prefix.

During the matching, the router checks items identified by index-number in ascending order. Once an item is met, the ip-prefix filtering is passed and no other item will be checked.

5.2 IP Routing Policy Configuration Tasks

Table 5-1 IP routing policy configuration tasks

Configuration task		Description	Related section
Route-policy configuration	Defining a route-policy	Required	5.3.2
	Defining **if-match** clauses and **apply** clauses	—	5.3.3

Configuration task	Description	Related section
ip-prefix configuration	—	5.4
Displaying IP routing policy	—	5.5

5.3 Route-Policy Configuration

A route-policy is used to match given routing information or some attributes of routing information and change the attributes of the routing information if the conditions are met. The above-mentioned filtering lists can serve as the match conditions:

A route-policy can comprise multiple nodes and each node comprises:

- **if-match** clause: Defines matching rules; that is, the filtering conditions that the routing information should satisfy for passing the current route-policy. The matching objects are some attributes of the routing information.
- **apply** clause: Specifies actions, which are the configuration commands executed after a route satisfies the filtering conditions specified by the **if-match** clause. Thereby, some attributes of the route can be modified.

5.3.1 Configuration Prerequisites

Before configuring a route-policy, perform the following tasks:

- Configuring a filtering list,
- Configuring a routing protocol

Prepare the following data before the configuration:

- Route-policy name and node number
- Match conditions
- Route attributes to be changed

5.3.2 Defining a Route-Policy

Table 5-2 Define a route-policy

Operation	Command	Description
Enter system view	**system-view**	—
Define a route-policy and enter the route-policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	Required By default, no route-policy is defined.

Note:

- The **permit** argument specifies the matching mode for a defined node in the route-policy to be in **permit** mode. If a route matches the rules for the node, the **apply** clauses for the node will be executed and the test of the next node will not be taken. If not, however, the route takes the test of the next node.
- The **deny** argument specifies the matching mode for a defined node in the route-policy to be in **deny** mode. In this mode, no **apply** clause is executed. If a route satisfies all the **if-match** clauses of the node, no **apply** clause for the node will be executed and the test of the next node will not be taken. If not, however, the route takes the test of the next node.
- If multiple nodes are defined in a route-policy, at least one of them should be in **permit** mode. When a route-policy is applied to filtering routing information, if a piece of 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.

5.3.3 Defining if-match Clauses and apply Clauses

Table 5-3 Define if-match clauses and apply clauses

Operation	Command	Description
Enter system view	**system-view**	—
Enter the route-policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	Required
Define a rule to match the IP address of routing information	**if-match** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }	Optional By default, no matching is performed on the address of routing information.
Define a rule to match the routing cost of routing information	**if-match cost** *value*	Optional By default, no matching is performed on the routing cost of routing information.
Define a rule to match the next-hop interface of routing information	**if-match interface** *interface-type interface-number*	Optional By default, no matching is performed on the next-hop interface of routing information.

Operation	Command	Description
Define a rule to match the next-hop address of routing information	**if-match ip next-hop** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }	Optional By default, no matching is performed on the next-hop address of routing information.
Define a rule to match the tag field of OSPF routing information	**if-match tag** *value*	Optional By default, no matching is performed on the tag field of OSPF routing information.
Define an action to set the cost of routing information	**apply cost** *value*	Optional By default, no action is defined to set the routing cost of routing information.
Define an action to set the tag field of routing information	**apply tag** *value*	Optional By default, no action is defined to set the tag field of OSPF routing information.

Note:

- A route-policy comprises multiple nodes. The relationship among the nodes in a route-policy is “OR”. As a result, the system examines the nodes in sequence, and once the route passes a node in the route-policy, it will pass the matching test of the route-policy without entering the test of the next node.
- During the matching, the relationship among the **if-match** clauses for a route-policy node is “AND”. That is, a matching test against a node is successful only when all the matching conditions specified by the **if-match** clauses in the node are satisfied.
- If no **if-match** clauses are specified, all the routes will filter through the node.
- A node can comprise no **if-match** clause or multiple **if-match** clauses.
- Each node comprises a set of **if-match** and **apply** clauses. **if-match** clauses define matching rules. **apply** clauses specify the actions performed after a matching test against the node is successful, and the actions can be the attribute settings of routing information.

5.4 ip-prefix Configuration

ip-prefix plays a role similar to ACL and but is more flexible and easier to understand. When ip-prefix is applied to filtering routing information, its matching object is the destination address information field of routing information.

5.4.1 Configuration Prerequisites

Before configuring a filter list, prepare the following data:

- ip-prefix name
- Range of addresses to be matched
- Extended community attribute list number

5.4.2 Configuring an ip-prefix list

An ip-prefix list is identified by its ip-prefix list name. Each ip-prefix list can comprise multiple items. Each item can independently specify a match range in the form of network prefix and is identified by an index-number. For example, the following is an ip-prefix list named abcd:

- ip ip-prefix abcd index 10 permit 1.0.0.0 8
- ip ip-prefix abcd index 20 permit 2.0.0.0 8

During the matching of a route, the router checks the items in the ascending order of index-number. Once the route match an item, the route passes the filtering of the ip-prefix list and no other item will be matched.

Table 5-4 Configure an IPv4 ip-prefix list

Operation	Command	Description
Enter system view	**system-view**	—
Configure an IPv4 ip-prefix list	**ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *network len* [**greater-equal** *greater-equal* | **less-equal** *less-equal*]	Required By default, no ip-prefix list is specified. If all the list items are in **deny** mode, all routing information will be denied by the filter list. You are recommended to define the item **permit 0.0.0.0 0 greater-equal 0 less-equal 32** after multiple items in the **deny** mode so as to permit all other IPv4 routes.

Note:

If more than one ip-prefix item are defined, the match mode of at least one item should be the **permit** mode.

5.5 Displaying IP Routing Policy

After the above configuration, execute the **display** command in any view to display and verify the routing policy configuration.

Table 5-5 Display a route policy

Operation	Command	Description
Display route-policy information	**display route-policy** [*route-policy-name*]	You can execute the **display** command in any view.
Display address prefix list information	**display ip ip-prefix** [*ip-prefix-name*]	

5.6 IP Routing Policy Configuration Example

5.6.1 Configuring to Filter Received Routing Information

I. Network requirements

SwitchA communicates with SwitchB. OSPF protocol is enabled on both switches. The router ID of SwitchA is 1.1.1.1 and that of SwitchB is 2.2.2.2.

Configure three static routes and enable OSPF on SwitchA.

By configuring route filtering rules on SwitchA make the three received static routes partially visible and partially shielded: the routes of network segments 20.0.0.0 and 40.0.0.0 are visible, and the route of network segment 30.0.0.0 is shielded.

View the OSPF routing table to check the routing policy takes effect.

II. Network diagram

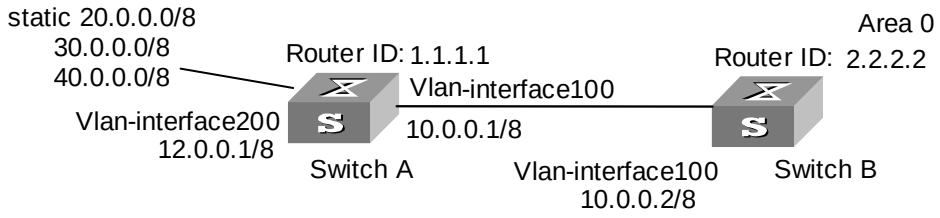


Figure 5-1 Filtering received routing information

III. Configuration procedure

- Configure SwitchA:

Configure the IP addresses of the interfaces.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] ip address 10.0.0.1 255.0.0.0
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ip address 12.0.0.1 255.0.0.0
[SwitchA-Vlan-interface200] quit
```

Configure three static routes.

```
[SwitchA] ip route-static 20.0.0.1 255.0.0.0 12.0.0.2
[SwitchA] ip route-static 30.0.0.1 255.0.0.0 12.0.0.2
[SwitchA] ip route-static 40.0.0.1 255.0.0.0 12.0.0.2
```

Enable the OSPF protocol and specify the ID of the area to which the interface 10.0.0.1 belongs.

```
<SwitchA> system-view
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1]quit
```

Configure an ACL.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule deny source 30.0.0.0 0.255.255.255
[SwitchA-acl-basic-2000] rule permit source any
[SwitchA-acl-basic-2000] quit
```

Configure a route-policy.

```
[SwitchA] route-policy ospf permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] quit
```

Apply route policy when the static routes are imported.

```
[SwitchA] ospf
[SwitchA-ospf-1] import-route static route-policy ospf
```

- Configure SwitchB:

Configure the IP address of the interface.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 10.0.0.2 255.0.0.0
[SwitchB-Vlan-interface100] quit
```

Enable the OSPF protocol and specify the ID of the area to which the interface belongs.

```
[SwitchB] router id 2.2.2.2
```

```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Display the OSPF routing table on SwitchB and check if route policy takes effect.

```
<SwitchB> display ospf routing

          OSPF Process 1 with Router ID 2.2.2.2
                  Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 10.0.0.0/8         1     Transit    10.0.0.2        1.1.1.1         0.0.0.0

 Routing for ASEs
 Destination       Cost      Type       Tag        NextHop        AdvRouter
 20.0.0.0/8        1         Type2      1          10.0.0.1       1.1.1.1
 40.0.0.0/8        1         Type2      1          10.0.0.1       1.1.1.1

 Total Nets: 3
 Intra Area: 1  Inter Area: 0  ASE: 2  NSSA: 0
```

5.7 Troubleshooting IP Routing Policy

Symptom: Routing information cannot be filtered when the routing protocol runs normally.

Solution: Check to see the following requirements are satisfied.

At least one node in a route-policy should be in **permit** mode. When a route-policy is used to filter routing information, if a piece of routing information filters through no node in the route-policy, it means that the route information does not pass the filtering of the route-policy. Therefore, when all the nodes in the route-policy are in the **deny** mode, no routing information will pass the filtering of the route-policy.

At least one item in an ip-prefix list should be in **permit** mode. The items in **deny** mode can be defined first to rapidly filter out the routing information not meeting the condition. However, if all the items are in the **deny** mode, no route will pass the ip-prefix filtering. You can define the item “**permit** 0.0.0.0 0 less-equal 32” after multiple items in the **deny** mode for all other routes to pass the filtering (if less-equal 32 is not specified, only the default route will be matched).

Chapter 6 Route Capacity Configuration

Note:

When running a routing protocol, the Ethernet switch also functions as a router. The words “router” and the router icons covered in the following text represent routers in common sense and Ethernet switches running a routing protocol.

Among S3600 series, only S3600-EI series switches support route capacity configuration.

6.1 Route Capacity Configuration Overview

6.1.1 Introduction

In practical networking applications, there are a large number of routes, especially OSPF routes, in the routing table. Normally, routing information is stored in the memory of the switch. While the size of the routing table increases, the total memory of the switch remains unchanged unless the hardware is upgraded. However, upgrading may not always solve the problem.

To solve this problem, the S3600 series provide a mechanism to control the size of the routing table; that is, monitoring the free memory in the system to determine whether to add new routes to the routing table and whether to keep the connection of a routing protocol.

Caution:

Note that, normally, the default system configuration meets the requirements. To avoid decreasing system stability and availability due to improper configuration, it is not recommended to modify the configuration yourself.

6.1.2 Route Capacity Limitation on the S3600 Series

Huge routing tables are usually caused by OSPF routes. Therefore, the route capacity limitation implemented by an S3600 Ethernet switch applies to OSPF routes only but not to static and RIP routes.

When the free memory of the switch is equal to or lower than the lower limit, OSPF connection will be disconnected and OSPF routes will be removed from the routing table.

If automatic protocol connection recovery is enabled, when the free memory of the switch restores to a value larger than the safety value, the switch automatically re-establishes the OSPF connection. If the automatic protocol connection recovery function is disabled, the switch will not reestablish the disconnected OSPF connection even when the free memory restores to a value larger than the safety value.

6.2 Route Capacity Configuration

Route capacity configuration includes:

- Configuring the lower limit and the safety value of switch memory,
- Enabling/disabling the switch to recover the disconnected routing protocol automatically.

6.2.1 Configuring the Lower Limit and the Safety Value of the Switch Memory

Table 6-1 Set the lower limit and the safety value of switch memory

Operation	Command	Description
Enter system view	**system-view**	—
Set the lower limit and the safety value of switch memory	**memory** { **safety** *safety-value* | **limit** *limit-value* }*	Optional By default, the default values are used.

Note:

The *safety-value* must be greater than the *limit-value*.

6.2.2 Enabling/Disabling Automatic Protocol Recovery

Table 6-2 Enable automatic protocol recovery

Operation	Command	Description
Enter system view	**system-view**	—
Enable automatic protocol recovery	**memory auto-establish enable**	Optional By default, automatic protocol recovery is enabled.

Table 6-3 Disable automatic protocol recovery

Operation	Command	Description
Enter system view	**system-view**	—
Disable automatic protocol recovery	**memory auto-establish disable**	Optional By default, automatic protocol recovery is enabled.

Note:

If automatic protocol recovery is disabled, the OSPF connection will not recover even when the free memory exceeds the safety value. Therefore, take cautions when disabling the function.

6.3 Displaying Route Capacity Configuration

After the above configuration, you can use the **display** command in any view to display and verify the route capacity configuration.

Table 6-4 Display route capacity configuration

Operation	Command	Description
Display memory occupancy of a switch	**display memory** [**unit** *unit-id*]	You can execute the **display** command in any view.
Display the route capacity related memory setting and state information	**display memory limit**	

Table of Contents

Chapter 1 Multicast Overview 1-1
1.1 Multicast Overview 1-1
1.1.1 Information Transmission in the Unicast Mode 1-1
1.1.2 Information Transmission in the Broadcast Mode 1-2
1.1.3 Information Transmission in the Multicast Mode 1-3
1.1.4 Advantages and Applications of Multicast 1-4
1.2 Multicast Architecture 1-5
1.2.1 Multicast Address 1-6
1.2.2 IP Multicast Protocols 1-9
1.3 Forwarding Mechanism of Multicast Packets 1-10

Chapter 2 IGMP Snooping Configuration 2-1
2.1 Overview 2-1
2.1.1 IGMP Snooping Fundamentals 2-1
2.1.2 IGMP Snooping Implementation 2-2
2.2 IGMP Snooping Configuration 2-6
2.2.1 Enabling IGMP Snooping 2-6
2.2.2 Configuring Timers 2-7
2.2.3 Enabling IGMP Fast Leave 2-8
2.2.4 Configuring IGMP Snooping Filtering ACL 2-9
2.2.5 Configuring to Limit Number of Multicast Groups on a Port 2-10
2.2.6 Configuring IGMP Querier 2-10
2.2.7 Configuring Multicast VLAN 2-11
2.3 Displaying and Maintaining IGMP Snooping 2-13
2.4 IGMP Snooping Configuration Example 2-14
2.4.1 Example 1 2-14
2.4.2 Example 2 2-15
2.5 Troubleshooting IGMP Snooping 2-18

Chapter 3 Common Multicast Configuration 3-1
3.1 Overview 3-1
3.2 Common Multicast Configuration 3-1
3.2.1 Enabling Multicast and Configuring Limit on the Number of Route Entries 3-2
3.2.2 Configuring Suppression on the Multicast Source Port 3-3
3.2.3 Clearing the Related Multicast Entries 3-3
3.3 Displaying Common Multicast Configuration 3-4

Chapter 4 Multicast MAC Address Entry Configuration 4-1
4.1 Overview 4-1
4.2 Configuring a Multicast MAC Address Entry 4-1

4.3 Displaying and Maintaining Multicast MAC Address 4-2

Chapter 5 Unknown Multicast Packet Drop Configuration 5-1

5.1 Overview 5-1

5.2 Unknown Multicast Packet Drop Configuration 5-1

Chapter 6 IGMP Configuration 6-1

6.1 Overview 6-1

6.1.1 Introduction to IGMP 6-1

6.1.2 IGMP Version 6-1

6.1.3 Work Mechanism of IGMPv1 6-1

6.1.4 Enhancements Provided by IGMPv2 6-3

6.1.5 IGMP Proxy 6-4

6.2 IGMP Configuration 6-5

6.2.1 Configuring IGMP Version 6-6

6.2.2 Configuring IGMP Query Packets 6-6

6.2.3 Configuring IGMP Multicast Groups on the Interface 6-9

6.2.4 Configuring Router Ports to Join the Specified Multicast Group 6-11

6.2.5 Configuring IGMP Proxy 6-12

6.2.6 Removing the Joined IGMP Groups from the Interface 6-13

6.3 Displaying IGMP 6-13

Chapter 7 PIM Configuration 7-1

7.1 PIM Overview 7-1

7.1.1 Introduction to PIM-DM 7-1

7.1.2 Work Mechanism of PIM-DM 7-2

7.1.3 Introduction to PIM-SM 7-4

7.1.4 Work Mechanism of PIM-SM 7-5

7.2 Common PIM Configuration 7-10

7.2.1 Enabling PIM-DM (PIM-SM) on the Interface 7-10

7.2.2 Configuring the Interval of Sending Hello Packets 7-10

7.2.3 Configuring PIM Neighbors 7-11

7.2.4 Clearing the Related PIM Entries 7-12

7.3 PIM-DM Configuration 7-13

7.3.1 Configuring Filtering Policies for Multicast Source/Group 7-13

7.4 PIM-SM Configuration 7-13

7.4.1 Configuring Filtering Policies for Multicast Source/Group 7-14

7.4.2 Configuring BSR/RP 7-14

7.4.3 Configuring PIM-SM Domain Boundary 7-16

7.4.4 Filtering the Registration Packets from RP to DR 7-17

7.4.5 Configuring the Threshold for Switching from RPT to SPT 7-18

7.5 Displaying and Debugging PIM 7-19

7.6 PIM Configuration Example 7-20

7.6.1 PIM-DM Configuration Example 7-20

7.6.2 PIM-SM Configuration Example 7-21
7.7 Troubleshooting PIM 7-24

Chapter 8 MSDP Configuration 8-1
8.1 Overview 8-1
8.1.1 MSDP Working Mechanism 8-4
8.2 Configuring MSDP Basic Functions 8-6
8.2.1 Configuration Prerequisites 8-7
8.2.2 Configuring MSDP Basic Functions 8-7
8.3 Configuring Connection between MSDP Peers 8-8
8.3.1 Configuration Prerequisites 8-8
8.3.2 Configuring Description Information for MSDP Peers 8-9
8.3.3 Configuring Anycast RP Application 8-9
8.3.4 Configuring an MSDP Mesh Group 8-10
8.3.5 Configuring MSDP Peer Connection Control 8-11
8.4 Configuring SA Message Transmission 8-11
8.4.1 Configuration Prerequisites 8-12
8.4.2 Configuring the Transmission and Filtering of SA Request Messages 8-12
8.4.3 Configuring a Rule for Filtering the Multicast Sources of SA Messages 8-13
8.4.4 Configuring a Rule for Filtering Received and Forwarded SA Messages 8-14
8.4.5 Configuring SA Message Cache 8-14
8.5 Displaying and Maintaining MSDP Configuration 8-15
8.6 MSDP Configuration Example 8-17
8.6.1 Configuration Example of Anycast RP Application 8-17
8.7 Troubleshooting MSDP Configuration 8-19
8.7.1 MSDP Peer Always in the Down State 8-19
8.7.2 No SA Entry in the SA Cache of the Router 8-19

Chapter 1 Multicast Overview

Note:

- Among S3600 series Ethernet switches, S3600-EI series support all the multicast protocols listed in this manual, while S3600-SI series only support IGMP Snooping.
- When running IP multicast protocols, Ethernet switches also provide the functions of routers. In this manual, routers stand for not only the common routers but also the Layer 3 Ethernet switches running IP multicast protocols.

1.1 Multicast Overview

With development of networks on the Internet, more and more interaction services such as data, voice, and video services are running on the networks. In addition, services highly dependent on bandwidth and real-time data interaction, such as e-commerce, web conference, online auction, video on demand (VoD), and tele-education have come into being. These services have higher requirements for information security, legal use of paid services, and network bandwidth.

In the network, packets are sent in three modes: unicast, broadcast and multicast. The following sections describe and compare data interaction processes in unicast, broadcast, and multicast.

1.1.1 Information Transmission in the Unicast Mode

In unicast, the system establishes a separate data transmission channel for each user requiring this information, and sends separate copy information to the user, as shown in Figure 1-1:

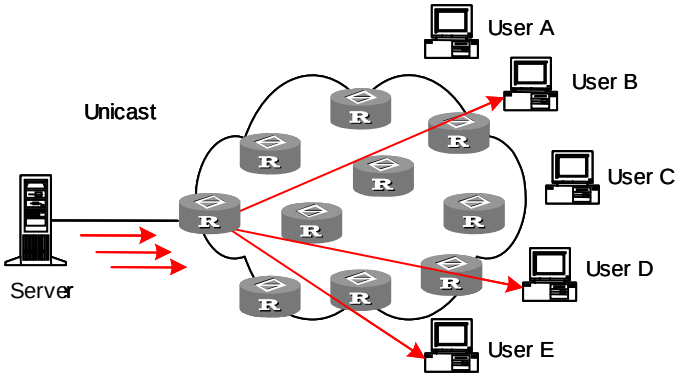


Figure 1-1 Information transmission in the unicast mode

Assume that users B, D and E need this information. The source server establishes transmission channels for the devices of these users respectively. As the transmitted traffic over the network is in direct proportion to the number of users that receive this information, when a large number of users need this information, the server must send many pieces of information with the same content to the users. Therefore, the limited bandwidth becomes the bottleneck in information transmission. This shows that unicast is not good for the transmission of a great deal of information.

1.1.2 Information Transmission in the Broadcast Mode

When you adopt broadcast, the system transmits information to all users on a network. Any user on the network can receive the information, no matter the information is needed or not. Figure 1-2 shows information transmission in broadcast mode.

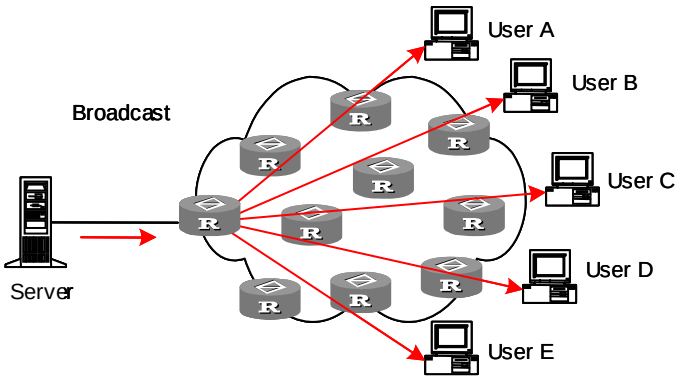


Figure 1-2 Information transmission in the broadcast mode

Assume that users B, D, and E need the information. The source server broadcasts this information through routers, and users A and C on the network also receive this information. The security and payment of the information cannot be guaranteed.

As we can see from the information transmission process, the security and legal use of paid service cannot be guaranteed. In addition, when only a small number of users on

the same network need the information, the utilization ratio of the network resources is very low and the bandwidth resources are greatly wasted.

Therefore, broadcast is disadvantageous in transmitting data to specified users; moreover, broadcast occupies large bandwidth.

1.1.3 Information Transmission in the Multicast Mode

As described in the previous sections, unicast is suitable for networks with sparsely distributed users, whereas broadcast is suitable for networks with densely distributed users. When the number of users requiring information is not certain, unicast and broadcast deliver a low efficiency.

Multicast solves this problem. When some users on a network require specified information, the multicast information sender (namely, the multicast source) sends the information only once. With tree-type routes established for multicast data packets through a multicast routing protocol, the packets are duplicated and distributed at the nearest nodes, as shown in Figure 1-3:

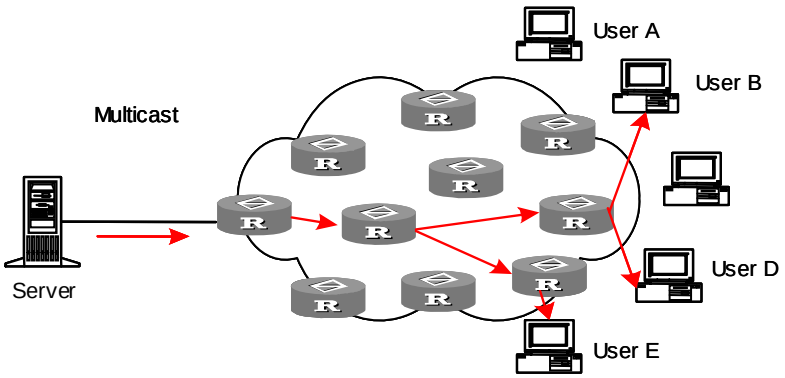


Figure 1-3 Information transmission in the multicast mode

Assume that users B, D and E need the information. To transmit the information to the right users, it is necessary to group users B, D and E into a receiver set. The routers on the network duplicate and distribute the information based on the distribution of the receivers in this set. Finally, the information is correctly delivered to users B, D, and E.

The advantages of multicast over unicast are as follows:

- No matter how many receivers exist, there is only one copy of the same multicast data flow on each link.
- With the multicast mode used to transmit information, an increase of the number of users does not add to the network burden remarkably.

The advantages of multicast over broadcast are as follows:

- A multicast data flow can be sent only to the receiver that requires the data.
- Multicast brings no waste of network resources and makes proper use of bandwidth.

In the multicast mode, network components can be divided in to the following roles:

- An information sender is referred to as a multicast source.
- Multiple receivers receiving the same information form a multicast group. Multicast group is not limited by physical area.
- Each receiver receiving multicast information is a multicast group member.
- A router providing multicast routing is a multicast router. The multicast router can be a member of one or multiple multicast groups, and it can also manage members of the multicast groups.

For a better understanding of the multicast concept, you can assimilate a multicast group to a TV channel. A TV station is a multicast source. It sends data to the channel. The audiences are the receivers. After turning on a TV set (a computer), they can select a channel to receive a program (namely join a group) and then watch the program. Therefore, a multicast group should be an agreement between the sender and the receivers, like the frequency of a channel.

Caution:

A multicast source does not necessarily belong to a multicast group. A multicast source sends data to a multicast group, and it is not necessarily a receiver. Multiple multicast sources can send packets to the same multicast group at the same time.

There may be routers that do not support multicast on the network. A multicast router encapsulates multicast packets in unicast IP packets in the tunnel mode, and then sends them to the neighboring multicast routers through the routers that do not support multicast. The neighboring multicast routers remove the header of the unicast IP packets, and then continue to multicast the packets, thus avoiding changing the network structure greatly.

1.1.4 Advantages and Applications of Multicast

I. Advantages of multicast

Advantages of multicast include:

- Enhanced efficiency: Multicast decreases network traffic and reduces server load and CPU load.
- Optimal performance: Multicast reduces redundant traffic.
- Distributive application: Multicast makes multiple-point application possible.

II. Application of multicast

The multicast technology effectively addresses the issue of point-to-multipoint data transmission. By enabling high-efficiency point-to-multipoint data transmission, over an IP network, multicast greatly saves network bandwidth and reduces network load.

Multicast provides the following applications:

- Applications of multimedia and flow media, such as Web TV, Web radio, and real-time video/audio conferencing.
- Communication for training and cooperative operations, such as remote education.
- Database and financial applications (stock), and so on.
- Any point-to-multiple-point data application.

1.2 Multicast Architecture

The purpose of IP multicast is to transmit information from a multicast source to receivers in the multicast mode and to satisfy information requirements of receivers. You should be concerned about:

- Host registration: What receivers reside on the network?
- Technologies of discovering a multicast source: Which multicast source should the receivers receive information from?
- Multicast addressing mechanism: Where should the multicast source transports information?
- Multicast routing: How is information transported?

IP multicast is a kind of peer-to-peer service. Based on the protocol layer sequence from bottom to top, the multicast mechanism contains addressing mechanism, host registration, multicast routing, and multicast application, as shown in Figure 1-4:

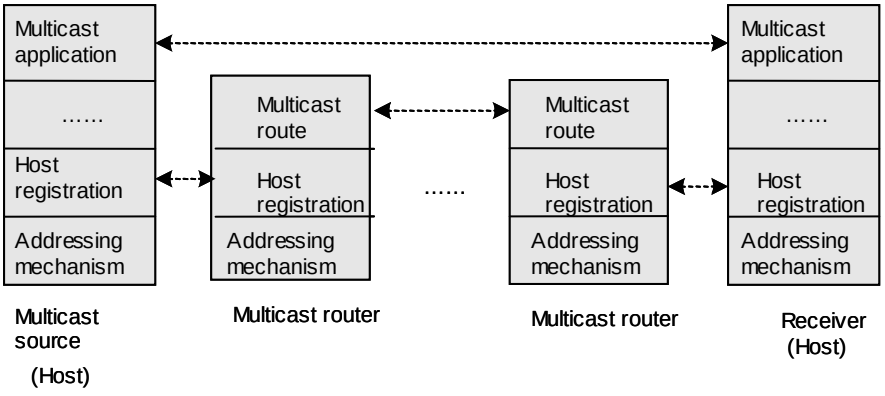


Figure 1-4 Architecture of the multicast mechanism

The multicast addressing mechanism involves the planning of multicast addresses. Host registration and multicast routing are implemented based on the IP multicast protocol. Multicast application software is not described in this chapter.

- Addressing mechanism: Information is sent from a multicast source to a group of receivers through multicast addresses.
- Host registration: A receiving host joins and leaves a multicast group dynamically to implement membership registration.
- Multicast routing: A router or switch establishes a packet distribution tree and transports packets from a multicast source to receivers.
- Multicast application: A multicast source must support multicast applications, such as video conferencing. The TCP/IP protocol suite must support the function of sending and receiving multicast information.

1.2.1 Multicast Address

As receivers are multiple hosts in a multicast group, you should be concerned about the following questions:

- What destination should the information source send the information to in the multicast mode?
- How to select the destination address, that is, how does the information source know who the user is?

These questions are about multicast addressing. To enable the communication between the information source and members of a multicast group (a group of information receivers), network-layer multicast addresses, namely, IP multicast addresses must be provided. In addition, a technology must be available to map IP multicast addresses to link-layer MAC multicast addresses. The following sections describe these two types of multicast addresses:

I. IP multicast address

Internet Assigned Numbers Authority (IANA) categorizes IP addresses into five classes: A, B, C, D, and E. Unicast packets use IP addresses of Class A, B, and C based on network scales. Class D IP addresses are used as destination addresses of multicast packets. Class D address must not appear in the IP address field of a source IP address of IP packets. Class E IP addresses are reserved for future use.

In unicast data transport, a data packet is transported hop by hop from the source address to the destination address. In an IP multicast environment, the destination address of a packet is a multicast address identifying a mutlicast group.All the receivers join a group. Once they join the group, the data sent to this group of addresses starts to be transported to the receivers. All the members in this group can receive the data packets. This group is a multicast group.

A multicast group has the following characteristics:

- The membership of a group is dynamic. A host can join and leave a multicast group at any time.
- A multicast group can be either permanent or temporary.

- A multicast group whose addresses are assigned by IANA is a permanent multicast group. It is also called reserved multicast group.

Note that:

- The IP addresses of a permanent multicast group keep unchanged, while the members of the group can be changed.
- There can be any number of, or even zero, members in a permanent multicast group.
- Those IP multicast addresses not assigned to permanent multicast groups can be used by temporary multicast groups.

Class D IP addresses range from 224.0.0.0 to 239.255.255.255. For details, see Table 1-1.

Table 1-1 Range and description of Class D IP addresses

Class D address range	Description
224.0.0.0 to 224.0.0.255	Reserved multicast addresses (IP addresses for permanent multicast groups). The IP address 224.0.0.0 is reserved. Other IP addresses can be used by routing protocols.
224.0.1.0 to 231.255.255.255 233.0.0.0 to 238.255.255.255	Available any-source multicast (ASM) multicast addresses (IP addresses for temporary groups). They are valid for the entire network.
232.0.0.0 to 232.255.255.255	Available source-specific multicast (SSM) multicast group addresses.
239.0.0.0 to 239.255.255.255	Local management multicast addresses, which are for specific local use only.

As specified by IANA, the IP addresses ranging from 224.0.0.0 to 224.0.0.255 are reserved for network protocols on local networks. The following table lists commonly used reserved IP multicast addresses:

Table 1-2 Reserved IP multicast addresses

Class D address range	Description
224.0.0.1	Address of all hosts
224.0.0.2	Address of all multicast routers
224.0.0.3	Unassigned
224.0.0.4	Distance vector multicast routing protocol (DVMRP) routers
224.0.0.5	Open shortest path first (OSPF) routers
224.0.0.6	Open shortest path first designated routers (OSPF DR)

Class D address range	Description
224.0.0.7	Shared tree routers
224.0.0.8	Shared tree hosts
224.0.0.9	RIP-2 routers
224.0.0.11	Mobile agents
224.0.0.12	DHCP server/relay agent
224.0.0.13	All protocol independent multicast (PIM) routers
224.0.0.14	Resource reservation protocol (RSVP) encapsulation
224.0.0.15	All core-based tree (CBT) routers
224.0.0.16	The specified subnetwork bandwidth management (SBM)
224.0.0.17	All SBMS
224.0.0.18	Virtual router redundancy protocol (VRRP)
224.0.0.19 to 224.0.0.255	Other protocols

Note:

Like having reserved the private network segment 10.0.0.0/8 for unicast, IANA has also reserved the network segments ranging from 239.0.0.0 to 239.255.255.255 for multicast. These are administratively scoped addresses. With the administratively scoped addresses, you can define the range of multicast domains flexibly to isolate IP addresses between different multicast domains, so that the same multicast address can be used in different multicast domains without causing collisions.

II. Ethernet multicast MAC address

When a unicast IP packet is transported in an Ethernet network, the destination MAC address is the MAC address of the receiver. When a multicast packet is transported in an Ethernet network, a multicast MAC address is used as the destination address because the destination is a group with an uncertain number of members.

As stipulated by IANA, the high-order 24 bits of a multicast MAC address are 0x01005e, while the low-order 23 bits of a MAC address are the low-order 23 bits of the multicast IP address. Figure 1-5 describes the mapping relationship:

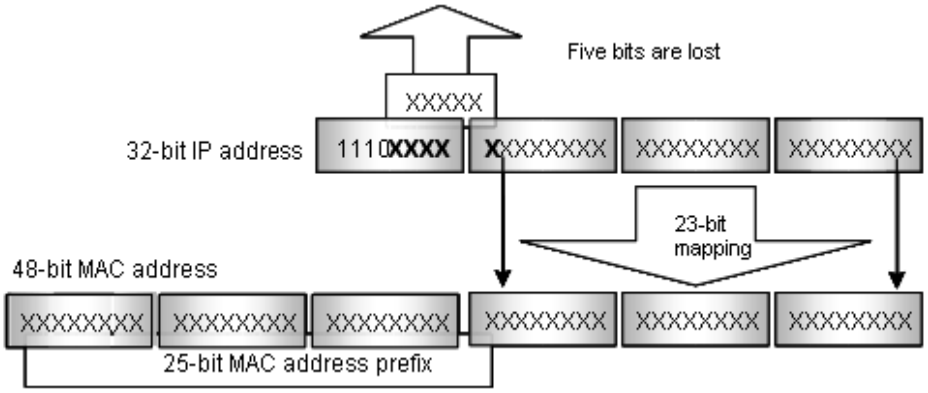


Figure 1-5 Mapping relationship between multicast IP address and multicast MAC address

The high-order four bits of the IP multicast address are 1110, representing the multicast ID. Only 23 bits of the remaining 28 bits are mapped to a MAC address. Thus, five bits of the multicast IP address are lost. As a result, 32 IP multicast addresses are mapped to the same MAC address.

1.2.2 IP Multicast Protocols

IP multicast protocols include the multicast group management protocol and the multicast routing protocol. Figure 1-6 describes the positions of the protocols related to multicast in the network.

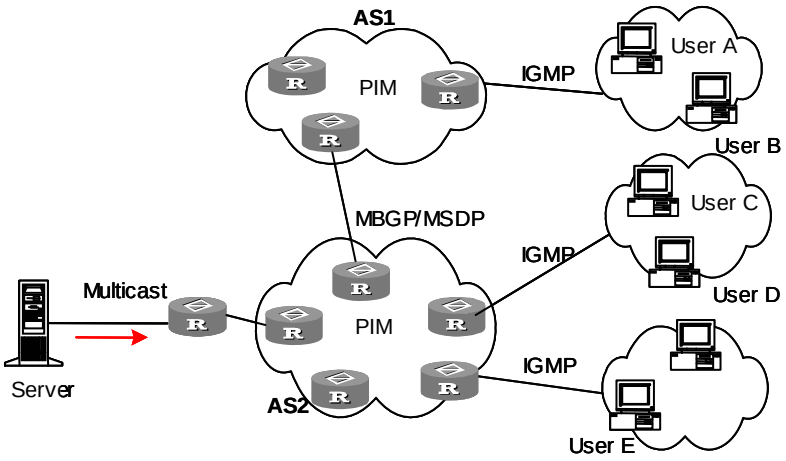


Figure 1-6 Positions of protocols related to multicast

I. Multicast group management protocol

Internet group membership protocol (IGMP) is adopted between hosts and multicast routers. This protocol defines the mechanism of establishing and maintaining group membership between hosts and multicast routers.

II. Multicast routing protocols

A multicast routing protocol operates between multicast routers to establish and maintain multicast routes and forward multicast packets accurately and effectively. A multicast route establishes a loop-free data transport path from a data source to multiple receivers. The task of multicast routing protocol is to establish a distribution tree structure. Multicast routers can establish the data transmission path (namely, distribution tree) in many ways.

Like unicast routes, multicast routes come in intra-domain routes and inter-domain routes. Intra-domain multicast routes are quite mature now. Protocol independent multicast (PIM) is the most commonly used protocol currently. It can cooperate with any unicast routing protocol.

1.3 Forwarding Mechanism of Multicast Packets

In a multicast model, a multicast source host transports information to the host group, which is identified by the multicast group address in the destination address field of an IP data packet. Unlike a unicast model, a multicast model must forward data packets to multiple external interfaces so that all receiver sites can receive the packets. Therefore the forwarding process of multicast is more complicated than that of unicast.

In order to guarantee the transmission of multicast packets in the network, multicast packets must be forwarded based on unicast routing tables or those specially provided to multicast (such as an MBGP multicast routing table). In addition, to prevent the interfaces from receiving the same information from different peers, routers must check the receiving interfaces. This check mechanism is reverse path forwarding (RPF) check, which is the basis of performing multicast forwarding for most multicast routing protocols.

Based on source addresses, multicast routers judge whether multicast packets come from specified interfaces; that is, RPF check determines whether inbound interfaces are correct by comparing the interfaces that the packets reach with the interfaces that the packets should reach. If the router resides on a shortest path tree (SPT), the interface that multicast packets should reach points to the multicast source. If the router resides on a rendezvous point tree (RPT), the interface that multicast packets should reach points to the rendezvous point (RP). When multicast data packets reach the router, if RPF check passes, the router forwards the data packets based on multicast forwarding entries; otherwise, the data packets are dropped.

Chapter 2 IGMP Snooping Configuration

2.1 Overview

2.1.1 IGMP Snooping Fundamentals

Internet group management protocol snooping (IGMP Snooping) is a multicast control mechanism running on Layer 2 switches. It is used to manage and control multicast groups.

When the IGMP messages transferred from the hosts to the router pass through the Layer 2 switch, the switch uses IGMP Snooping to analyze and process the IGMP messages, as shown in Table 2-1.

Table 2-1 IGMP message processing on the switch

Received message type	Sender	Receiver	Switch processing
IGMP host report message	Host	Switch	Add the host to the corresponding multicast group.
IGMP leave message	Host	Switch	Remove the host from the multicast group.

By listening to IGMP messages, a switch establishes and maintains IP multicast address tables, according to which it forwards the multicast packets delivered from the router.

As shown in Figure 2-1, multicast packets are broadcast at Layer 2 when IGMP Snooping is disabled and multicast (not broadcast) at Layer 2 when IGMP Snooping is enabled.

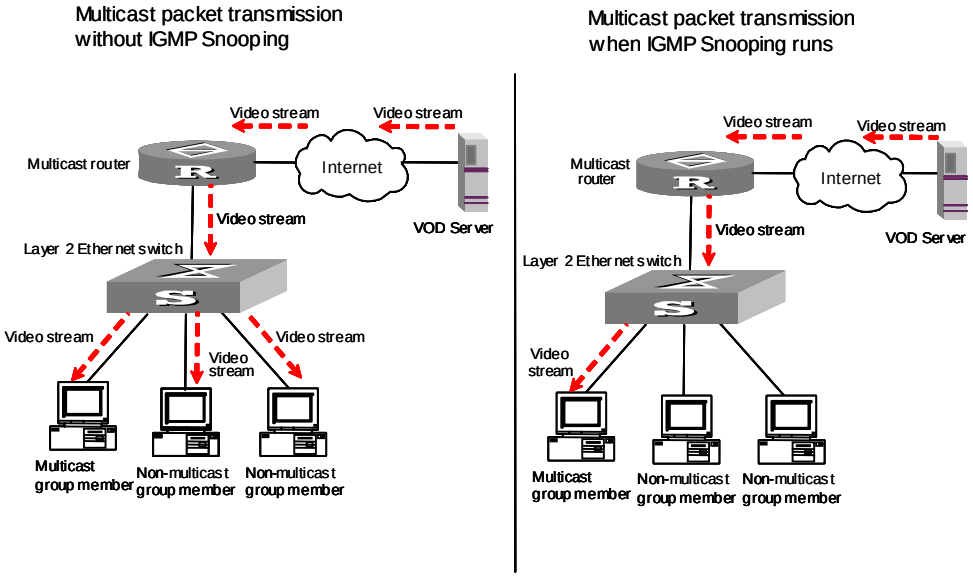


Figure 2-1 Multicast packet transmission with or without IGMP Snooping enabled

2.1.2 IGMP Snooping Implementation

I. IGMP Snooping terminologies

Before going on, we first describe the following terms involved in IGMP Snooping:

- Router port: the switch port directly connected to the multicast router.
- Multicast member port: a switch port connected to a multicast group member (a host in a multicast group).
- MAC multicast group: a multicast group identified by a MAC multicast address and maintained by the switch.

The following three timers are closely associated with IGMP snooping.

Table 2-2 IGMP Snooping timers

Timer	Setting	Packet normally received before timeout	Timeout action on the switch
Router port aging timer	Aging time of the router port	IGMP general query message	Consider that this port is not a router port any more.
Multicast member port aging timer	Aging time of the multicast member ports	IGMP message/PIM message/Dvmrp Probe message	Send an IGMP group-specific query message to the multicast member port.
Query response timer	Query response timeout time	IGMP report message	Remove the port from the member port list of the multicast group.

II. Layer 2 multicast with IGMP Snooping

The switch runs IGMP Snooping to listen to IGMP messages, based on which the multicast forward table is established.

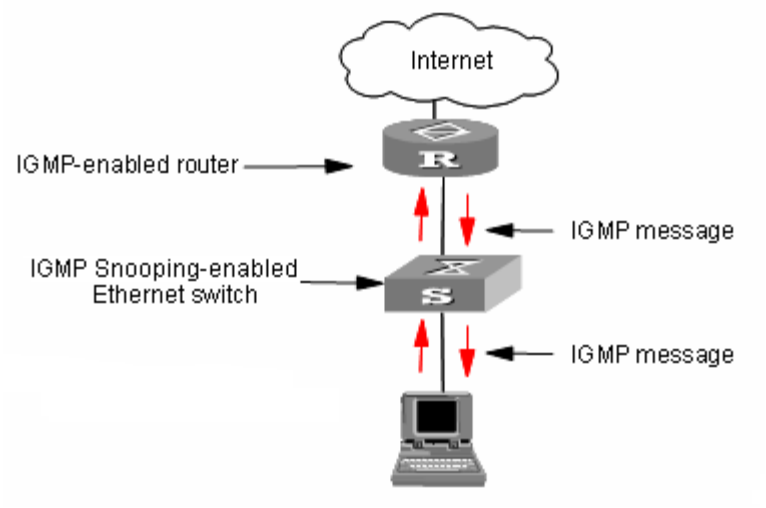


Figure 2-2 IGMP Snooping implementation

To implement Layer 2 multicast, the switch processes four different types of IGMP messages it received, as shown in Table 2-3.

Table 2-3 IGMP Snooping messages

Message	Sender	Receiver	Purpose	Switch action	
IGMP general query message	Multicast router and multicast switch	Multicast member switch and host	Query if the multicast groups contain any member	Check if the message comes from the original router port	If yes, reset the aging timer of the router port
					If not, notify the multicast router that a member is in a multicast group and start the aging timer for the router port
IGMP group-specific query message	Multicast router and multicast switch	Multicast member switch and host	Query if a specific IGMP multicast group contains any member	Send an IGMP group-specific query message to the IP multicast group being queried.	

<table>
<tr><th>Message</th><th>Sender</th><th>Receiver</th><th>Purpose</th><th colspan="4">Switch action</th></tr>
<tr><td rowspan="4">IGMP host report message</td><td rowspan="4">Host</td><td rowspan="4">Multicast router and multicast switch</td><td rowspan="4">Apply for joining a multicast group, or respond to an IGMP query message</td><td rowspan="4">Check if the IP multicast group has a corresponding MAC multicast group</td><td rowspan="3">If yes, check if the port exists in the MAC multicast group</td><td colspan="2">If yes, add the IP multicast group address to the MAC multicast group table.</td></tr>
<tr><td rowspan="2">If not, add the port to the MAC multicast group, reset the aging timer of the port and check if the corresponding IP multicast group exists.</td><td>If yes, add the port to the IP multicast group.</td></tr>
<tr><td>If not, create an IP multicast group and add the port to it.</td></tr>
<tr><td colspan="3">If not:
Create a MAC multicast group and notify the multicast router that a member is ready to join the multicast group.
Add the port to the MAC multicast group and start the aging timer of the port.
Add all ports in the VLAN owning this port to the forward port list of the MAC multicast group.
Add the port to the IP multicast group.</td></tr>
</table>

Message	Sender	Receiver	Purpose	Switch action	
IGMP leave message	Host	Multicast router and multicast switch	Notify the multicast router and multicast switch that the host is leaving its multicast group.	Multicast router and multicast switch send IGMP group-specific query packet(s) to the multicast group whose member host sends leave packets to check if the multicast group has any members and enable the corresponding query timer.	If no response is received from the port before the timer times out, the switch will check whether the port corresponds to a single MAC multicast group. • If yes, remove the corresponding MAC multicast group and IP multicast group • If no, remove only those entries that correspond to this port in the MAC multicast group, and remove the corresponding IP multicast group entries
					If no response is received from the multicast group before the timer times out, notify the router to remove this multicast group node from the multicast tree

Caution:

An IGMP-Snooping-enabled S3600 Ethernet switch judges whether the multicast group exists when it receives an IGMP leave packet sent by a host in a multicast group. If this multicast group does not exist, the switch will drop the IGMP leave packet instead of forwarding it.

2.2 IGMP Snooping Configuration

The following table lists all the IGMP Snooping configuration tasks:

Table 2-4 IGMP Snooping configuration tasks

Operation	Description	Related section
Enable IGMP Snooping	Required	Section 2.2.1 "Enabling IGMP Snooping"
Configure timers	Optional	Section 2.2.2 "Configuring Timers"
Enable IGMP fast leave	Optional	Section 2.2.3 "Enabling IGMP Fast Leave"
Configure IGMP Snooping filter	Optional	Section 2.2.4 "Configuring IGMP Snooping Filtering ACL"
Configure the number of the multicast groups a port can be added to	Optional	Section 2.2.5 "Configuring to Limit Number of Multicast Groups on a Port"
Configure IGMP Snooping queriers	Optional	Section 2.2.6 "Configuring IGMP Querier"
Configure multicast VLAN	Optional	Section 2.2.7 "Configuring Multicast VLAN"

2.2.1 Enabling IGMP Snooping

You can use the command here to enable IGMP Snooping so that it can establish and maintain MAC multicast group forwarding tables at Layer 2.

Table 2-5 Enable IGMP Snooping

Operation	Command	Description
Enter system view	**system-view**	—
Enable IGMP Snooping globally	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled globally.
Enter VLAN view	**vlan** *vlan-id*	—
Enable IGMP Snooping on the VLAN	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled on the VLAN.

Caution:

- Although both Layer 2 and Layer 3 multicast protocols can run on the same switch simultaneously, they cannot run simultaneously on a VLAN or its corresponding VLAN interface.
- Before configuring IGMP Snooping in VLAN view, you must enable IGMP Snooping globally in system view. Otherwise, the IGMP Snooping feature cannot be enabled in VLAN view.

2.2.2 Configuring Timers

This configuration task is to manually configure the aging timer of the router port, the aging timer of the multicast member ports, and the query response timer.

- If the switch receives no general IGMP query message from a router within the aging time of the router port, the switch removes the router port from the port member lists of all the multicast groups.
- If the switch receives no IGMP host report message within the aging time of the member port, it sends IGMP group-specific query to the port.

Table 2-6 Configure timers

Operation	Command	Description
Enter system view	**system-view**	—
Configure the aging timer of the router port	**igmp-snooping router-aging-time** *seconds*	Optional By default, the aging time of the router port is 105 seconds.

Operation	Command	Description
Configure the query response timer	**igmp-snooping max-response-time** *seconds*	Optional By default, the query response timeout time is 10 seconds.
Configure the aging timer of the multicast member port	**igmp-snooping host-aging-time** *seconds*	Optional By default, the aging time of multicast member ports is 260 seconds

2.2.3 Enabling IGMP Fast Leave

Normally, when receiving an IGMP Leave message, Switch does not immediately remove the port from the multicast group but sends an IGMP group-specific query message. If no response is received in a given period, it then removes the port from the multicast group.

If IGMP fast leave processing is enabled, when receiving an IGMP Leave message, Switch immediately removes the port from the multicast group. When a port has only one user, enabling IGMP fast leave processing on the port can save bandwidth.

I. Enable the IGMP fast leave in system view

Table 2-7 Enable the IGMP fast leave in system view

Operation	Command	Description
Enter system view	**system-view**	—
Enable the fast leave from the multicast groups of specific VLANs	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	Required By default, the fast leave from the multicast group for a port is disabled.

II. Enable the IGMP fast leave in Ethernet port view

Table 2-8 Enable the IGMP fast leave in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Enable the fast leave from the multicast groups of specific VLANs for a port	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	Required By default, the fast leave from the multicast group for a port is disabled.

Note:

The configuration performed in system view applies to all the ports in the specified VLANs. While the configuration performed in Ethernet port view only applies to the port in the specified VLANs.

2.2.4 Configuring IGMP Snooping Filtering ACL

You can configure multicast filtering ACLs on the switch ports connected to user ends so as to use the IGMP Snooping filter function to limit the multicast streams that the users can access. With this function, you can treat different VoD users in different ways by allowing them to access the multicast streams in different multicast groups.

In practice, when a user orders a multicast program, an IGMP report message is generated. When the message arrives at the switch, the switch examines the multicast filtering ACL configured on the access port to determine if the port can join the corresponding multicast group or not. If yes, it adds the port to the forward port list of the multicast group. If not, it drops the IGMP report message and does not forward the corresponding data stream to the port. In this way, you can control the multicast streams that users can access.

Make sure that ACL rules have been configured before configuring this feature.

Table 2-9 Configure IGMP Snooping filtering ACL

Operation	Command	Description
Enter system view	**system-view**	—
Enable IGMP Snooping filter	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	Required • You can configure the ACL to filter the IP addresses of corresponding multicast group. • By default, the multicast filtering feature is disabled.
Enter Ethernet port view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Configure the multicast filtering feature on the port	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	Optional • You can configure the ACL to filter the IP addresses of corresponding multicast group. • By default, the multicast filtering feature is disabled.

2.2.5 Configuring to Limit Number of Multicast Groups on a Port

With a limit imposed on the number of multicast groups on the switch port, users can no longer have as many multicast groups as they want when demanding multicast group programs. In this way, the bandwidth on the port is controlled.

Table 2-10 Configure to limit the number of multicast groups on a port

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Limit the number of multicast groups on a port	**igmp-snooping group-limit** *limit* [**vlan** *vlan-list* [**overflow-replace**]]	Required The number of multicast groups on a port is not limited by default.

2.2.6 Configuring IGMP Querier

In an IGMP-enabled multicast network, a query multicast router or Layer 3 multicast switch is specifically responsible for sending IGMP query packets.

However, the Layer 2 multicast switch does not support the IGMP feature. Therefore, the Layer 2 multicast switch cannot implement the querier feature and cannot send general group query packets. By configuring IGMP Snooping queriers, you can enable the Layer 2 multicast switch to send general group query packets actively at data link layer, and thereby establish and maintain the multicast forwarding entries.

Additionally, you can enable the Layer 2 switch to send the source addresses, maximum query response time, and query interval of general group query packets,

Table 2-11 Configure IGMP Snooping querier

Operation	Command	Description
Enter system view	**system-view**	—
Enable the IGMP Snooping feature in system view	**igmp-snooping enable**	Required The IGMP Snooping feature is disabled by default.
Enter VLAN view	**vlan** *vlan-id*	—
Enable the IGMP Snooping feature in VLAN view	**igmp-snooping enable**	Required By default, the IGMP Snooping feature is disabled.
Configure the IGMP Snooping querier feature	**igmp-snooping querier**	Required The IGMP Snooping querier feature is disabled by default.
Configure the interval of sending general query packets	**igmp-snooping query-interval** *seconds*	Optional By default, the interval of sending general query packets is 60 seconds.
Configure the source IP address to send general query packets	**igmp-snooping general-query source-ip** { **current-interface** | *ip-address* }	Optional By default, the source IP address to send general query packets is 0.0.0.0.

2.2.7 Configuring Multicast VLAN

In an old multicast mode, when users in different VLANs order the same multicast group, the multicast stream is copied to each of the VLANs. This mode wastes a lot of bandwidth.

By configuring a multicast VLAN, adding switch ports to the multicast VLAN and enabling IGMP Snooping, you can make users in different VLANs share the same multicast VLAN. This saves bandwidth since multicast streams are transmitted only within the multicast VLAN, and also guarantees security because the multicast VLAN is isolated from user VLANs.

Multicast VLAN is mainly used in Layer 2 switching, but you must make corresponding configuration on the Layer 3 switch.

Perform the following configuration to configure multicast VLAN.

Table 2-12 Configure multicast VLAN on Layer 3 switch

Operation	Command	Description
Enter system view	**system-view**	—
Create a multicast VLAN and enter VLAN view	**vlan** *vlan-id*	Create the multicast VLAN to be configured.
Exit VLAN view	**quit**	—
Create a multicast VLAN interface and enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Enable IGMP	**igmp enable**	Required By default, the IGMP feature is disabled.
Exit VLAN interface view	**quit**	—
Enter the view of the Ethernet port connected to the Layer 2 switch	**interface** *interface-type interface-number*	—
Define the port as a trunk or hybrid port	**port link-type** { **trunk** | **hybrid** }	Required
Specify the VLANs to be allowed to pass through the Ethernet	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Required The multicast VLAN defined on the Layer 2 switch must be included and set as tagged.
	port trunk pvid vlan *vlan-list*	

Table 2-13 Configure multicast VLAN on Layer 2 switch

Operation	Command	Description
Enter system view	**system-view**	—
Enable IGMP Snooping globally	**igmp-snooping enable**	Required
Enter VLAN view	**vlan** *vlan-id*	*vlan-id* is a VLAN ID.
Enable IGMP Snooping on the VLAN	**igmp-snooping enable**	Required By default, the IGMP Snooping feature is disabled
Enable multicast VLAN	**service-type multicast**	Required
Exit VLAN view	**quit**	—
Enter the view of the Ethernet port connected to the Layer 3 switch	**interface** *interface-type interface-number*	—

Operation	Command	Description
Define the port as a trunk or hybrid port	**port link-type** { **trunk** | **hybrid** }	—
Specify the VLANs to be allowed to pass through the Ethernet	**port hybrid vlan** *vlan-list* { **tagged** | **untagged** }	The multicast VLAN must be included and set as tagged.
	port trunk pvid vlan *vlan-list*	
Enter the view of the Ethernet port connected to a user device	**interface** *interface-type interface-number*	—
Define the port as a hybrid port	**port link-type hybrid**	Required
Specify the VLANs to be allowed to pass the port	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Required The multicast VLAN must be included and set as untagged.

Note:

- An Isolate user VLAN cannot be configured as a multicast VLAN.
- One port can belong to only one multicast VLAN.
- The port connected to a user end can only be a hybrid port.
- The multicast member port must be in the same VLAN with the router port. Otherwise, the multicast member port cannot receive multicast packets.
- When a router port is added to a multicast VLAN, the router port must be set as a Trunk port or tagged Hybrid port. Otherwise, all the multicast member ports in this multicast VLAN cannot receive multicast packets.
- When the multicast VLAN is set up, all IGMP host report messages are broadcast in the multicast VLAN only. For a multicast member port of a non-multicast VLAN, its VLAN interface cannot establish the corresponding Layer 2 multicast entry. Therefore, you are recommended to delete the port from the multicast VLAN.

2.3 Displaying and Maintaining IGMP Snooping

After the configuration above, you can execute the **display** command in any view to verify the configuration by checking the displayed information.

You can execute the **reset** command in user view to clear the statistics information about IGMP Snooping.

Table 2-14 Display information about IGMP Snooping

Operation	Command	Description
Display the current IGMP Snooping configuration	**display igmp-snooping configuration**	You can execute the **display** commands in any view.
Display IGMP Snooping message statistics	**display igmp-snooping statistics**	
Display IP and MAC multicast groups in one or all VLANs	**display igmp-snooping group** [**vlan** *vlanid*]	
Clear IGMP Snooping statistics	**reset igmp-snooping statistics**	You can execute the **reset** command in user view.

2.4 IGMP Snooping Configuration Example

2.4.1 Example 1

Configure IGMP Snooping on a switch.

I. Network requirements

Connect the router port on the switch to the router, and connect non-router ports that belong to VLAN 10 to user PCs. Enable IGMP Snooping on the switch.

II. Network diagram

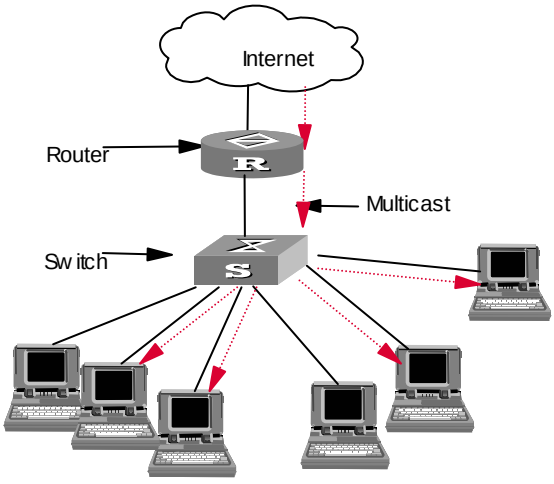


Figure 2-3 Network diagram for IGMP Snooping configuration

III. Configuration procedure

Enable IGMP Snooping in system view.

```
<H3C> system-view
[H3C] igmp-snooping enable
```

Enable IGMP Snooping on VLAN 10 where no Layer 3 multicast protocol is enabled.

```
[H3C] vlan 10
[H3C-vlan10] igmp-snooping enable
```

2.4.2 Example 2

Configure multicast VLAN on Layer 2 and Layer 3 switches.

I. Network requirements

The multicast source is Workstation. Switch A forwards the multicast data flows that the multicast source sends. The multicast data flows are forwarded by the Layer 2 switch Switch B to the end user PC1 and PC2.

Table 2-15 describes the network devices involved in this example and the configurations you should make on them.

Table 2-15 Network devices and their configurations

Device		Description
Switch A	Layer 3 switch	The interface IP address of VLAN 20 is 168.10.1.1. Ethernet1/0/1 is connected to the workstation and belongs to VLAN 20. VLAN 10 is the multicast VLAN. Ethernet1/0/5 belongs to VLAN 2, Ethernet1/0/6 belongs to VLAN 3, and Ethernet1/0/10 is connected to Switch B.
Switch B	Layer 2 switch	VLAN 2 contains Ethernet1/0/1 and VLAN 3 contains Ethernet1/0/2. The two ports are connected to PC1 and PC2, respectively. Ethernet1/0/10 is connected to Switch A.
PC 1	User 1	PC1 is connected to Ethernet1/0/1 on Switch B.
PC 2	User 2	PC2 is connected to Ethernet1/0/2 on Switch B.

Configure a multicast VLAN, so that the users in VLAN 2 and VLAN 3 can receive multicast streams through the multicast VLAN.

II. Network diagram

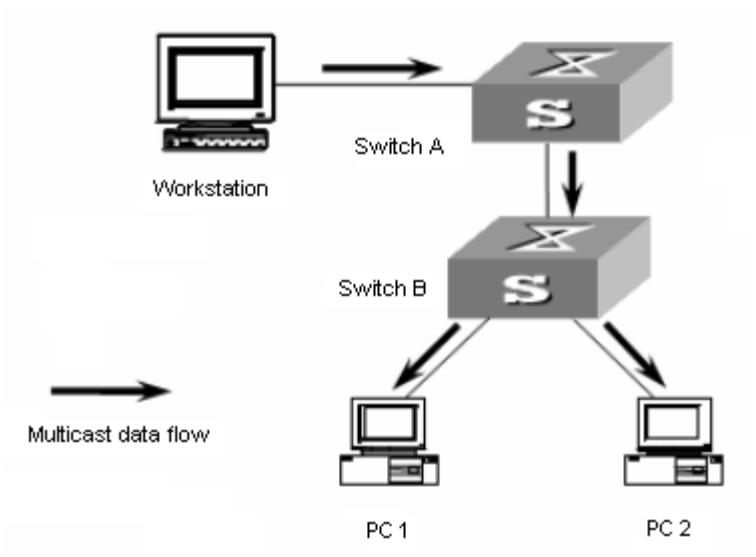


Figure 2-4 Network diagram for multicast VLAN configuration

III. Configuration procedure

The following configuration is based on the prerequisite that the devices are properly connected and all the required IP addresses are already configured.

1) Configure Switch A:

Set the interface IP address of VLAN 20 to 168.10.1.1 and enable the PIM DM protocol on the VLAN interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] vlan 20
[SwitchA-vlan20] interface Vlan-interface 20
[SwitchA-Vlan-interface20] ip address 168.10.1.1 255.255.255.0
[SwitchA-Vlan-interface20] pim dm
[SwitchA-Vlan-interface20] quit
```

Configure multicast VLAN 10.

```
[SwitchA] vlan 10
[SwitchA-vlan10] quit
```

Configure VLAN 2.

```
[SwitchA] vlan 2
[SwitchA-vlan2] quit
[SwitchA] interface Ethernet 1/0/5
[SwitchA-Ethernet1/0/5] port hybrid vlan 2
```

Configure VLAN 3.

```
[SwitchA] vlan 3
[SwitchA-vlan3] quit
[SwitchA] interface Ethernet 1/0/6
[SwitchA-Ethernet1/0/6] port hybrid vlan 3
```

Define Ethernet1/0/10 as a hybrid port, add the port to VLAN 2, VLAN 3, and VLAN 10, and configure the port to include VLAN tags in its outbound packets of VLAN 2, VLAN 3, and VLAN 10.

```
[SwitchA] interface Ethernet 1/0/10
[SwitchA-Ethernet1/0/10] port link-type hybrid
[SwitchA-Ethernet1/0/10] port hybrid vlan 2 3 10 tagged
[SwitchA-Ethernet1/0/10] quit
```

Enable PIM DM and IGMP on VLAN 10.

```
[SwitchA] interface Vlan-interface 10
[SwitchA-Vlan-interface10] pim dm
[SwitchA-Vlan-interface10] igmp enable
```

2) Configure Switch B:

Enable the IGMP Snooping feature on Switch B.

```
<SwitchB> system-view
[SwitchB] igmp-snooping enable
```

Configure VLAN 10 as a multicast VLAN and enable the IGMP Snooping feature on it.

```
[SwitchB] vlan 10
[SwitchB-vlan10] service-type multicast
[SwitchB-vlan10] igmp-snooping enable
[SwitchB-vlan10] quit
```

Define Ethernet1/0/10 as a hybrid port, add the port to VLAN 2, VLAN 3, and VLAN 10, and configure the port to include VLAN tags in its outbound packets of VLAN 2, VLAN 3, and VLAN 10.

```
[SwitchB] interface Ethernet 1/0/10
[SwitchB-Ethernet1/0/10] port link-type hybrid
[SwitchB-Ethernet1/0/10] port hybrid vlan 2 3 10 tagged
[SwitchB-Ethernet1/0/10] quit
```

Define Ethernet1/0/1 as a hybrid port, add the port to VLAN 2 and VLAN 10, and configure the port to exclude VLAN tags from its outbound packets of VLAN 2 and VLAN 10 and set VLAN 2 as the default VLAN of the port.

```
[SwitchB] interface Ethernet 1/0/1
[SwitchB-Ethernet1/0/1] port link-type hybrid
[SwitchB-Ethernet1/0/1] port hybrid vlan 2 10 untagged
[SwitchB-Ethernet1/0/1] port hybrid pvid vlan 2
[SwitchB-Ethernet1/0/1] quit
```

Define Ethernet1/0/2 as a hybrid port, add the port to VLAN 3 and VLAN 10, and configure the port to exclude VLAN tags in its outbound packets of VLAN 3 and VLAN 10, and set VLAN 3 as the default VLAN of the port.

```
[SwitchB] interface Ethernet 1/0/2
[SwitchB-Ethernet1/0/2] port link-type hybrid
[SwitchB-Ethernet1/0/2] port hybrid vlan 3 10 untagged
[SwitchB-Ethernet1/0/2] port hybrid pvid vlan 3
[SwitchB-Ethernet1/0/2] quit
```

2.5 Troubleshooting IGMP Snooping

Symptom: Multicast function does not work on the switch.

Solution:

The reason may be:

1) IGMP Snooping is not enabled.

- Use the **display current-configuration** command to check the status of IGMP Snooping.
- If IGMP Snooping is disabled, check whether it is disabled globally or on the corresponding VLAN. If it is disabled globally, use the **igmp-snooping enable** command in both system view and VLAN view to enable it both globally and on the corresponding VLAN at the same time. If it is only disabled on the corresponding VLAN, use the **igmp-snooping enable** command in VLAN view only to enable it on the corresponding VLAN.

2) Multicast forwarding table set up by IGMP Snooping is wrong.

- Use the **display igmp-snooping group** command to check if the multicast groups are expected ones.
- If the multicast group set up by IGMP Snooping is not correct, contact your technical support personnel.

Chapter 3 Common Multicast Configuration

3.1 Overview

Common multicast configuration tasks are the common contents of multicast group management protocol and multicast routing protocol. You must enable the common multicast configuration on the switch before enabling the two protocols.

Common multicast configuration includes:

- Configuring a limit on the number of route entries: When the multicast routing protocol is configured on the switch, plenty of multicast route entries will be sent to upstream Layer 3 switches or routers. In order to prevent plenty of multicast route entries from consuming all the memory of the Layer 3 switches or routers, you can configure a limit on the number of route entries to prevent too many route entries from being sent to Layer 3 switches or routers.
- Configuring suppression on the multicast source port: In the network, some users may set up multicast servers privately, which results in the shortage of multicast network resources and affects the multicast bandwidth and the transmission of valid information in the network. You can configure the suppression on the multicast source port feature to filter multicast packets on the unauthorized multicast source port, so as to prevent the users connected to the port from setting up multicast servers privately.
- Clearing the related multicast entries: By clearing the related multicast entries, you can clear the multicast route entries saved in the memory of the Layer 3 switches or routers to release the system memory

3.2 Common Multicast Configuration

Common multicast configuration tasks:

Table 3-1 Common multicast configuration tasks

Operation	Description	Related section
Enable multicast and configure limit on the number of route entries	Required	Section 3.2.1 "Enabling Multicast and Configuring Limit on the Number of Route Entries"
Configure suppression on the multicast source port	Optional	Section 3.2.2 "Configuring Suppression on the Multicast Source Port"
Clear the related multicast entries	Optional	Section 3.2.3 "Clearing the Related Multicast Entries"

3.2.1 Enabling Multicast and Configuring Limit on the Number of Route Entries

Table 3-2 Enable multicast and configure limit on the number of route entries

Operation	Command	Description
Enter system view	**system-view**	—
Enable multicast	**multicast routing-enable**	Required Multicast must be enabled before the multicast group management protocol and the multicast routing protocol are configured.
Configure limit on the number of multicast route entries	**multicast route-limit** *limit*	Optional By default, the limit on the number of multicast route entries is 256

Note:

To guard against attacks on any socket not in use, S3600 series provide the following functions to achieve enhanced security:

- The system opens RAW Socket used by multicast routing only if multicast routing is enabled.
- If you disable multicast routing, RAW Socket used by multicast routing will also be closed.

Perform the following steps to implement the above-mentioned functions:

- Use the **multicast routing-enable** command to enable multicast routing and to open RAW Socket used by multicast routing.
- Use the **undo multicast routing-enable** command to disable multicast routing as well as close RAW Socket.

Caution:

The other multicast configurations do not take effect until multicast is enabled.

3.2.2 Configuring Suppression on the Multicast Source Port

I. Configure suppression on the multicast source port in system view

Table 3-3 Configure suppression on the multicast source port in system view

Operation	Command	Description
Enter system view	**system-view**	—
Configure suppression on the multicast source port	**multicast-source-deny** [**interface** *interface-list*]	Required The suppression on the multicast source port feature is disabled by default.

II. Configure suppression on the multicast source port in Ethernet port view

Table 3-4 Configure suppression on the multicast source port in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure suppression on the multicast source port in Ethernet port view	**multicast-source-deny**	Optional The suppression on the multicast source port feature is disabled on all ports of the switch by default.

3.2.3 Clearing the Related Multicast Entries

Use the **reset** command in user view to clear the related statistics information about the common multicast configuration.

Table 3-5 Clear the related multicast entries

Operation	Command	Description
Clear the multicast forwarding case (MFC) forwarding entries or statistics information about the forwarding entries	**reset multicast forwarding-table** [**statistics**] { **all** | { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** *interface-type interface-number* } * }	Clear the related MFC forwarding entries

Operation	Command	Description
Clear the route entries in the core multicast routing table	**reset multicast routing-table** { **all** | { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | { **incoming-interface** *interface-type interface-num*ber } } * }	Clear the route entries in the core multicast routing table

3.3 Displaying Common Multicast Configuration

After the configuration above, you can execute the **display** command in any view to verify the configuration by checking the displayed information.

The multicast forwarding table is mainly used for debugging. Generally, you can get the required information by checking the core multicast routing table.

Table 3-6 Display common multicast configuration

Operation	Command	Description
Display the statistics information about the suppression on the multicast source port	**display multicast-source-deny** [**interface** *interface-type* [*interface-number*]]	This command can be executed in any view. • If neither the port type nor the port number is specified, the statistics information about the suppression on all the multicast source ports on the switch is displayed. • If only the port type is specified, the statistics information about the suppression on the multicast source ports of the type is displayed. • If both the port type and the port number are specified, the statistics information about the suppression on the specified multicast source port is displayed.

Operation	Command	Description
Display the information about the multicast routing table	**display multicast routing-table** [*group-address* [**mask** { *group-mask* | *mask-length* }] | *source-address* [**mask** { *group-mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** }]*	These commands can be executed in any view.
Display the information about the multicast forwarding table	**display multicast forwarding-table** [*group-address* [**mask** { *group-mask* | *mask-length* }] | *source-address* [**mask** { *group-mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number*] **register** }]*	
Display the information about a multicast forward table containing port information	**display mpm forwarding-table** [*group-address*]	
Display the information about the IP multicast groups and MAC multicast groups contained in a VLAN (or all the VLANs) configured on a switch	**display mpm group** [**vlan vlan-id**]	

Three kinds of tables affect data transmission. Their correlations are as follows:

- Each multicast routing protocol has its own multicast routing table.
- The multicast routing information of all multicast routing protocols is integrated to form the core multicast routing table.
- The core multicast routing table is consistent with the multicast forwarding table, which is actually in charge of multicast packet forwarding.

Chapter 4 Multicast MAC Address Entry Configuration

4.1 Overview

In Layer 2 multicast, the system can add multicast forwarding entries dynamically through a Layer 2 multicast protocol. Alternatively, you can statically bind a port to a multicast address entry by configuring a multicast MAC address entry manually.

Generally, when receiving a multicast packet whose multicast address has not yet been registered on the switch, the switch will broadcast the packet in the VLAN to which the port belongs. You can configure a static multicast MAC address entry to avoid this.

4.2 Configuring a Multicast MAC Address Entry

You can configure multicast MAC address entries in system view or Ethernet port view.

Table 4-1 Configure a multicast MAC address entry in system view

Operation	Command	Description
Enter system view	**system-view**	—
Create a multicast MAC address entry	**mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	Required The *mac-address* argument must be a multicast MAC address The *vlan-id* argument is the ID of the VLAN to which the port belongs

Table 4-2 Configure a multicast MAC address entry in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Create a multicast MAC address entry.	**mac-address multicast** *mac-address* **vlan** *vlan-id*	Required The *mac-address* argument must be a multicast MAC address The *vlan-id* argument is the ID of the VLAN to which the port belongs.

Note:

- If the multicast MAC address entry to be created already exists, the system gives you a prompt.
- If you want to add a port to a multicast MAC address entry created through the **mac-address multicast** command, you need to remove the entry first, create this entry again, and then add the specified port to the forwarding ports of this entry.
- The system does not support adding multicast MAC addresses to IRF ports. If a port is already an IRF port, the system will prompt that you cannot add multicast MAC addresses to this port.
- You cannot enable link aggregation on a port on which you have configured a multicast MAC address; and you cannot configure a multicast MAC address on an aggregation port.

4.3 Displaying and Maintaining Multicast MAC Address

After the configuration above, you can execute the **display** command in any view to verify the configuration effect by checking the displayed information.

Table 4-3 Display and maintain multicast MAC address

Operation	Command	Description
Display the multicast MAC address entry/entries manually configured	**display mac-address multicast** [**static** { { { *mac-address* **vlan** *vlan-id* **|** **vlan** *vlan-id* } [**count**] } | **count** }]	You can use the **display** command in any view.

Chapter 5 Unknown Multicast Packet Drop Configuration

5.1 Overview

Generally, if the multicast address of the multicast packet received on the switch is not registered on the local switch, the packet will be broadcast in the VLAN. When the unknown multicast packet drop feature is enabled, the switch will drop the received multicast packet whose multicast address is not registered. Thus, the bandwidth is saved and the processing efficiency of the system is improved.

5.2 Unknown Multicast Packet Drop Configuration

Table 5-1 Configure unknown multicast packet drop

Operation	Command	Description
Enter system view	**system-view**	—
Configure the unknown multicast packet drop feature	**unknown-multicast drop enable**	Required By default, the unknown multicast packet drop feature is disabled.

Chapter 6 IGMP Configuration

6.1 Overview

6.1.1 Introduction to IGMP

Internet group management protocol (IGMP) is responsible for the management of IP multicast members. It is used to establish and maintain membership between IP hosts and their directly connected neighboring routers.

However, the IGMP feature does not transmit or maintain the membership information among multicast routers. This task is completed by multicast routing protocols. All the hosts participating in multicast must support the IGMP feature.

IGMP is divided into two function parts:

- Host side: the hosts participating IP multicast can join or exit a multicast group anywhere at anytime, without being restricted on the total number of group members.
- Router side: through the IGMP protocol, a multicast router checks the network segment connected to each interface to see whether there are receivers of a multicast group, namely, group members.

A multicast router needs not and cannot save the membership information of all the hosts, while a host has to save the information that which multicast groups that it joins.

IGMP is asymmetric between the host and the router. The host needs to respond to the IGMP query packets of the multicast routers, that is, report packet responses as an IGMP hosts. The multicast router sends IGMP general query packets periodically and determines whether any host of a specified group joins its subnet based on the received response packets. When the router receives IGMP leave packets, it will send IGMPv2 group-specific query packets to find out whether the specified group still has any member.

6.1.2 IGMP Version

Until now, IGMP has three versions: including IGMP Version 1 (defined by RFC1112), IGMP Version 2 (defined by RFC2236), and IGMP Version 3.

6.1.3 Work Mechanism of IGMPv1

IGMPv1 manages multicast groups mainly based on the query and response mechanism.

Of multiple multicast routers on the same subnet, only one router is needed for sending IGMP queries because all the routers can receive IGMP reports from hosts. So, a

querier election mechanism is required to determine which router will act as the IGMP querier on the subnet.

In IGMPv1, the designated router (DR) elected by the Layer 3 multicast routing protocol (such as PIM) serves as the IGMP querier.

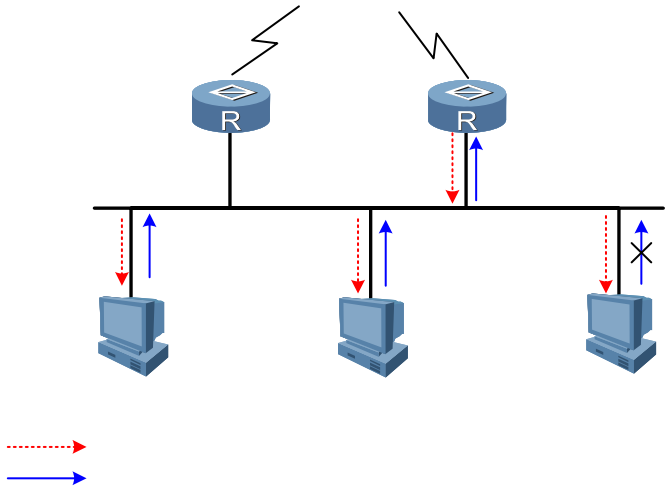


Figure 6-1 Work mechanism of IGMPv1

Assume that Host B and Host C are expected to receive multicasts address to multicast group G1, while Host A is expected to receive multicasts address to G2, as shown in Figure 6-1. The hosts join the multicast group in a process described below:

1) The IGMP querier (DR in the figure) periodically sends IGMP queries (with the destination address of 224.0.0.1) to all hosts and routers on the same subnet.
2) Upon receiving a query message, either Host B or Host C (the delay timer of whichever expires first) that is of concern to G1 sends an IGMP report first, with the destination address being the group address of G1, to announce that it will join G1. Assume it is Host B that sends the report message.
3) Because Host C is also interested in G1, it also receives the report that Host B sends to G1. Upon receiving the report, Host C will suppress itself from sending the same G1-specific message, because the IGMP routers already know that a host on the subnet is interested in G1. This IGMP report suppression mechanism helps reduce traffic over the local subnet.
4) Meanwhile, because Host A is interested in G2, it sends a report (with the group address of G2 as the destination address) to announce that it will join G2.
5) Through the query/response process, the IGMP routers learn about the receivers corresponding to G1 and G2 on the local subnet, and generate (*, G1) and (*, G2) multicast forwarding entries as the basis for forwarding the multicast information, where * represents any multicast source.
6) When the multicast data addressed to G1 or G2 reaches an IGMP router, because the (*, G1) and (*, G2) multicast forwarding entries exist on the IGMP router, the

Ethernet

router forwards the data to the local subnet so that the receivers on the subnet can receive the data.

As IGMPv1 does not specifically define a Leave Group message, upon leaving a multicast group, an IGMPv1 host stops sending reports with the destination address being the address of that multicast group. If no member of a multicast group exists on the subnet, the IGMP routers will not receive any report addressed to that multicast report, so the routers will delete the forwarding entries corresponding to that multicast group.

6.1.4 Enhancements Provided by IGMPv2

Compared with IGMPv1, IGMPv2 provides the querier election mechanism and Leave Group mechanism.

I. Querier election mechanism

In IGMPv1, the DR elected by the Layer 3 multicast routing protocol (such as PIM) serves as the querier.

In IGMPv2, an independent querier election mechanism is introduced, The querier election process is as follows:

1) Initially, every IGMPv2 router assumes itself as the querier and sends IGMP general queries (with the destination address of 224.0.0.1) to all hosts and routers on the local subnet.
2) Then, every IGMPv2 router compares the source IP address of the received message with its own interface address. After comparison, the IGMPv2 router with the lowest IP address wins the querier election and all other IGMPv2 routers are non-queriers.
3) All the IGMP routers that have lost the querier election start a timer, namely the “other querier present interval”. If a router receives an IGMP query from the querier before the timer expires, it resets its timer; otherwise, it will assume the querier to have timed out and initiate a new querier election process.

II. “Leave group” mechanism

In IGMPv1, when a host leaves a multicast group, it does not send any notification to any multicast router. As a result, a multicast router relies on the response timeout to know that a member has left a group.

In IGMPv2, on the other hand, when a host leaves a multicast group:

1) This host sends a leave message to the all-system group (224.0.0.2) on the local subnet.
2) Upon receiving the leave message, the querier sends a group-specific query to the group that the host announced to leave.

3) Up receiving this group-specific query, each of the other members of that group, if any, will send a membership report within the maximum response time specified in the query.
4) If the querier receives a membership report sent by any member of the group within the maximum response time, it will maintain the memberships of that group; otherwise, the querier will assume that there is no longer any member of that group on the subnet and will stop maintaining the memberships of the group.

6.1.5 IGMP Proxy

A lot of leaf networks (leaf domains) are involved in the application of a multicast routing protocol (PIM-DM for example) over a large-scaled network. It is a hard work to configure and manage these leaf networks.

To reduce the workload of configuration and management without affecting the multicast connection of leaf networks, you can configure an IGMP Proxy on a Layer 3 switch in the leaf network (Switch B shown in Figure 6-2). The Layer 3 switch will then forward IGMP join or IGMP leave messages sent by the connected hosts. After IGMP Proxy is configured, the leaf switch is no longer a PIM neighbor but a host for the external network. The Layer 3 switch receives the multicast data of corresponding groups only when it has directly connected members.

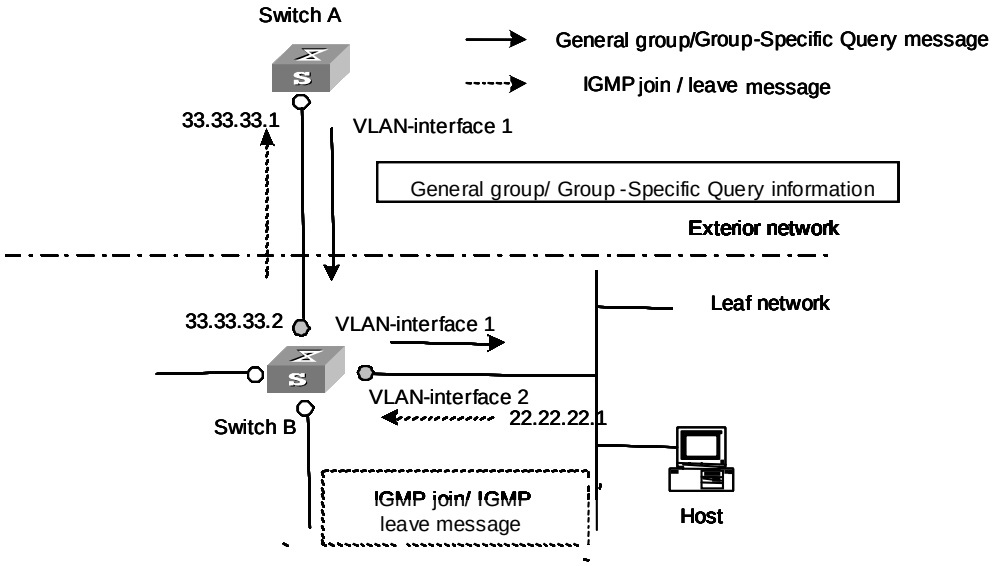


Figure 6-2 Diagram for IGMP Proxy

Figure 6-2 shows an IGMP Proxy diagram for a leaf network.

Configure Switch B as follows:

- Enable multicast routing on VLAN-interface1 and VLAN-interface2, and then configure the PIM protocol on it. And configure the IGMP protocol on VLAN-interface1 at the same time.

- On VLAN-interface2, configure VLAN-interface1 as the outbound IGMP Proxy interface to external networks. You must enable the IGMP protocol on the interface first, and then configure the **igmp proxy** command.

Configure Switch A as follows:

- Enable multicast routing and configure the IGMP protocol on VLAN-interface1.
- Configure the **pim neighbor-policy** command to filter PIM neighbors in the network segment 33.33.33.0/24. That is, Switch A does not consider Switch B as its PIM neighbor.

In this case, when Switch B of leaf network receives from VLAN-interface2 an IGMP join or IGMP leave message sent by the host, it will change the source address of the IGMP information to the address of VLAN-interface1: 33.33.33.2 and send the information to VLAN-interface1 of Switch A. For Switch A, this works as if there is a host directly connected to VLAN-interface1.

Similarly, when Switch B receives the IGMP general group or group-specific query message from the Layer 3 Switch A, it will also change the source address of the query message to the IP address of VLAN-interface2: 22.22.22.1 and send the message from VLAN-interface2.

In Figure 6-2, VLAN-interface2 of Switch B is called the client and VLAN-interface1 of Switch B is called the proxy.

6.2 IGMP Configuration

You cannot perform other IGMP configuration tasks until you enable the IGMP protocol after multicast is enabled.

IGMP configuration tasks include:

Table 6-1 Configuration task overview

Operation	Description	Related section
Configure IGMP version	Optional	Section 6.2.1 "Configuring IGMP Version"
Configure IGMP query packets	Optional	Section 6.2.2 "Configuring IGMP Query Packets"
Configure IGMP multicast groups on the interface	Optional	Section 6.2.3 “Configuring IGMP Multicast Groups on the Interface"
Configure router ports to join the specified multicast group	Optional	Section 6.2.4 "Configuring Router Ports to Join the Specified Multicast Group"
Configure IGMP Proxy	Optional	Section 6.2.5 "Configuring IGMP Proxy"

Operation	Description	Related section
Remove the joined IGMP groups from the interface	Optional	Section 6.2.6 "Removing the Joined IGMP Groups from the Interface"

6.2.1 Configuring IGMP Version

Table 6-2 Configure IGMP version

Operation	Command	Description
Enter system view	**system-view**	—
Enable the multicast routing protocol	**multicast routing-enable**	Enable the multicast routing protocol
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	—
Enable IGMP on the current interface	**igmp enable**	Required IGMP is disabled on the interface by default.
Configure the IGMP version of the Layer 3 switch (router)	**igmp version** { **1** | **2** }	Optional IGMP version 2 is used by default.

Caution:

IGMP versions cannot be switched to one another automatically. Therefore, all the Layer 3 switches on a subnet must be configured to use the same IGMP version.

6.2.2 Configuring IGMP Query Packets

I. IGMP general query packets

The Layer 3 switch sends IGMP general query packets to the connected network segment periodically to get to know which multicast groups in the network segment have members according to the returned IGMP report packets. The multicast router also sends query packets periodically. When it receives the IGMP join packets of a group member, it will refresh the membership information of the network segment.

II. IGMP group-specific packets

The query router (querier for short) maintains the IGMP join packets on the interface on the shared network. After the related features are configured, the IGMP querier will send IGMP group-specific query packets at the user-defined interval for the user-defined times when it receives the IGMP leave packets from the hosts.

Suppose a host in a multicast group decides to leave the multicast group. The related procedure is as follows:

- The host sends an IGMP leave packet.
- When the IGMP querier receives the packet, it will send IGMP group-specific query packets at the interval configured by the **igmp lastmember-queryinterval** command (the interval is 1 second by default) for the *robust-value* times (the *robust-value* argument is configured by the **igmp robust-count** command and it is 2 by default).
- If other hosts are interested in the group after receiving the IGMP group-specific query packet from the querier, they will send IGMP join packets in the maximum response time specified in the packet.
- If the IGMP querier receives IGMP join packets from other hosts within the period of *robust-value* x lastmember-queryinterval, it will maintain the membership of the group.
- If the IGMP querier does not receive IGMP join packets from other hosts after the period of *robust-value* x lastmember-queryinterval, it considers that the group has timed out and will not maintain the membership of the group.

Note:

You can use the **igmp max-response-time** command to set the maximum response time for general IGMP query packets, while that of an IGMP group-specific query packet is determined by the following expression:robust-value x lastmember-queryinterval.

The procedure is only fit for the occasion where IGMP queriers run IGMP version 2.

If the host runs IGMP version 1, it does not send IGMP leave messages when leaving a group, so the conditions will be the same as described in the procedure above.

III. IGMP querier substitution rules

In a network segment containing multiple IGMP-enabled interfaces, the one with the least IP address becomes the IGMP querier. If no query message is received within the period specified by the **igmp timer other-querier-present** command, the current IGMP querier is considered to be invalid. In this case, the interface with the second least IP address becomes the IGMP queerer instead.

IV. The maximum query time of IGMP packets

When the host receives a query message, it will set a timer for each of its multicast groups. The timer value is selected from 0 to the maximum response time at random. When the value of a timer decreases to 0, the host will send the membership information of the multicast group.

By configuring reasonable maximum response time, you can enable the host to respond to the query information quickly and enable the Layer 3 switch to understand the membership information of multicast groups quickly.

Table 6-3 Configure IGMP query packets

Operation	Command	Description
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	—
Enable IGMP on the current interface	**igmp enable**	Required IGMP is disabled on the interface by default.
Configure the query interval	**igmp timer query** *seconds*	Optional The query interval is 60 seconds by default.
Configure the interval of sending IGMP group-specific query packets	**igmp lastmember-queryinterval** *seconds*	Optional By default, the interval of sending IGMP group-specific query packets is one second.
Configure the times of sending IGMP group-specific query packets	**igmp robust-count** *robust-value*	Optional By default, the number of times of sending IGMP group-specific query packets is 2.
Configure the maximum lifetime of an IGMP querier	**igmp timer other-querier-present** *seconds*	Optional The system default is 120 seconds, twice that specified by the **igmp timer query** command.
Configure the maximum IGMP query response time	**igmp max-response-time** *seconds*	Optional The maximum IGMP query response time is 10 seconds.

Caution:

When there are multiple multicast routers in a network segment, the querier is responsible for sending IGMP query messages to all the hosts in the network segment.

6.2.3 Configuring IGMP Multicast Groups on the Interface

You can perform the following configurations on the interface for the IGMP multicast groups:

- Limit the number of joined multicast groups
- Limit the range of multicast groups that the interface serves

I. Limit the number of joined multicast groups

If the number of joined IGMP groups on the multicast routing interface of the switch is not limited, the memory of the switch may be used out and the routing interface of the switch may fail when plenty of multicast groups join in the routing interface.

You can configure a limit on the number of joined IGMP multicast groups on the interface of the switch. Thus, when users order the programs of multicast groups, the network bandwidth can be controlled because the number of multicast groups is limited.

II. Limit the range of multicast groups that the interface serves

The Layer 3 switch determines the membership of the network segment by translating the received IGMP join packets. You can configure a filter for each interface to limit the range of multicast groups that the interface serves.

Table 6-4 Configure IGMP multicast groups on the interface

Operation	Command	Description
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	—
Enable IGMP on the current interface	**igmp enable**	Required IGMP is disabled on the interface by default.
Configure a limit on the number of joined IGMP groups on the interface	**igmp group-limit** *limit*	Required By default, the number of multicast groups passing a port is not limited.

Operation	Command	Description
Limit the range of multicast groups that the interface serves	**igmp group-policy** *acl-number* [**1** | **2** | **port** *interface-type interface-number* [**to** *interface-type interface-number*]]	Optional • By default, the filter is not configured, that is, any multicast group is permitted on a port. • If the **port** keyword is specified, the specified port must belong to the VLAN of the VLAN interface. • You can configure to filter the IP addresses of some multicast groups in ACL. • 1 and 2 are the IGMP version numbers. IGMPv2 is used by default.
Quit interface view.	**quit**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Limit the range of multicast groups that the interface serves	**igmp group-policy** *acl-number* **vlan** *vlan-id*	Optional • By default, the filter is not configured, that is, any multicast group is permitted on the port. • The port must belong to the IGMP-enabled VLAN specified in the command. Otherwise, the command does not take effect.

Caution:

- If the number of joined multicast groups on the interface exceeds the user-defined limit, new groups are not allowed to join.
- If you configure the number of IGMP groups on the interface to 1, the new group takes precedence. That is, if a new group joins the interface, the former multicast group will be replaced automatically and leaves the interface automatically.
- If the number of existing IGMP multicast groups has exceeded the configured limit on the number of joined multicast groups on the interface, the system will delete some existing multicast groups automatically until the number of multicast groups on the interface is conforming to the configured limit.

6.2.4 Configuring Router Ports to Join the Specified Multicast Group

Generally, the host running IGMP will respond to the IGMP query packets of the multicast switch. If the host cannot respond for some reason, the multicast switch may consider that there is no member of the multicast group in this network segment and then cancel the corresponding paths.

In order to avoid such cases, you must configure a port of the VLAN interface of the switch as a router port to add it to the multicast group. When the port receives IGMP query packets, the multicast switch will respond to it. As a result, the network segment where the Layer 3 interfaces reside can continue to receive multicast packets.

Table 6-5 Configure router ports to join the specified multicast group

Operation	Command	Description
Enter system view	**system-view**	—
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	—
Enable IGMP on the current interface	**igmp enable**	Required IGMP is disabled on the interface by default.
Configure router ports to join a multicast group	**igmp host-join port** *group-address interface-list*	Optional By default, the router port does not join any multicast group.
Quit VLAN interface view	**quit**	—

Operation	Command	Description
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure router ports to join a multicast group	**igmp host-join** *group-address* **vlan** *vlan-id*	Optional By default, the router port does not join in any multicast group.

6.2.5 Configuring IGMP Proxy

I. Configure IGMP Proxy

You can configure IGMP proxy to reduce the workload of configuration and management of leaf networks without affecting the multicast connections of the leaf network.

After IGMP Proxy is configured on the Layer 3 switch of the leaf network, the leaf Layer 3 switch is just a host for the external network. The Layer 3 switch receives the multicast data of corresponding groups only when it has directly connected members.

Table 6-6 Configure IGMP Proxy

Operation	Command	Description
Enter system view	**system-view**	—
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter VLAN interface (connected to the external network) view	**interface Vlan-interface** *interface-number*	—
Enable the IGMP protocol	**igmp enable**	Required
Configure IGMP Proxy	**igmp proxy Vlan-interface** *interface-number*	Required

The IGMP Proxy feature is disabled by default.

Caution:

- Both the multicast routing protocol and the IGMP protocol must be enabled on the proxy interface.
- You must enable the PIM protocol on the interface before configuring the **igmp proxy** command. Otherwise, the IGMP Proxy feature does not take effect.
- One interface cannot serve as the proxy interface of two or more interfaces.

6.2.6 Removing the Joined IGMP Groups from the Interface

You can remove all the joined IGMP groups on all ports of the router or all the joined IGMP groups on the specified interfaces, or remove the specified IGMP group address or group address network segment on the specified interface.

Perform the following configuration in user view.

Table 6-7 Remove the joined IGMP groups from the interface

Operation	Command	Description
Remove the joined IGMP groups from the interface	**reset igmp group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [*group-mask*] } }	Optional

Caution:

After an IGMP group is removed from an interface, the IGMP group can join the group again.

6.3 Displaying IGMP

After completing the above-mentioned configurations, you can execute the **display** command in any view to verify the configuration by checking the displayed information.

Table 6-8 Display IGMP

Operation	Command	Description
Display the membership information of the IGMP multicast group	**display igmp group** [*group-address* | **interface** *interface-type interface-number*]	You can execute the **display** command in any view.
Display the IGMP configuration and running information of the interface	**display igmp interface** [*interface-type interface-number*]	

Chapter 7 PIM Configuration

7.1 PIM Overview

Protocol independent multicast (PIM) means that the unicast routing protocols providing routes for the multicast could be static routes, RIP, OSPF, IS-IS, or BGP. The multicast routing protocol is independent of unicast routing protocols as long as unicast routing protocols can generate route entries.

With the help of reverse path forwarding, PIM can transmit multicast information in the network. For the convenience of description, a network consisting of PIM-enabled multicast routers is called a PIM multicast domain.

7.1.1 Introduction to PIM-DM

Protocol independent multicast dense mode (PIM-DM) is a dense mode multicast protocol. It is suitable for small networks.

The features of such networks are:

- Members in a multicast group are dense.
- PIM-DM assumes that in each subnet of the network there is at least one receiver interested in the multicast source.
- Multicast packets are flooded to all the nodes in the network, and the related resources (such as bandwidth and the CPU of the router) are consumed at the same time.

In order to reduce the network resource consumption, PIM-DM prunes the branches that do not forward multicast data and keeps only the branches containing receivers. In order that the pruned branches that are demanded to forward multicast data can receive multicast data flows again, the pruned braches can be restored to the forwarding status periodically.

In order to reduce the delay time for a pruned branch to be restored to the forwarding status, PIM-DM uses the graft mechanism to restore the multicast packet forwarding automatically. Such periodical floods and prunes are the features of PIM-DM, which is suitable for small LANs only. The "flood-prune” technology adopted in PIM-DM is unacceptable in WAN.

Generally, the packet forwarding path in PIM-DM is a shortest path tree (SPT) with the multicast source as the root and multicast members as the leaves. The SPT uses the shortest path from the multicast source to the receiver.

7.1.2 Work Mechanism of PIM-DM

The working procedure of PIM-DM is summarized as follows:

- Neighbor discovery
- SPT establishing
- Graft
- RPF check
- Assert mechanism

I. Neighbor discovery

In a PIM-DM network, a multicast router needs to use Hello messages to perform neighbor discovery and maintain the neighbor relation when it is started. All routers keep in touch with each other by sending Hello messages periodically, and thus SPT is established and maintained.

II. SPT establishment

The procedure of establishing SPT is also called Flooding & Prune.

The procedure is as follows:

- PIM-DM assumes that all hosts on the network are ready to receive multicast data.
- When a multicast router receives a multicast packet sent from a multicast source "S" to a multicast group "G", it begins with an RPF check according to the unicast routing table.
- If the RPF check passes, the router will create an entry (S, G) and forward the packet to all the downstream PIM-DM nodes. This process is known as flooding.
- If the RPF check fails, the router considers that the multicast packets travel into the router through incorrect interfaces and just discards the packets.

After this process is complete, the router creates a (S, G) entry for every host in the PIM-DM domain.

If there is no multicast group member in downstream nodes, the router sends a prune message to upstream nodes to inform them not to forward data any more. The upstream nodes, as informed, remove the related interface from the outgoing interface list corresponding to the multicast forwarding entry (S, G). The pruning process continues until there are only necessary branches in PIM-DM. In this way, an SPT (Shortest Path Tree) rooted at source S is established.

The pruning process is initiated by leaf routers. As shown in Figure 7-1, the routers without receivers (such as the router connected to User A) initiate the pruning process automatically.

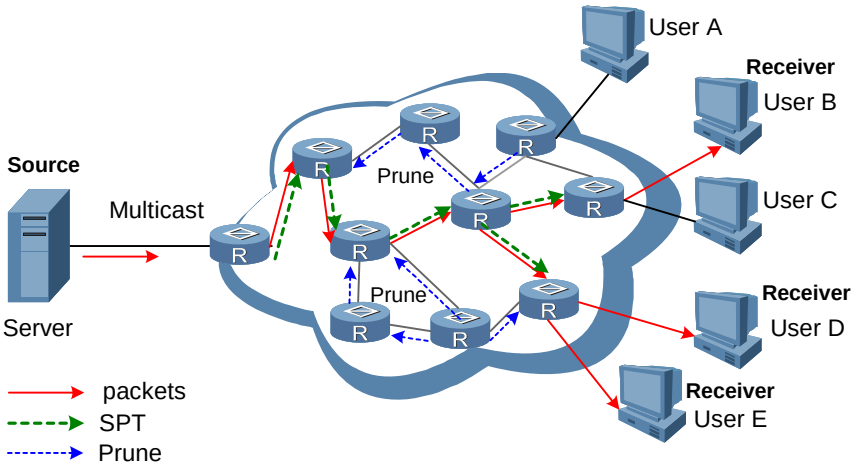


Figure 7-1 Diagram for SPT establishment in PIM-DM

The above-mentioned process is called "Flooding and Pruning". Every pruned node also provides a timeout mechanism. When pruning times out, the router initiates another flooding and pruning process. This process is performed periodically for PIM-DM.

III. Graft

When a pruned downstream node needs to be restored to the forwarding state, it may send a graft packet to inform the upstream node. As shown in Figure 7-1, user A receives multicast data again. Graft messages will be sent hop by hop to the multicast source S. The intermediate nodes return acknowledgements upon receiving Graft messages. Thus, the pruned branches are restored to the information transmission state.

IV. RPF check

PIM-DM adopts the RPF check mechanism to establish a multicast forwarding tree from the data source S based on the existing unicast routing table, static multicast routing table, and MBGP routing table.

The procedure is as follows:

- When a multicast packet arrives, the router first checks the path.
- If the interface this packet reaches is the one along the unicast route towards the multicast source, the path is considered correct.
- Otherwise, the multicast packet will be discarded as a redundant one.

The unicast routing information on which path judgment is based can be of any unicast routing protocol such as RIP or OSPF. It is independent of the specified unicast routing protocol.

V. Assert mechanism

In a shared network such as Ethernet, the same packets may be sent repeatedly. For example, the LAN network segment contains multiple multicast routers, A, B, C, and D. They each have their own receiving path to the multicast source S, as shown in Figure 7-2:

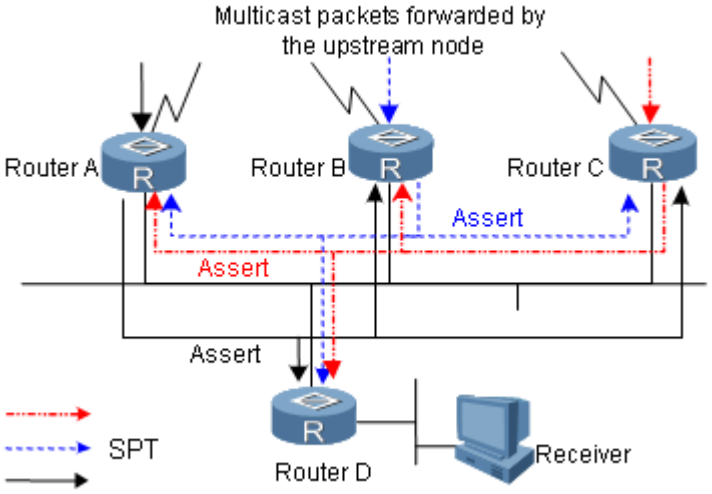


Figure 7-2 Diagram for assert mechanism

When Router A, Router B, and Router C receive a multicast packet sent from the multicast source S, they will all forward the multicast packet to the Ethernet. In this case, the downstream node Router D will receive three copies of the same multicast packet.

In order to avoid such cases, the Assert mechanism is needed to select one forwarder. Routers in the network select the best path by sending Assert packets. If two or more paths have the same priority and metric to the multicast source, the router with the highest IP address will be the upstream neighbor of the (S, G) entry, which is responsible for forwarding the (S, G) multicast packets. The unselected routers will prune the corresponding interfaces to disable the information forwarding.

7.1.3 Introduction to PIM-SM

Protocol independent multicast sparse mode (PIM-SM) is a sparse mode multicast protocol. It is generally used in the following occasions where:

- Group members are sparsely distributed
- The range is wide
- Large scaled networks exist

In PIM-SM, no host receives multicast packets by default. Multicast packets are forwarded to the hosts that need multicast packets explicitly.

In order that the receiver can receive the multicast data streams of the specific IGMP group, PIM-SM adopts rendezvous points (RP) to forward multicast information to all PIM-SM routers with receivers. RP is adopted in multicast forwarding. As a result, the network bandwidth that the data packets and control packets occupy is reduced, and the processing overhead of the router is also reduced.

At the receiving end, the router connected to the information receiver sends Join messages to the RP corresponding to the multicast group. The Join message reaches the root (namely, RP) after passing each router. The passed paths become the branches of the rendezvous point tree (RPT).

If the sending end wants to send data to a multicast group, the first hop router will send registration information to RP. When the registration information reaches RP, the source tree establishment is triggered. Then, the multicast source sends the data to RP. When the data reaches RP, the multicast packets are replicated and sent to the receiver along the RPT. Replication happens only where the tree branches. The procedure is repeated automatically until the multicast packets reach the receiver.

PIM-SM does not reply on any specific unicast routing protocol. Instead, it performs RPF check based on the existing unicast routing table.

7.1.4 Work Mechanism of PIM-SM

The working procedure of PIM-SM is:

- Neighbor discovery
- DR election
- RP discovery
- RPT shared tree building
- Multicast source registration
- Switching RPT to SPT

I. Neighbor discovery

The neighbor discovery mechanism is the same as described in PIM-DM. It is also implemented through Hello messages sent between each router.

II. DR election

With the help of Hello messages, DR can be elected for the shared network, such as Ethernet. DR will be the unique multicast information forwarder in the network. In either the network connected to the multicast source S or the network connected to the receiver, DR must be elected as long as the network is a shared network. The DR at the receiving end sends Join messages to RP and the DR at the multicast source side sends Register messages to RP, as shown in Figure 7-3:

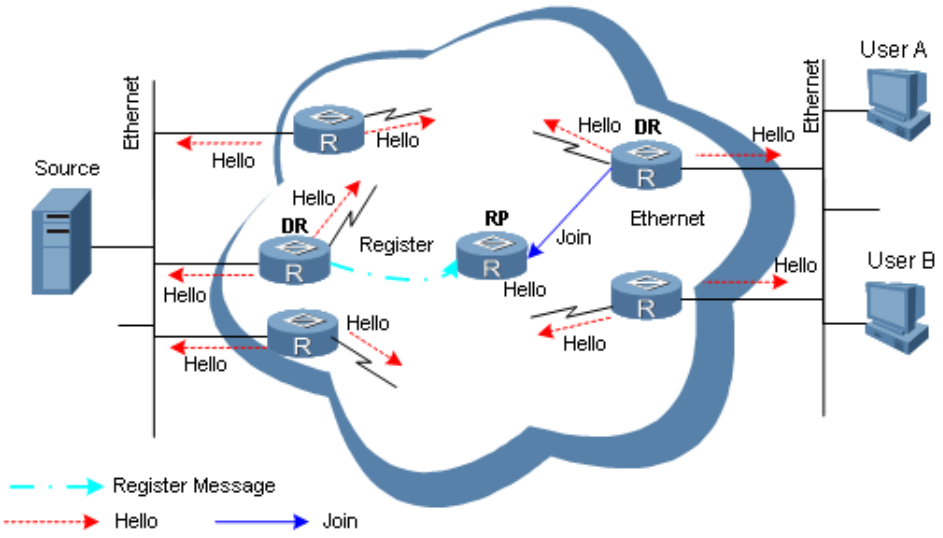


Figure 7-3 Diagram for DR election

Each router on the shared network sends Hello messages with the DR priority option to each other. The router with the highest DR priority is elected as the DR in the network. If the priority is the same, the router with the highest IP address is elected as the DR. When DR fails, the received Hello messages will time out. A new DR election procedure will be triggered among neighboring routers.

Note:

- S3600 Series Ethernet Switches do not support DR priority. In a network containing S3600 Series Ethernet Switches, the DR is elected by IP addresses.
- In a PIM-SM network, DR mainly serves as the querier of IGMPv1.

III. RP discovery

RP is the core router in a PIM-SM domain. The shared tree established based on the multicast routing information is rooted in RP. There is a mapping relationship between the multicast group and RP. One multicast group is mapped to one RP, and multiple multicast groups can be mapped to the same RP.

In a small and simple network, there is only little multicast information. One RP is enough for information forwarding. In this case, you can statically specify the position of RP in each router in the SM domain.

However, a PIM-SM network is normally of very large scale and RP forwards a lot of multicast information. In order to reduce the workload of RP and optimize the topology of the shared tree, different multicast groups must have different RPs. In this case, RP

must be elected dynamically through the auto-election mechanism and BootStrap router (BSR) must be configured.

BSR is the core management device in a PIM-SM network. It is responsible for:

- Collecting the Advertisement messages sent by the Candidate-RP (C-RP) in the network.
- Selecting part of the C-RP information to form the RP-set, namely, the mapping database between the multicast group and RP.
- Advertising the RP-set to the whole network so that all the routers (including DR) in the network know the position of RP.

One or more candidate BSRs must be configured in a PIM domain. Through auto-election, the candidate BSRs elect a BSR that is responsible for collecting and advertising RP information. The auto-election among candidate BSRs is described in the following section:

- Specify a PIM-SM-enabled interface when configuring a router as a candidate BSR.
- Initially, each candidate BSR considers itself as the BSR of the PIM-SM and uses the IP address of the specified interface as the BSR address to send Bootstrap messages.
- When the candidate BSR receives Bootstrap messages from other routers, it compares the BSR address in the received Bootstrap message with its own BSR address by priority and IP address. If the priority is the same, the candidate BSR with a higher IP address is considered to be better. If the former is better, the candidate BSR replaces its own BSR address with the new BSR address and does not consider itself as BSR any more. Otherwise, the candidate BSR keeps its own BSR address and continues to consider itself as BSR.

Figure 7-4 shows the positions of RPs and BSRs in the network:

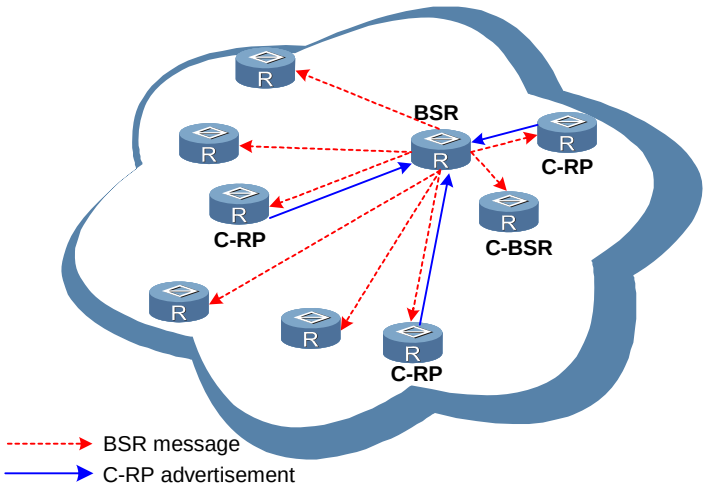


Figure 7-4 Diagram for the communication between RPs and BSRs

Only one BSR can be elected in a network or management domain, while multiple candidate BSRs (C-BSRs) can be configured. In this case, once the BSR fails, other C-BSRs can elect a new BSR through auto-election. Thus, service interruption is avoided.

In the same way, multiple C-RPs can be configured in a PIM-SM domain, and the RP corresponding to each multicast group is worked out through the BSR mechanism.

IV. RPT building

Assume the receiver hosts are User B, User D, and User E. When a receiver host joins a multicast group G, it sends IGMP packets to inform the leaf router directly connected to the host. Thus, the leaf router acquires the receiver information of the multicast group G, and then the leaf router sends Join messages to the upper-layer nodes in the direction of RP, as shown in Figure 7-5:

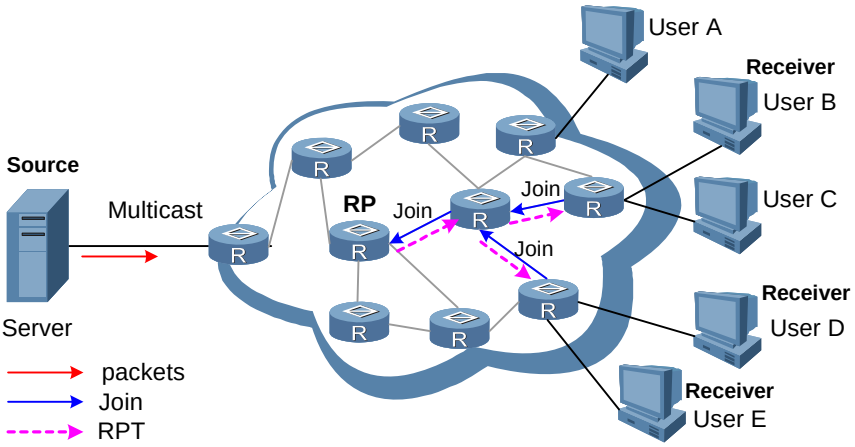


Figure 7-5 Diagram for RPT building in PIM-SM

Each router on the path from the leaf router to RP generate (*, G) entries in the forwarding table. The routers on the path form a branch of RPT. A (*, G) entry represents the information from any source to the multicast group G. RP is the root of RPT and the receivers are leaves of RPT.

When the packet from the multicast source S to the multicast group G passes by RP, the packet reaches the leaf router and receiver host along the established path in RPT.

When the receiver is not interested in the multicast information any more, the multicast router nearest the receiver will send Prune messages to RP hop by hop in the direction reverse to RPT. When the first upstream router receives the Prune message, it deletes the links with the downstream routers from the interface list and check whether it has any receiver interested in the multicast information. If not, the upstream router continues to forward the Prune message to upstream routers.

V. Multicast source registration

In order to inform RP about the existence of multicast source S, when multicast source S sends a multicast packet to the multicast group G, the router directly connected to S will encapsulate the received packet into a Register packet and send it to the corresponding RP through unicast, as shown in Figure 7-6:

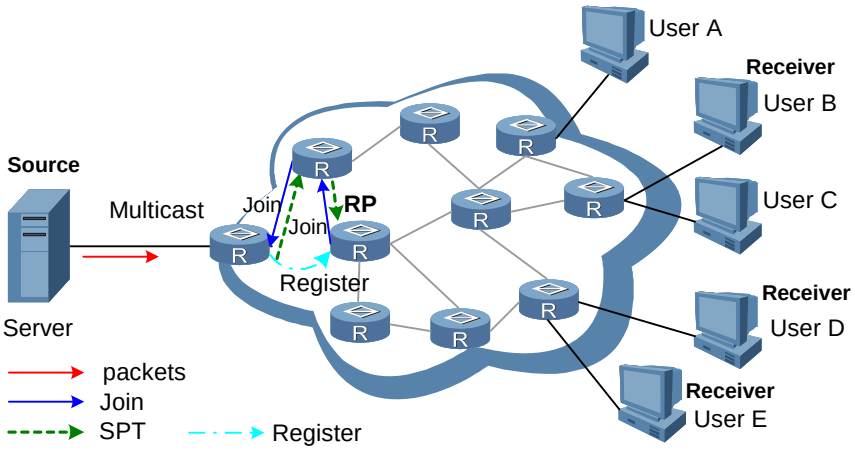


Figure 7-6 Diagram for SPT building in PIM-SM

When RP receives the registration information from S, it decapsulates the Register message and forwards the multicast information to the receiver along RPT, and on the other hand, it sends (S, G) Join messages to S hop by hop. The passed routers form a branch of SPT. The multicast source S is the root of SPT and RP is the destination of RP.

The multicast information sent by the multicast source S reaches RP along the built SPT, and then RP forwards the multicast information along the built RPT.

VI. Switching from RPT to SPT

When the multicast router nearest the receiver detects that the rate of the multicast packet from RP to the multicast group G exceeds the threshold value, it sends (S, G) Join messages to the upper-layer router of the multicast source S. The Join message reaches the router nearest the multicast source (namely, the first hop router) hop by hop and all the passed routers have the (S, G) entry. As a result, a branch of SPT is built.

Then, the last hop router sends a Prune message with the RP bit to RP hop by hop. When RP receives the message, it reversely forwards the Prune message to the multicast source. Thus, the multicast information stream is switched from RPT to SPT.

After the switching from RPT to SPT, the multicast information is sent from the multicast source S to the receiver directly. Through the switching from RPT to SPT, PIM-SM can build SPT in a more economical way than PIM-DM.

7.2 Common PIM Configuration

You can configure the PIM feature of the switch in interface view. The configuration includes:

Table 7-1 Configuration tasks

Operation	Description	Related section
Enable PIM-DM (PIM-SM) on the interface	Required	Section 7.2.1 "Enabling PIM-DM (PIM-SM) on the Interface"
Configure the interval of sending Hello packets	Optional	Section 7.2.2 "Configuring the Interval of Sending Hello
Configure PIM neighbors	Optional	Section 7.2.3 "Configuring PIM Neighbors"
Clear the related PIM entries	Optional	Section 7.2.4 "Clearing the Related PIM Entries"

7.2.1 Enabling PIM-DM (PIM-SM) on the Interface

Table 7-2 Enable PIM-DM (PIM-SM) on the interface

Operation	Command	Description
Enter system view	**system-view**	—
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	—
Enable PIM-DM/PIM-SM on the current interface	**pim dm / pim sm**	Optional Configure the PIM protocol type on the interface

7.2.2 Configuring the Interval of Sending Hello Packets

PIM-DM must be enabled on each interface. After the configuration, PIM-DM sends PIM Hello packets periodically and processes protocol packets that PIM neighbors send.

Table 7-3 Configure the interval of sending Hello packets

Operation	Command	Description
Enter system view	**system-view**	—
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	—
Enable PIM-DM/PIM-SM on the current interface	**pim dm / pim sm**	Required Configure the PIM protocol type on the interface.
Configure the interval of sending Hello packets on the interface	**pim timer hello** *seconds*	Required The interval of sending Hello packets is 30 seconds.

Caution:

- When PIM-DM is enabled on an interface, PIM-SM cannot be enabled on the interface any more, and vice versa.
- When PIM-DM is enabled on an interface of the switch, only PIM-DM can be enabled on the other interfaces of the switch, and vice versa.

7.2.3 Configuring PIM Neighbors

In order to prevent plenty of PIM neighbors from exhausting the memory of the router, which may result in router failure, you can limit the number of PIM neighbors on the router interface. However, the total number of PIM neighbors of a router is defined by the system, and you cannot modify it through commands.

You can configure basic ACL 2000 to 2999 (refer to the part about ACL in this manual). Only the filtered Layer 3 switches (routers) can serve as the PIM neighbors of the current interface.

Table 7-4 Configure PIM neighbors

Operation	Command	Description
Enter system view	**system-view**	—
Enable the multicast routing protocol	**multicast routing-enable**	Required

Operation	Command	Description
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	—
Enable PIM-DM/PIM-SM on the current interface	**pim dm / pim sm**	Required Configure the PIM protocol type on the interface
Configure a limit on the number of PIM neighbors on the interface	**pim neighbor-limit** *limit*	Optional By default, the upper limit on the number of PIM neighbors on a interface is 128
Configure the filtering policy for PIM neighbors	**pim neighbor-policy** *acl-number*	Optional • You can configure to filter the IP addresses of some multicast groups in ACL. • By default, the filtering policy for neighbors cannot be enabled on an interface.

Caution:

If the number of existing PIM neighbors exceeds the user-defined limit, the existing PIM neighbors will not be deleted.

7.2.4 Clearing the Related PIM Entries

You can execute the **reset** command in user view to clear the related statistics about multicast PIM.

Table 7-5 Clear the related PIM entries

Operation	Command	Description
Clear PIM route entries	**reset pim routing-table** { **all** | { *group-address* [**mask** *group-mask* | **mask-length** *group-mask-length*] | *source-address* [**mask** *source-mask* | **mask-length** *source-mask-length*] | { **incoming-interface** { *interface-type interface-number* | **null** } } } * }	Perform the configuration in user view.

Operation	Command	Description
Clear PIM neighbors	**reset pim neighbor** { **all** | { *neighbor-address* | **interface** *interface-type interface-number* } * }	Perform the configuration in user view.

7.3 PIM-DM Configuration

Perform the following configuration to configure PIM-DM. When the router runs in a PIM-DM domain, you are recommended to enable PIM-DM on all the interfaces of non-boarder routers.

7.3.1 Configuring Filtering Policies for Multicast Source/Group

Table 7-6 Configure filtering policies for multicast source/group

Operation	Command	Description
Enter system view	**system-view**	—
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter PIM view	**pim**	—
Perform source/group filter on the received multicast packets	**source-policy** *acl-number*	Optional You can configure to filter the IP addresses of some multicast groups in ACL.

Caution:

- If you configure basic ACLs, the source address match is performed on all the received multicast packets. The packets failing to match are discarded.
- If you configure advanced ACLs, the source address and group address match is performed on all the received multicast packets. The packets failing to match are discarded.

7.4 PIM-SM Configuration

PIM-SM configuration includes:

Table 7-7 Configuration tasks

Operation	Description	Section
Configure filtering policies for multicast sources/groups	Optional	Section 7.4.1 "Configuring Filtering Policies for Multicast Source/Group"
Configure BSR/RP	Optional	Section 7.4.2 "Configuring BSR/RP"
Configure PIM-SM domain boundary	Optional	Section 7.4.3 "Configuring PIM-SM Domain Boundary"
Filter the registration packets from RP to DR	Optional	Section 7.4.4 "Filtering the Registration Packets from RP to DR"

7.4.1 Configuring Filtering Policies for Multicast Source/Group

For the configuration of filtering policies for multicast source/group, refer to section 7.3.1 "Configuring Filtering Policies for Multicast Source/Group".

7.4.2 Configuring BSR/RP

Table 7-8 Configure BSR/RP

Operation	Command	Description
Enter system view	**system-view**	—
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter PIM view	**pim**	—
Configure candidate BSRs	**c-bsr** *interface-type interface-number hash-mask-len* [*priority*]	Optional By default, candidate BSRs are not set for the switch and the value of priority is 0.
Configure candidate RPs	**c-rp** *interface-type interface-number* [**group-policy** *acl-number* | **priority** *priority*]*	Optional • You can configure to filter the IP addresses of some multicast groups in ACL. • By default, candidate RPs are not set for the switch and the value of priority is 0.

Operation	Command	Description
Configure static RPs	**static-rp** *rp-address* [*acl-number*]	Optional • You can configure to filter the IP addresses of some multicast groups in ACL. • By default, static RPs are not set for the switch.
Limit the range of valid BSRs	**bsr-policy** *acl-number*	Optional • You can configure to filter the IP addresses of some multicast groups in ACL. • By default, the range of valid BSRs is not set for the switch.
Limit the range of valid C-RPs	**crp-policy** *acl-number*	Optional • You can configure to filter the IP addresses of some multicast groups in ACL. • By default, the range of valid C-RPs is not set for the switch.

Caution:

- Only one candidate BSR can be configured on a Layer 3 switch. The BSR configuration on another interface will replace the former configuration.
- You are recommended to configure both the candidate BSR and candidate RP on the Layer 3 switch in the backbone.
- If the range of multicast groups that RP serves is not specified when RP is configured, the RP serves all multicast groups. Otherwise, the RP serves the multicast groups within the specified range.
- You can configure basic ACLs to filter related multicast IP addresses and control the range of multicast groups that RP serves.
- If you use static RPs, all routers in the PIM domain must adopt the same configuration.
- If the configured static RP address is the address of an UP interface on the local switch, the switch will serve as RP.
- Static RPs do not take effect when the RP generated by the BSR mechanism takes effect.
- The PIM protocol does not need to be enabled on the interface of static RPs.
- The limit on the range of valid BSRs is to prevent the valid BSRs in the network from being replaced maliciously. The other BSR information except the range will not be received by the Layer 3 switch, and thus the security of BSRs in the network is protected.
- The limit on the range of C-RPs is to avoid C-RP cheating. You can limit the range of valid C-RPs and limit the range of multicast groups that each C-RP serves.

7.4.3 Configuring PIM-SM Domain Boundary

Table 7-9 Configure PIM-SM domain boundary

Operation	Command	Description
Enter system view	**system-view**	—
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	—
Enable PIM-SM on the current interface	**pim sm**	Required Configure the PIM protocol type on the interface.

Operation	Command	Description
Configure PIM-SM domain boundary	**pim bsr-boundary**	Required By default, domain boundary is not set for the switch.

Caution:

- After the PIM-SM domain boundary is set, Bootstrap messages cannot pass the boundary in any direction. In this way, PIM-SM domains are divided.
- After this feature is configured, Bootstrap messages cannot pass the boundary. However, the other PIM messages can pass the domain boundary. The network can be effectively divided into domains that use different BSRs.

7.4.4 Filtering the Registration Packets from RP to DR

Through the registration packet filtering mechanism in a PIM-SM network, you can determine which sources send packets to which groups on RP, that is, RP can filter the registration packets sent from DR and receive the specified packets only.

Table 7-10 Filter the registration packets from RP to DR

Operation	Command	Description
Enter system view	**system-view**	—
Enable the multicast routing protocol	**multicast routing-enable**	Required Enable the multicast routing protocol
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	—
Enable PIM-SM on the current interface	**pim sm**	Required Configure the PIM protocol type on the interface
Quit VLAN view	**quit**	—
Enter PIM view	**pim**	—

Operation	Command	Description
Configure to filter the registration packets from RP to DR	**register-policy** *acl-number*	Required • You can configure to filter the IP addresses of some multicast groups in ACL. • By default, the switch does not filter the registration packets from DR.

Caution:

- If a source group entry (S, G) is denied in ACL, or no operation on the entry is defined in the ACL, or ACLs are not defined, RP will send RegisterStop messages to DR to stop the registration process of the multicast data flow.
- Only the registration packets matching the **permit** command of ACLs can be accepted. When an invalid ACL is defined, RP will reject all the registration packets.

7.4.5 Configuring the Threshold for Switching from RPT to SPT

PIM-SM routers initially use the RPT to forward multicast packets. If the threshold is specified as 0, the last hop switch that the packets pass initiates the switching from the RPT to the SPT.

Table 7-11 Configure the threshold for switching from RPT to SPT

Operation	Command	Description
Enter system view	**system-view**	—
Enter PIM view	**pim**	—
Configure the threshold for switching from RPT to SPT	**spt-switch-threshold** { *traffic-rate* | **infinity** } [**group-policy** *acl-number*]	Required By default, a RPT-to-SPT switch occurs once the device receives the first multicast packet from the RPT.

Note:

When you execute the **spt-switch-threshold** command on an S3600 Ethernet switch, the *traffic-rate* argument can only be set to 0. That is, the threshold can be set to 0 or **infinity**.

- With the threshold set to 0, the last hop switch switches to SPT once it receives the first multicast packet.
- With the threshold set to **infinity**, the last hop switch never switches to SPT.

7.5 Displaying and Debugging PIM

After completing the above-mentioned configurations, you can execute the **display** command in any view to verify the configuration by checking the displayed information.

Table 7-12 Display and maintain PIM

Configuration	Command	Description
Display PIM multicast routing tables	**display pim routing-table** [{ { ***g** [*group-address* [**mask** { *mask-length* | *mask* }]] | ****rp** [*rp-address* [**mask** { *mask-length* | *mask* }]] } | { *group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] } ***** } | **incoming-interface** { *interface-type interface-number* | **null** } | { **dense-mode** | **sparse-mode** }] *****	You can execute the **display** command in any view.
Display the information about PIM interfaces	**display pim interface** [*interface-type interface-number*]	
Display the information about PIM neighbor routers	**display pim neighbor** [**interface** *interface-type interface-number*]	
Display BSR information	**display pim bsr-info**	
Display RP information	**display pim rp-info** [*group-address*]	

7.6 PIM Configuration Example

7.6.1 PIM-DM Configuration Example

I. Network requirements

Lanswitch1 is connected to Multicast Source through VLAN-interface10, to Lanswitch2 through VLAN-interface11 and to Lanswitch3 through VLAN-interface12. Through PIM-DM, multicast is implemented among Receiver 1, Receiver 2, and Multicast Source.

II. Network diagram

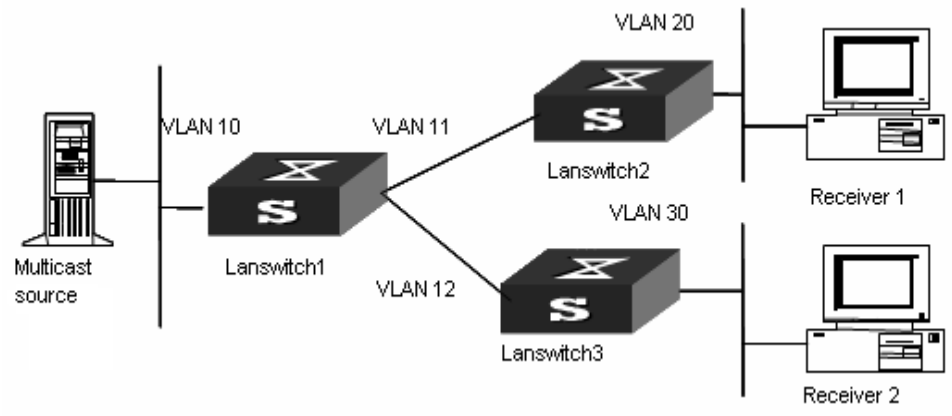


Figure 7-7 Network diagram for PIM-DM configuration

III. Configuration procedure

1) Configure Lanswitch1.

Enable multicast routing protocol.

```
<H3C> system-view
[H3C] multicast routing-enable
```

Enable IGMP and PIM-DM on the interfaces.

```
[H3C] vlan 10
[H3C-vlan10] port Ethernet 1/0/2 to Ethernet 1/0/3
[H3C-vlan10] quit
[H3C] vlan 11
[H3C-vlan11] port Ethernet 1/0/4 to Ethernet 1/0/5
[H3C-vlan11] quit
[H3C] vlan 12
[H3C-vlan12] port Ethernet 1/0/6 to Ethernet 1/0/7
[H3C-vlan12] quit
[H3C] interface Vlan-interface 10
[H3C-Vlan-interface10] ip address 1.1.1.1 255.255.0.0
```

```
[H3C-Vlan-interface10] pim dm
[H3C-Vlan-interface10] quit
[H3C] interface Vlan-interface 11
[H3C-Vlan-interface11] ip address 2.2.2.2 255.255.0.0
[H3C-Vlan-interface11] pim dm
[H3C-Vlan-interface11] quit
[H3C] interface Vlan-interface 12
[H3C-Vlan-interface12] ip address 3.3.3.3 255.255.0.0
[H3C-Vlan-interface12] pim dm
```

2) Configure Lanswitch2.

Enable multicast routing protocol.

```
<H3C> system-view
[H3C] multicast routing-enable
```

Enable IGMP and PIM-DM on the ports.

```
[H3C] vlan 20
[H3C-vlan20] port Ethernet 1/0/2 to Ethernet 1/0/3
[H3C-vlan20] quit
[H3C] vlan 11
[H3C-vlan11] port Ethernet 1/0/4 to Ethernet 1/0/5
[H3C-vlan11] quit
[H3C] interface Vlan-interface 20
[H3C-Vlan-interface20] ip address 6.6.6.6 255.255.0.0
[H3C-Vlan-interface20] igmp enable
[H3C-Vlan-interface20] pim dm
[H3C-Vlan-interface20] quit
[H3C] interface Vlan-interface 11
[H3C-Vlan-interface11] ip address 4.4.4.4 255.255.0.0
[H3C-Vlan-interface11] pim dm
```

3) The configuration for Lanswitch3is similar to that of Lanswitch2 and is thus omitted.

7.6.2 PIM-SM Configuration Example

I. Network requirements

All Ethernet switches are reachable to each other in the practical network.

- LS_A is connected to LS_B through VLAN-interface10, to Host A through VLAN-interface11 and to LS_C through VLAN-interface12.
- LS_B is connected to LS_A through VLAN-interface10, to LS_C through VLAN-interface11 and to LS_D through VLAN-interface12.
- LS_C is connected to Host B through VLAN-interface10, to LS_B through VLAN-interface11 and to LS_A through VLAN-interface12.

Host A is the receiver of the multicast group whose multicast IP address is 225.0.0.1. Host B begins to send data to the destination 225.0.0.1 and LS_A receives the multicast data from Host B through LS_B.

II. Network diagram

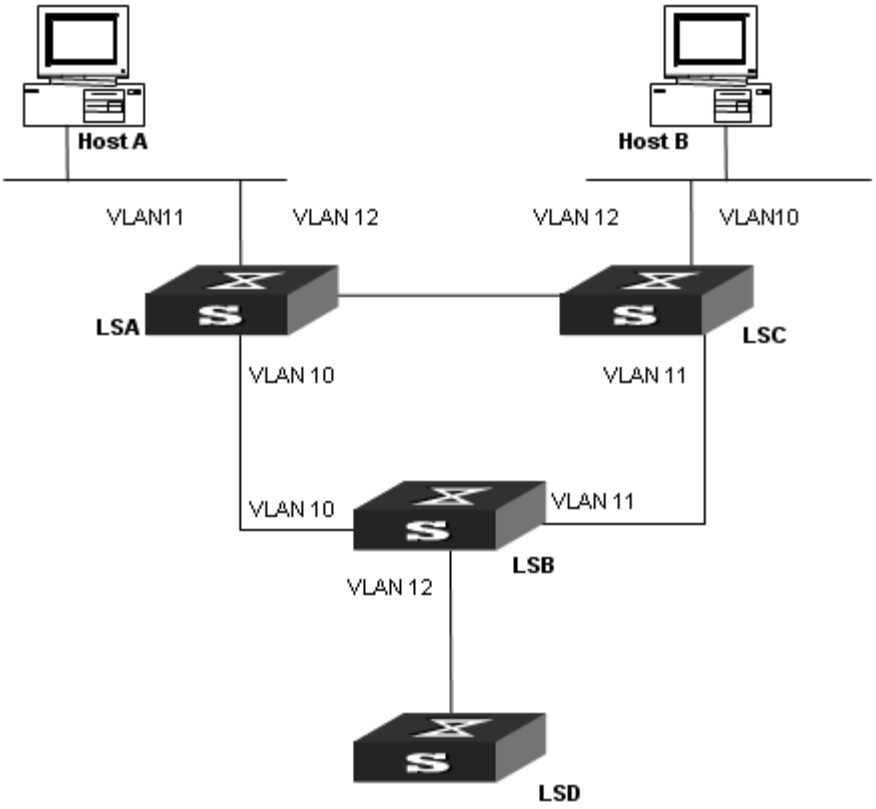


Figure 7-8 Network diagram for PIM-SM configuration

III. Configuration procedure

1) Configure LS_A.

Enable PIM-SM.

```
<H3C> system-view
[H3C] multicast routing-enable
[H3C] vlan 10
[H3C-vlan10] port Ethernet 1/0/2 to Ethernet 1/0/3
[H3C-vlan10] quit
[H3C] interface Vlan-interface 10
[H3C-Vlan-interface10] pim sm
[H3C-Vlan-interface10] quit
[H3C] vlan 11
[H3C-vlan11] port Ethernet 1/0/4 to Ethernet 1/0/5
[H3C-vlan11] quit
```

```
[H3C] interface Vlan-interface 11
[H3C-Vlan-interface11] igmp enable
[H3C-Vlan-interface11] pim sm
[H3C-Vlan-interface11] quit
[H3C] vlan 12
[H3C-vlan12] port Ethernet 1/0/6 to Ethernet 1/0/7
[H3C-vlan12] quit
[H3C] interface Vlan-interface 12
[H3C-Vlan-interface12] pim sm
[H3C-Vlan-interface12] quit
```

2) Configure LS_B.

Enable PIM-SM.

```
<H3C> system-view
[H3C] multicast routing-enable
[H3C] vlan 10
[H3C-vlan10] port Ethernet 1/0/2 to Ethernet 1/0/3
[H3C-vlan10] quit
[H3C] interface Vlan-interface 10
[H3C-Vlan-interface10] pim sm
[H3C-Vlan-interface10] quit
[H3C] vlan 11
[H3C-vlan11] port Ethernet 1/0/4 to Ethernet 1/0/5
[H3C-vlan11] quit
[H3C] interface Vlan-interface 11
[H3C-Vlan-interface11] igmp enable
[H3C-Vlan-interface11] pim sm
[H3C-Vlan-interface11] quit
[H3C] vlan 12
[H3C-vlan12] port Ethernet 1/0/6 to Ethernet 1/0/7
[H3C-vlan12] quit
[H3C] interface Vlan-interface 12
[H3C-Vlan-interface12] pim sm
[H3C-Vlan-interface12] quit
```

Configure candidate BSRs.

```
[H3C] pim
[H3C-pim] c-bsr Vlan-interface 10 30 2
```

Configure candidate RPs.

```
[H3C] acl number 2000
[H3C-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255
[H3C] pim
[H3C-pim] c-rp Vlan-interface 10 group-policy 2000
```

```
[H3C-pim] quit
```

Configure PIM domain boundary

```
[H3C] interface Vlan-interface 12
[H3C-Vlan-interface12] pim bsr-boundary
```

After VLAN-interface 12 is configured as the PIM domain boundary, LS_D cannot receive BSR information from LS_B any more; that is, LS_D is excluded from the PIM domain.

3) Configure LS_C.

Enable PIM-SM.

```
<H3C> system-view
[H3C] multicast routing-enable
[H3C] vlan 10
[H3C-vlan10] port Ethernet 1/0/2 to Ethernet 1/0/3
[H3C-vlan10] quit
[H3C] interface Vlan-interface 10
[H3C-Vlan-interface10] pim sm
[H3C-Vlan-interface10] quit
[H3C] vlan 11
[H3C-vlan11] port Ethernet 1/0/4 to Ethernet 1/0/5
[H3C-vlan11] quit
[H3C] interface Vlan-interface 11
[H3C-Vlan-interface11] pim sm
[H3C-Vlan-interface11] quit
[H3C] vlan 12
[H3C-vlan12] port Ethernet 1/0/6 to Ethernet 1/0/7
[H3C-vlan12] quit
[H3C] interface Vlan-interface 12
[H3C-Vlan-interface12] pim sm
[H3C-Vlan-interface12] quit
```

7.7 Troubleshooting PIM

Symptom: The router cannot set up multicast routing tables correctly.

Solution: You can troubleshoot PIM according to the following procedure.

Make sure that the unicast routing is correct before troubleshooting PIM.

- Because PIM-SM needs the support of RP and BSR, you must execute the **display pim bsr-info** command to see whether BSR information exists. If not, you must check whether there is any unicast route to the BSR. Then, use the **display pim rp-info** command to check whether the RP information is correct. If RP information does not exist, you must check whether there is any unicast route to RP.

- Use the **display pim neighbor** command to check whether the neighboring relationship is correctly established.

Chapter 8 MSDP Configuration

Note:

- Because multicast source discovery protocol (MSDP) does not support the IRF feature, MSDP cannot be configured in Fabric.
- Routers and router icons in this chapter represent routers in the common sense and Ethernet switches running routing protocols.

8.1 Overview

Internet service providers (ISP) are not willing to rely on devices of their competitors to forward multicast traffic. On the other hand, ISPs want to obtain information from information sources no matter where the information resources reside and forward the information to their own members. MSDP is designed to address this issue and used to discover multicast sources in other protocol independent multicast sparse mode (PIM-SM) domains. MSDP is only valid for the any-source multicast (ASM) model.

MSDP describes a mechanism of interconnecting multiple PIM-SM domains. It requires that the inter-domain multicast routing protocol must be PIM-SM and allows the rendezvous points (RPs) of different domains to share multicast source information.

I. MSDP peers

The RP in a PIM-SM domain can sense the existence of an active multicast source S, if any, in this domain through multicast source register messages. If a PIM-SM domain managed by another ISP wants to obtain information from this multicast source, the routers in both PIM-SM domains must establish an MSDP peering relationship with each other, as shown in Figure 8-1:

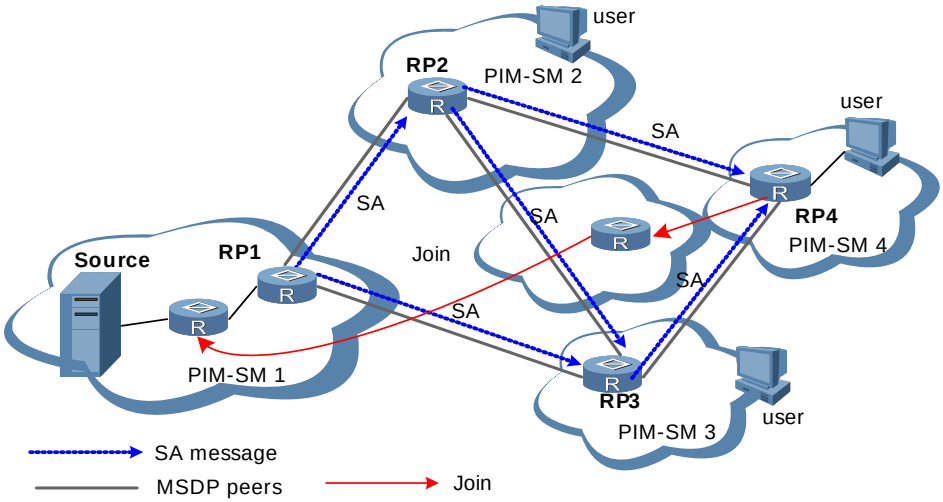


Figure 8-1 MSDP peering relationship

Note:

MSDP peers are interconnected over TCP connections (through port 639). A TCP connection can be established between RPs in different PIM-SM domains, between RPs in the same PIM-SM domain, between an RP and a common router, or between common routers. Figure 8-1 shows the MSDP peering relationship between RPs. Unless otherwise specified, examples in the following descriptions are based on MSDP peering relationship between RPs.

An active multicast source S exists in the PIM-SM1 domain. RP1 in this domain learns the specific location of the multicast source S through multicast source register messages, and then sends source active (SA) messages periodically to MSDP peers (RP nodes) in other PIM-SM domains. An SA message contains the IP address of the multicast source S, the multicast group address G, the address of the RP that has generated the SA message, and the first multicast data received by the RP in the PIM-SM1 domain. The SA message is forwarded by peers. Finally, the SA message reaches all the MSDP peers. In this way, the information of multicast source S in the PIM-SM domain is delivered to all PIM-SM domains.

By performing reverse path forwarding (RPF) check, MSDP peers accept SA messages only from the correct paths and forward the SA messages, thus avoiding SA message loop. In addition, you can configure a mesh group among MSDP peers to avoid SA flooding among MSDP peers.

Assume that RP4 in the PIM-SM4 domain receives the SA message. RP4 checks whether receivers exist in the corresponding multicast group. If yes, RP4 sends a (S, G) Join message hop by hop to the multicast source S, thus creating a shortest path tree

(SPT) based on the multicast source S. However, a rendezvous point tree (RPT) exists between RP4 and receivers in the PIM-SM4 domain.

Note:

Through MSDP, a PIM-SM domain receiving information from the multicast source S does not rely on RPs in other PIM-SM domains; that is, receivers can directly join the SPT based on the multicast source without passing RPs in other PIM-SM domains.

II. MSDP application

You can also implement Anycast RP through MSDP. Anycast RP refers to such an application that an MSDP peering relationship can be established between two RPs with the same IP address in the same PIM-SM domain, to enable load balancing and redundancy backup between the two RPs in the same domain. The candidate RP (C-RP) function is enabled on an interface (typically the loopback interface) of each of multiple routers in the same PIM-SM domain, and these interfaces have the same IP address. An MSDP peering relationship is formed among these interfaces, as shown in Figure 8-2.

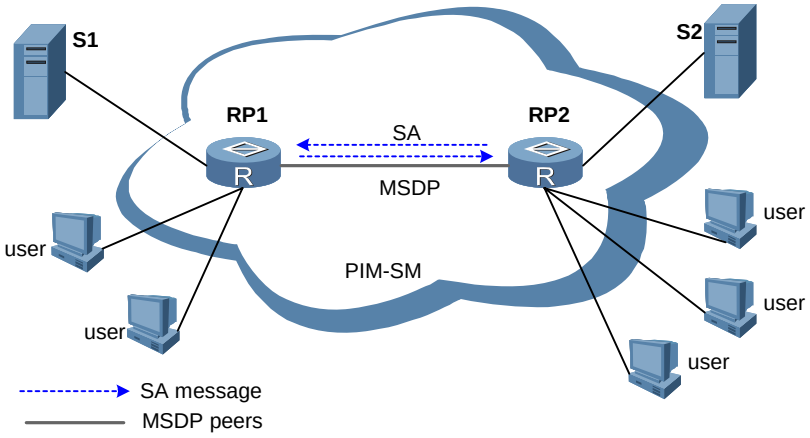


Figure 8-2 Typical networking of Anycast RP

Typically, a multicast source S registers with the nearest RP to create an SPT, and receivers also send Join messages to the nearest RP to construct an RPT. Therefore, it is likely that the RP with which the multicast source has registered is not the RP that receivers join. To ensure information consistency between RPs, the RPs, serving as MSDP peers of one another, learn information of the peer multicast source by sending SA messages to one another. As a result, each RP can know all the multicast sources in the PIM-SM domain. In this way, the receivers connected to each RP can receive multicast data sent by all the multicast sources in the entire PIM-SM domain.

As described above, RPs exchange information among one another through MSDP, a multicast source registers with the nearest RP, and receivers join the nearest RPT. In this way, RP load balancing can be achieved. When an RP fails, the multicast source and receivers previously registered to/joined it will register to or join another nearest RP automatically, thus implementing RP redundancy backup.

8.1.1 MSDP Working Mechanism

I. Identifying a multicast source and receiving multicast data

A network contains four PIM-SM domains, PIM-SM1, PIM-SM2, PIM-SM3, and PIM-SM4. An MSDP peering relationship is established between RPs in different domains. Multicast group members exist in the PIM-SM1 and PIM-SM4 domains. See Figure 8-3.

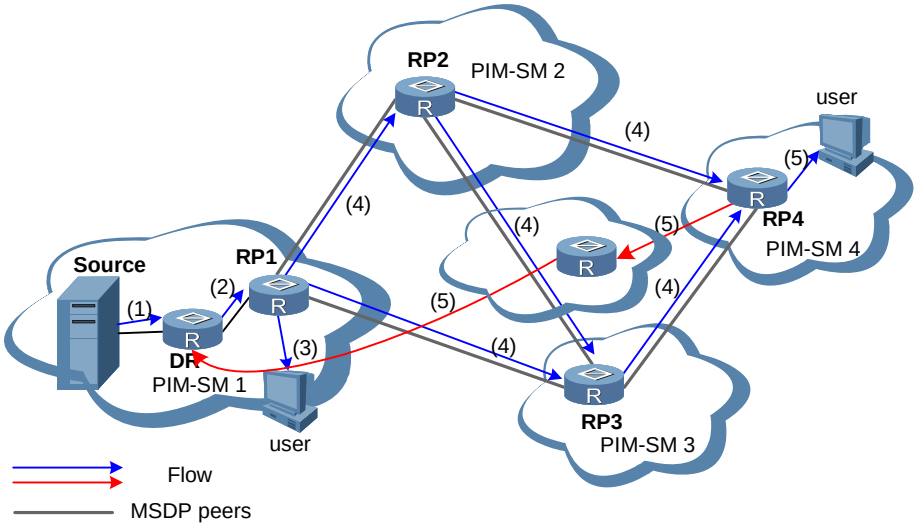


Figure 8-3 Identifying the multicast source and receiving multicast data

The complete interoperation process between a multicast source S in the PIM-SM1 domain and receivers in the PIM-SM1 and PIM-SM4 domains is as follows:

1) The multicast source S in the PIM-SM1 domain begins to send data packets.
2) The designated router (DR) connected to the multicast source S encapsulates the received data in a Register message, and then forwards the message to RP1 in the PIM-SM1 domain.
3) RP1 in the PIM-SM1 domain decapsulates the Register message, and then forwards the message to all the members in the domain along the RPT. The members in the domain can select whether to switch to the SPT.
4) At the same time, RP1 in the PIM-SM1 domain generates an SA message and sends the message to the corresponding MSDP peers (RPs in the PIM-SM2 and PIM-SM3 domains). Finally, the SA message is forwarded to the RP in the PIM-SM4 domain. The SA message contains the IP address of the multicast

source, the multicast group address, the address of the RP that has generated the SA message, and the first multicast data received by the RP in the PIM-SM1 domain.

5) If group members (namely, receivers) exist in the PIM-SM domains where MSDP peers of RP1 reside (for example, if group members exist in the PIM-SM4 domain), RP4 decapsulates the multicast data in the SA message and distributes the multicast data to receivers along the RPT. RP4 also sends a Join message to the multicast source S at the same time.

6) To avoid SA loop, MSDP peers perform RPF check on the received SA message. After the RPF path is established, the data from the multicast source S is directly sent to RP4 in the PIM-SM4 domain. Then, RP4 forwards the data along the RPT within the domain. Now, the last-hop router connected to group members in the PIM-SM4 domain selects whether to switch to the SPT.

II. Forwarding messages between MSDP peers and performing RPF check

To establish an MSDP peering relationship between routers, you have to create routes between routers for SA messages to travel.

Assume that three autonomous systems (ASs) exist. They are AS1, AS2, and AS3. Each AS has a PIM-SM domain associated with it. Each PIM-SM domain contains at least one RP. See Figure 8-4.

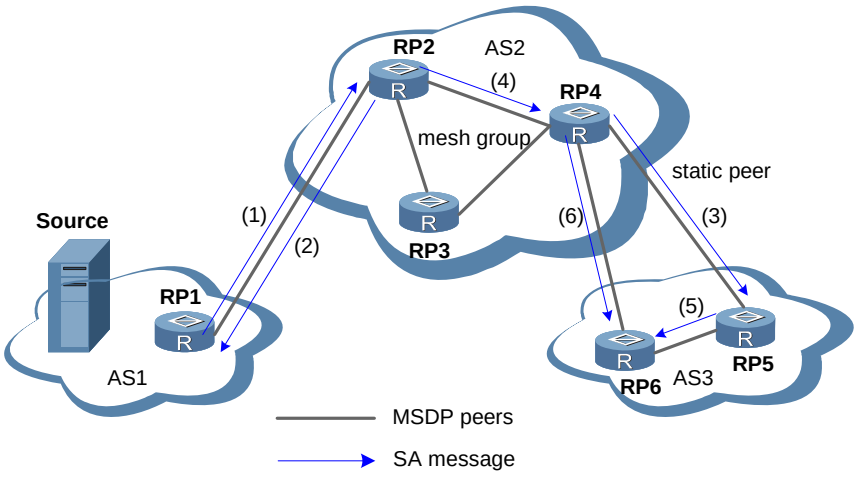


Figure 8-4 Forwarding SA messages between MSDP peers

As shown above, RP1 belongs to AS1. RP2, RP3 and RP4 belong to AS2. RP5 and RP6 belong to AS3. An MSDP peering relationship exists among these RPs. RP2, RP3, and RP4 form a mesh group. These MSDP peers perform RPF check and process SA messages forwarded to one another according to the following rules:

- If an MSDP peer sending an SA message is an RP in the PIM-SM domain where the multicast source resides (for example, when RP1 sends an SA message to

RP2), the receiver accepts the SA message and forwards the message to other peers.

- If an RP has only one MSDP peer (for example, when RP2 sends an SA message to RP1), the receiver accepts the SA message from the peer.
- If an SA message comes from a static RPF peer (for example, when RP4 sends an SA message to RP5), the receiver accepts the SA message and forwards it to other peers.
- If an SA message comes from a peer that belongs to the same MSDP mesh group with the receiver, the receiver accepts the SA message and forwards it to peers out of the mesh group. For example, when RP2 sends an SA message to RP4, RP4 accepts the message and forwards it to RP5 and RP6.
- If an SA message comes from an MSDP peer in the same AS, and this peer is the next hop on the optimal path to the RP in the PIM-SM domain where the multicast source resides, the receiver accepts the SA message and forwards it to other peers. For example, when RP4 sends an SA message to RP5, RP5 receives the message and forwards it to RP6.
- If an SA message comes from an MSDP peer in a different AS, and this AS is the next AS of the RP optimal path in the PIM-SM domain where the multicast source resides (for example, when RP4 sends an SA message to RP6), the receiver accepts the SA message and forwards it to other peers.
- The receiver does not accept or forward other SA messages.

Note:

S3600 series switches do not support inter-domain routing (BGP protocol); therefore, the fifth rule described above is adopted in RPF check.

8.2 Configuring MSDP Basic Functions

To enable exchange of information from the multicast source S between two PIM-SM domains, you need to establish MSDP peering relationships between RPs in these PIM-SM domains. In this way, the information from the multicast source can be sent through SA messages between the MSDP peers, and the receivers in other PIM-SM domains can finally receive the multicast source information.

A route is required between two routers that are MSDP peers to each other. Through this route, the two routers can transfer SA messages between PIM-SM domains. For an area containing only one MSDP peer, known as a stub area, the route is not compulsory. SA messages are transferred in a stub area through the configuration of static RPF peers. In addition, the use of static RPF peers can avoid RPF check on the received SA messages, thus saving resources.

Before configuring static RPF peers, you must create an MSDP peering connection. If you configure only one MSDP peer on a router, the MSDP peer will act as a static RPF peer. If you configure multiple RPF peers, you need to handle them by using different rules according to the configured policies.

When configuring multiple static RPF peers for the same router, you must follow the following two configuration methods:

- In the case that all the peers use the **rp-policy** keyword: Multiple static RPF peers function at the same time. RPs in SA messages are filtered based on the configured prefix list, and only the SA messages whose RP addresses pass the filtering are received. If multiple static RPF peers using the same **rp-policy** keyword are configured, when any of the peers receives an SA message, it will forward the SA message to other peers.
- None of the peers use the **rp-policy** keyword: Based on the configured sequence, only the first static RPF peer whose connection state is UP is active. All the SA messages from this peer will be received, while the SA messages from other static RPF peers will be discarded. Once the active static RPF peer fails (because the configuration is removed or the connection is terminated), based on the configuration sequence, the subsequent first static RPF peer whose connection is in the UP state will be selected as the active static RPF peer.

8.2.1 Configuration Prerequisites

Before configuring basic MSDP functions, you need to configure:

- A unicast routing protocol
- PIM-SM basic functions

8.2.2 Configuring MSDP Basic Functions

Table 8-1 Configure MSDP basic functions

Operation	Command	Description
Enter system view	**system-view**	—
Enable IP multicast routing	**multicast routing-enable**	Required
Enable MSDP function and enter MSDP view	**msdp**	Required

Operation	Command	Description
Create an MSDP peer connection	**peer** *peer-address* **connect-interface** *interface-type interface-number*	Required To establish an MSDP peer connection, you must configure the parameters on both peers. The peers are identified by an address pair (the address of the interface on the local router and the IP address of the remote MSDP peer).
Configure a static RPF peer	**static-rpf-peer** *peer-address* [**rp-policy** *ip-prefix-name*]	Optional For an area containing only one MSDP peer, if BGP or MBGP does not run in this area, you need to configure a static RPF peer.

8.3 Configuring Connection between MSDP Peers

An AS may contain multiple MSDP peers. To avoid SA flooding between the MSDP peers, you can use the MSDP mesh mechanism to improve traffic. When multiple MSDP peers are fully connected with one another, these MSDP peers form a mesh group. When an MSDP peer in the mesh group receives SA messages from outside the mesh group, it sends them to other members of the group. On the other hand, a mesh group member does not perform RPF check on SA messages from within the mesh group and does not forward the messages to other members of the mesh group. This avoids SA message flooding since it is unnecessary to run BGP or MBGP between MSDP peers, thus simplifying the RPF checking mechanism.

The sessions between MSDP peers can be terminated and reactivated sessions as required. When a session between MSDP peers is terminated, the TCP connection is closed, and there will be no reconnection attempts. However, the configuration information is kept.

8.3.1 Configuration Prerequisites

Before configuring an MSDP peer connection, you need to configure:

- A unicast routing protocol
- Basic functions of IP multicast
- PIM-SM basic functions
- MSDP basic functions

Table 8-2 Configuration tasks

Operation	Description	Related section
Configure description information for MSDP peers	Required	Section 8.3.2 "Configuring Description Information for MSDP Peers"
Configure Anycast RP application	Optional	Section 8.3.3 "Configuring Anycast RP Application"
Configure an MSDP mesh group	Optional	Section 8.3.4 "Configuring an MSDP Mesh Group"
Configure MSDP peer connection control	Optional	Section 8.3.5 "Configuring MSDP Peer Connection Control"

8.3.2 Configuring Description Information for MSDP Peers

You can configure description information for each MSDP peer to manage and memorize the MSDP peers.

Table 8-3 Configure description information for an MSDP peer

Operation	Command	Description
Enter system view	**system-view**	—
Enter MSDP view	**msdp**	—
Configure description information for an MSDP peer	**peer** *peer-address* **description** *text*	Optional The *peer-address* argument is the address of the peer. You can configure addresses of multiple peers for multiple times. By default, an MSDP peer has no description text.

8.3.3 Configuring Anycast RP Application

If you configure the same interface (usually Loopback interface) addresses on two RPs in the same PIM-SM domain, the two RPs will be MSDP peers to each other. To prevent failure of RPF check on SA messages between MSDP peers, you must configure the RP address to be carried in the SA messages.

Table 8-4 Configure Anycast RP application

Operation	Command	Description
Enter system view	**system-view**	—
Enter MSDP view	**msdp**	—

Operation	Command	Description
Create an MSDP peer connection	**peer** *peer-address* **connect-interface** *interface-type interface-number*	Required
Configure the RP address to be carried in SA messages	**originating-rp** *interface-type interface-number*	Required By default, the RP address in SA messages is the RP address configured by PIM.

Note:

In Anycast RP application, C-BSR and C-RP must be configured on different devices or ports.

8.3.4 Configuring an MSDP Mesh Group

Configure a mesh group name on all the peers that will become members of the MSDP mesh group so that the peers are fully connected with one another in the mesh group.

Table 8-5 Configure an MSDP mesh group

Operation	Command	Description
Enter system view	**system-view**	—
Enter MSDP view	**msdp**	—
Add an MSDP peer to a mesh group	**peer** *peer-address* **mesh-group** *name*	Required This command must be configured on all the peers; therefore, you need to configure this command for multiple times.

Note:

- Before you configure an MSDP mesh group, make sure that the routers are fully connected with one another.
- The same group name must be configured on all the peers.
- If you add the same MSDP peer to multiple mesh groups, only the latest configuration takes effect.

8.3.5 Configuring MSDP Peer Connection Control

The connection between MSDP peers can be flexibly controlled. You can disable the MSDP peering relationships temporarily by shutting down the MSDP peers. As a result, SA messages cannot be transmitted between these two peers. On the other hand, when resetting an MSDP peering relationship between faulty MSDP peers or bringing faulty MSDP peers back to work, you can adjust the retry interval of establishing a peering relationship through the following configuration.

Table 8-6 Configure MSDP peer connection control

Operation	Command	Description
Enter system view	**system-view**	—
Enter MSDP view	**msdp**	—
Shut down an MSDP peer	**shutdown** *peer-address*	Optional
Configure retry interval of setting up an MSDP peer connection	**timer retry** *seconds*	Optional The default value is 30 seconds.

8.4 Configuring SA Message Transmission

An SA message contains the IP address of the multicast source S, multicast group address G, and RP address. In addition, it contains the first multicast data received by the RP in the domain where the multicast source resides. For some burst multicast data, if the multicast data interval exceeds the SA message hold time, the multicast data must be encapsulated in the SA message; otherwise, the receiver will never receive the multicast source information.

By default, when a new receiver joins, a router does not send any SA request message to its MSDP peer but has to wait for the next SA message. This defers the reception of the multicast information by the receiver. In order for the new receiver to know about the currently active multicast source as quickly as possible, the router needs to send SA request messages to the MSDP peer.

Generally, a router accepts all SA messages sent by all MSDP peers and sends all SA messages to all MSDP peers. By configuring the rules for filtering SA messages to receive/send, you can effectively control the transmission of SA messages among MSDP peers. For forwarded SA messages, you can also configure a Time-to-Live (TTL) threshold to control the range where SA messages carrying encapsulated data are transmitted.

To reduce the delay in obtaining the multicast source information, you can cache SA messages on the router. The number of SA messages cached must not exceed the system limit. The more messages are cached, the more router memory is occupied.

8.4.1 Configuration Prerequisites

Before you configure SA message transmission, perform the following tasks:

- Configuring a unicast routing protocol.
- Configuring basic IP multicast functions.
- Configuring basic PIM-SM functions.
- Configuring basic MSDP functions.

Table 8-7 Configuration tasks

Operation	Description	Related section
Configure the transmission and filtering of SA request messages	Optional	Section 8.4.2 "Configuring the Transmission and Filtering of SA Request Messages"
Configure a rule for filtering the multicast source of SA messages	Optional	Section 8.4.3 "Configuring a Rule for Filtering the Multicast Sources of SA Messages"
Configure a rule for filtering received and forwarded SA messages	Optional	Section 8.4.4 "Configuring a Rule for Filtering Received and Forwarded SA Messages"
Configure SA message cache	Optional	Section 8.4.5 "Configuring SA Message Cache"

8.4.2 Configuring the Transmission and Filtering of SA Request Messages

After you enable the sending of SA request messages, when a router receives a Join message, it sends an SA request message to the specified remote MSDP peer, which responds with an SA message that it has cached. After sending an SA request message, the router will get immediately a response from all active multicast sources. By default, the router does not send any SA request message to its MSDP peers upon receipt of a Join message; instead, it waits for the next SA message.

The SA message that the remote MSDP peer responds with is cached in advance; therefore, you must enable the SA message caching mechanism in advance. Typically, only the routers caching SA messages can respond to SA request messages.

After you have configured a rule for filtering received SA messages, if no ACL is specified, all SA request messages sent by the corresponding MSDP peer will be ignored; if an ACL is specified, the SA request messages that satisfy the ACL rule are received while others are ignored.

Table 8-8 Configure the transmission and filtering of SA request messages

Operation	Command	Description
Enter system view	**system-view**	—
Enter MSDP view	**msdp**	—
Enable SA message caching mechanism	**cache-sa-enable**	Optional By default, the router caches the SA state upon receipt of an SA message.
Enable MSDP peers to send SA request messages	**peer** *peer-address* **request-sa-enable**	Optional By default, upon receipt of a Join message, the router sends no SA request message to its MSDP peer but waits for the next SA message.
Configure a rule for filtering the SA messages received by an MSDP peer	**peer** *peer-address* **sa-request-policy** [**acl** *acl-number*]	Optional You can configure the rule for filtering related multicast group IP addresses in ACL. By default, a router receives all SA request messages from the MSDP peer.

8.4.3 Configuring a Rule for Filtering the Multicast Sources of SA Messages

An RP filters each registered source to control the information of active sources advertised in the SA message. An MSDP peer can be configured to advertise only the (S, G) entries in the multicast routing table that satisfy the filtering rule when the MSDP creates the SA message; that is, to control the (S, G) entries to be imported from the multicast routing table to the PIM-SM domain. If the **import-source** command is executed without the **acl** keyword, no source will be advertised in the SA message.

Table 8-9 Configure a rule for filtering multicast sources using SA messages

Operation	Command	Description
Enter system view	**system-view**	—
Enter MSDP view	**msdp**	—
Configure to filter multicast sources using SA messages	**import-source** [**acl** *acl-number*]	Optional You can configure the rule for filtering related multicast group IP addresses in ACL. By default, all the (S, G) entries in the domain are advertised in the SA message.

8.4.4 Configuring a Rule for Filtering Received and Forwarded SA Messages

Besides the creation of source information, controlling multicast source information allows you to control the forwarding and reception of source information. You can control the reception of SA messages using the MSDP inbound filter (corresponding to the **import** keyword); you can control the forwarding of SA messages by using either the MSDP outbound filter (corresponding to the **export** argument) or the TTL threshold. By default, an MSDP peer receives and forwards all SA messages.

MSDP inbound/outbound filter implements the following functions:

- Filtering out all (S, G) entries
- Receiving/forwarding only the SA messages permitted by advanced ACL rules (You can configure ACL rules for filtering source IP addresses and group IP addresses.)

An SA message carrying encapsulated data can reach the specified MSDP peer outside the domain only when the TTL in its IP header exceeds the threshold; therefore, you can control the forwarding of SA messages that carry encapsulated data by configuring the TTL threshold.

Table 8-10 Configure a rule for filtering received and forwarded SA messages

Operation	Command	Description
Enter system view	**system-view**	—
Enter MSDP view	**msdp**	—
Configure to filter imported and exported SA messages	**peer** *peer-address* **sa-policy** { **import** | **export** } [**acl** *acl-number*]	Optional By default, no filtering is imposed on SA messages to be received or forwarded, namely all SA messages from MSDP peers are received or forwarded.
Configure the minimum TTL for the multicast packets sent to the specified MSDP peer	**peer** *peer-address* **minimum-ttl** *ttl-value*	Optional By default, the value of TTL threshold is 0.

8.4.5 Configuring SA Message Cache

With the SA message caching mechanism enabled on the router, the group that a new member subsequently joins can obtain all active sources directly from the SA cache and join the corresponding SPT source tree, instead of waiting for the next SA message.

You can configure the number of SA entries cached in each MSDP peer on the router by executing the following command, but the number must be within the system limit. To protect a router against Deny of Service (DoS) attacks, you can manually configure the maximum number of SA messages cached on the router. Generally, the configured number of SA messages cached should be less than the system limit.

Table 8-11 Configure SA message cache

Operation	Command	Description
Enter system view	**system-view**	—
Enter MSDP view	**msdp**	—
Enable SA message caching mechanism	**cache-sa-enable**	Optional By default, the SA message caching mechanism is enabled.
Configure the maximum number of SA messages cached	**peer** *peer-address* **sa-cache-maximum** *sa-limit*	Optional By default, the maximum number of SA messages cached on a router is 2,048.

8.5 Displaying and Maintaining MSDP Configuration

I. Displaying and debugging MSDP configuration

After the above-mentioned configuration, you can use the **display** command in any view to display the MSDP running information, so as to verify configuration result.

In user view, you can execute the **reset** command to reset the MSDP counter.

Table 8-12 Display and debug MSDP configuration

Operation	Command	Description
Display the brief information of MSDP peer state	**display msdp brief**	You can execute the **display** command in any view.
Display the detailed information of MSDP peer status	**display msdp peer-status** [*peer-address*]	
Display the (S, G) state learned from MSDP peers	**display msdp sa-cache** [*group-address* | [*source-address*]] [*autonomous-system-number*]	
Display the number of sources and groups in the MSDP cache	**display msdp sa-count** [*autonomous-system-number*]	
Reset the TCP connection with the specified MSDP peer	**reset msdp peer** *peer-address*	
Clear the cached SA messages	**reset msdp sa-cache** [*group-address*]	
Clear the statistics information of the specified MSDP peer without resetting the MSDP peer	**reset msdp statistics** [*peer-address*]	

II. Tracing the transmission path of an SA message over the network

You can use the **msdp-tracert** command in any view to trace the path along which the multicast data travels from the multicast source to the destination receiver over the network, so as to locate errors, if any.

Table 8-13 Trace the transmission path of an SA message over the network

Operation	Command	Description
Trace the transmission path of an SA message over the network	**msdp-tracert** *source-address group-address rp-address* [**max-hops** *max-hops*] [**next-hop-info** | **sa-info** | **peer-info**]* [**skip-hops** *skip-hops*]	You can execute the **msdp-tracert** command in any view.
Trace the transmission path of messages sent by the multicast source over the network	**mtracert** *source-address* [*group-address* | *last-hop-router-address group-address*]	You can execute the **mtracert**command in any view.

You can locate message loss and configuration errors by tracing the network path of the specified (S, G, RP) entries. Once the transmission path of SA messages is determined, correct configuration can prevent the flooding of SA messages.

8.6 MSDP Configuration Example

8.6.1 Configuration Example of Anycast RP Application

I. Network requirements

Each PIM-SM network is a single-BSR administrative domain, with multiple multicast sources (S) and receivers. With Anycast RP configured in each PIM-SM domain, when a new member joins the multicast group, the switch directly connected to the receiver can send a Join message to the nearest RP on the topology.

The PIM-SM network implements OSPF to provide unicast routes and establish MSDP peers between SwitchC and SwitchD. Meanwhile, the Loopback10 interfaces of SwitchC and SwitchD play the roles of C-BSR and C-RP.

II. Network diagram

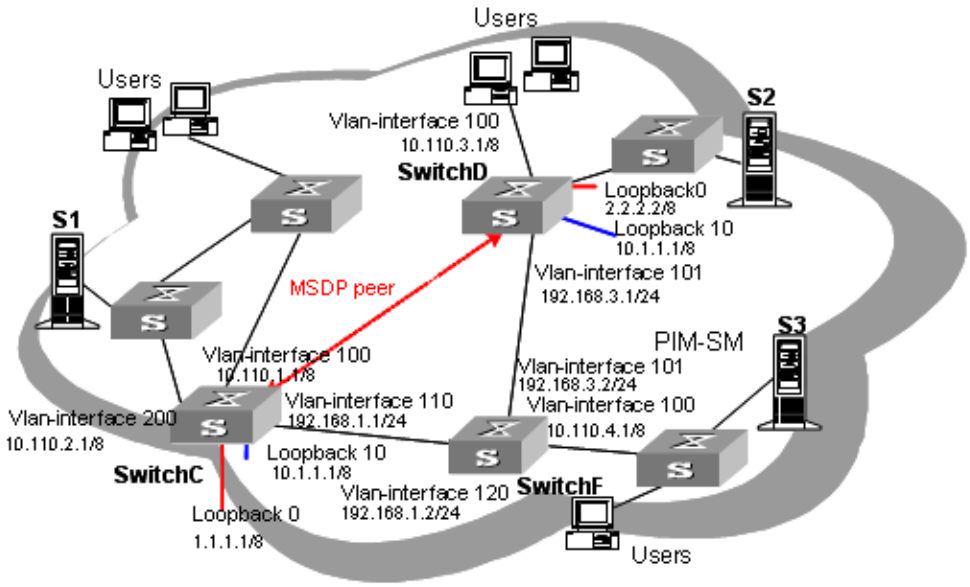


Figure 8-5 Network diagram for Anycast RP configuration

III. Configuration procedure

1) Configure interface IP addresses and unicast routing protocol on the switches.

In the PIM-SM domain, configure the interface IP addresses on the switches and interconnect the switches through OSPF. Configure the IP address and mask of each interface according to Figure 8-5. The details are omitted here.

2) Enable multicast and configure PIM-SM.

Enable multicast on SwitchC and enable PIM-SM on all interfaces. The configuration procedures on other switches are similar to that on SwitchC. The details are omitted here.

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface Vlan-interface 100
[SwitchC-Vlan-interface100] pim sm
[SwitchC-Vlan-interface100] quit
[SwitchC] interface Vlan-interface 200
[SwitchC-Vlan-interface200] pim sm
[SwitchC-Vlan-interface200] quit
[SwitchC] interface Vlan-interface 110
[SwitchC-Vlan-interface110] pim sm
[SwitchC-Vlan-interface110] quit
```

Configure the same Loopback10 interface address on SwitchC and SwitchD and configure the locations of C-BSR and C-RP. The configuration procedure on SwitchD is similar to that on SwitchC. The details are omitted here.

```
[SwitchC] interface loopback 10
[SwitchC-LoopBack10] ip address 10.1.1.1 255.255.255.255
[SwitchC-LoopBack10] pim sm
[SwitchC-LoopBack10] quit
[SwitchC] pim
[SwitchC-pim] c-bsr loopback 10
[SwitchC-pim] c-rp loopback 0
[SwitchC-pim] quit
```

3) Configure an MSDP peer.

Configure an MSDP peer on Loopback0 on SwitchC.

```
[SwitchC] msdp
[SwitchC-msdp] originating-rp loopback0
[SwitchC-msdp] peer 2.2.2.2 connect-interface loopback0
[SwitchC-msdp] quit
```

Configure an MSDP peer on Loopback0 on SwitchD.

```
[SwitchD] msdp
[SwitchD-msdp] originating-rp loopback0
[SwitchD-msdp] peer 1.1.1.1 connect-interface loopback0
[SwitchD-msdp] quit
```

8.7 Troubleshooting MSDP Configuration

8.7.1 MSDP Peer Always in the Down State

I. Symptom

An MSDP peer is configured, but it is always in the down state.

II. Analysis

An MSDP peer relationship between the locally configured **connect-interface** interface address and the configured peer address is based on a TCP connection. If the address of local **connect-interface** interface is inconsistent with the peer address configured on the peer router, no TCP connection can be established. If there is no route between the two peers, no TCP connection can be established.

III. Solution

1) Check the connectivity of the route between the routers. Use the **display ip routing-table** command to check that the unicast route between the routers is correct.
2) Further check that a unicast route exists between two routers that will become MSDP peers and that the route leads to the two peers.
3) Check that the interface addresses of the MSDP peers are consistent. Use the **display current-configuration** command to check that the address of the local connect-interface interface is consistent with the address of the corresponding MSDP peer.

8.7.2 No SA Entry in the SA Cache of the Router

I. Symptom

An MSDP fails to send (S, G) forwarding entries through an SA message.

II. Analysis

You can use the **import-source** command to send the (S, G) entries of the local multicast domain to the neighboring MSDP peer through SA messages. The **acl** keyword is optional. If you do not use this keyword, all (S, G) entries will be filtered out by default, that is, none of the (S, G) entries in the local multicast domain will be advertised. Before the **import-source** command is executed, the system will send all (S, G) entries in the local multicast domain. If the MSDP fails to send the (S, G) entries of the local multicast domain through SA messages, verify that the **import-source** command is configured correctly.

III. Solution

1) Check the connectivity of the route between the routers. Use the **display ip routing-table** command to check that the unicast route between the routers is correct.
2) Further check that a unicast route exists between two routers that will become MSDP peers and that the route leads to the two peers.
3) Verify the configuration of the **import-source** command and the corresponding ACL to ensure that the ACL rule filters the right (S, G) entries.

Table of Contents

Chapter 1 802.1x Configuration 1-1
1.1 Introduction to 802.1x 1-1
1.1.1 Architecture of 802.1x Authentication 1-1
1.1.2 The Mechanism of an 802.1x Authentication System 1-3
1.1.3 Encapsulation of EAPoL Messages 1-3
1.1.4 802.1x Authentication Procedure 1-6
1.1.5 Timers Used in 802.1x 1-9
1.1.6 802.1x Implementation on an S3600 Series Switch 1-10
1.2 802.1x Configuration 1-12
1.3 Basic 802.1x Configuration 1-13
1.3.1 Prerequisites 1-13
1.3.2 Configuring Basic 802.1x Functions 1-13
1.4 Timer and Maximum User Number Configuration 1-15
1.5 Advanced 802.1x Configuration 1-16
1.5.1 Prerequisites 1-16
1.5.2 Configuring Proxy Checking 1-16
1.5.3 Configuring Client Version Checking 1-17
1.5.4 Enabling DHCP-triggered Authentication 1-18
1.5.5 Configuring Guest VLAN 1-18
1.6 Displaying and Debugging 802.1x 1-19
1.7 Configuration Example 1-19
1.7.1 802.1x Configuration Example 1-19

Chapter 2 HABP Configuration 2-1
2.1 Introduction to HABP 2-1
2.2 HABP Server Configuration 2-1
2.3 HABP Client Configuration 2-2
2.4 Displaying HABP 2-2

Chapter 1 802.1x Configuration

1.1 Introduction to 802.1x

The 802.1x protocol (802.1x for short) was developed by IEEE802 LAN/WAN committee to address security issues of wireless LANs. It was then used in Ethernet as a common access control mechanism for LAN ports to address mainly authentication and security problems.

802.1x is a port-based network access control protocol. It authenticates and controls devices requesting for access in terms of the ports of LAN access control devices. With the 802.1x protocol employed, a user-side device can access the LAN only when it passes the authentication. Those fail to pass the authentication are denied when accessing the LAN, as if they are disconnected from the LAN.

1.1.1 Architecture of 802.1x Authentication

802.1x adopts a client/server architecture with three entities: a supplicant system, an authenticator system, and an authentication server system, as shown in the following figure.

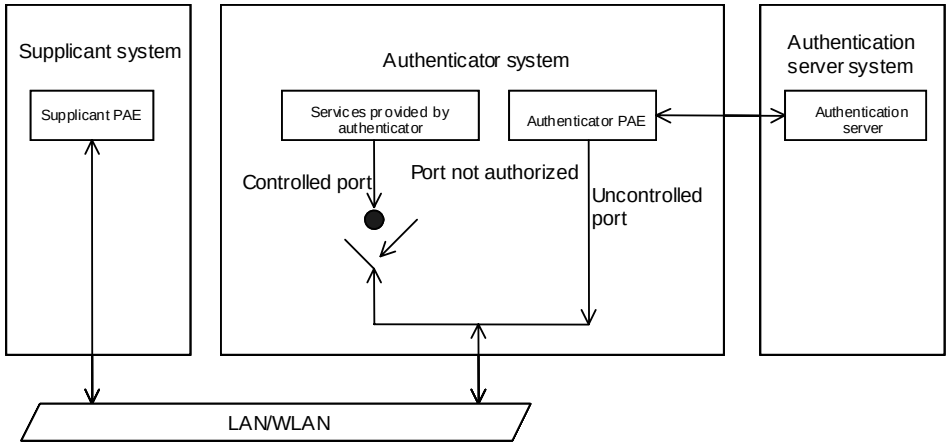


Figure 1-1 Architecture of 802.1x authentication

- The supplicant system is an entity residing at one end of a LAN segment and is authenticated by the authenticator system connected to the other end of the LAN segment. The supplicant system is usually a user terminal device. An 802.1x authentication is triggered when a user launches client program on the supplicant system. Note that the client program must support the EAPoL (extensible authentication protocol over LANs).

- The authenticator system is an entity residing at one end of a LAN segment. It authenticates the supplicant systems connecting to the other end of the LAN segment. The authenticator system is usually an 802.1x-supported network device (such as a H3Cseries switch). It provides the port (physical or logical) for the supplicant system to access the LAN.
- The authentication server system is an entity that provides authentication service to the authenticator system. Normally in the form of a RADIUS server, the authentication server system serves to perform AAA (authentication, authorization, and accounting) services to users. It also stores user information, such as user name, password, the VLAN a user belongs to, priority, and the ACLs (access control list) applied.

The four basic concept related to the above three entities are PAE, controlled port and uncontrolled port, the valid direction of a controlled port and the way a port is controlled.

I. PAE

A PAE (port access entity) is responsible for implementing algorithms and performing protocol-related operations in the authentication mechanism.

The authenticator system PAE authenticates the supplicant systems when they log into the LAN and controls the authorizing state (on/off) of the controlled ports according to the authentication result.

The supplicant system PAE responds to the authentication requests received from the authenticator system and submits user authentication information to the authenticator system. It also sends authentication requests and disconnection requests to the authenticator system PAE.

II. Controlled port and uncontrolled port

The Authenticator system provides ports for supplicant systems to access a LAN. Logically, a port of this kind is divided into a controlled port and an uncontrolled port.

- The uncontrolled port can always send and receive packets. It mainly serves to forward EAPoL packets to ensure that a supplicant system can send and receive authentication requests.
- The controlled port can be used to pass service packets when it is in authorized state. It is blocked when not in authorized state. In this case, no packets can pass through it.
- Controlled port and uncontrolled port are two properties of a port. Packets reaching a port are visible to both the controlled port and uncontrolled port of the port.

III. The valid direction of a controlled port

When a controlled port is in unauthorized state, you can configure it to be a unidirectional port, which sends packets to supplicant systems only.

By default, a controlled port is a unidirectional port.

IV. The way a port is controlled

A port of a H3Cseries switch can be controlled in the following two ways.

- Port-based authentication. When a port is controlled in this way, all the supplicant systems connected to the port can access the network without being authenticated after one supplicant system among them passes the authentication. And when the authenticated supplicant system goes offline, the others are denied as well.
- MAC address-based authentication. All supplicant systems connected to a port have to be authenticated individually in order to access the network. And when a supplicant system goes offline, the others are not affected.

1.1.2 The Mechanism of an 802.1x Authentication System

IEEE 802.1x authentication system uses extensible authentication protocol (EAP) to exchange information between supplicant systems and the authentication servers.

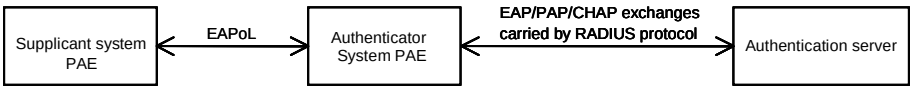


Figure 1-2 The mechanism of an 802.1x authentication system

- EAP protocol packets transmitted between the supplicant system PAE and the authenticator system PAE are encapsulated as EAPoL packets.
- EAP protocol packets transmitted between the authenticator system PAE and the RADIUS server can either be encapsulated as EAPoR (EAP over RADIUS) packets or be terminated at system PAEs. The system PAEs then communicate with RADIUS servers through PAP (password authentication protocol) or CHAP (challenge-handshake authentication protocol] protocol packets.
- When a supplicant system passes the authentication, the authentication server passes the information about the supplicant system to the authenticator system. The authenticator system in turn determines the state (authorized or unauthorized) of the controlled port according to the instructions (accept or reject) received from the RADIUS server.

1.1.3 Encapsulation of EAPoL Messages

I. The format of an EAPoL packet

EAPoL is a packet encapsulation format defined in 802.1x. To enable EAP protocol packets to be transmitted between supplicant systems and authenticator systems

through LANs, EAP protocol packets are encapsulated in EAPoL format. The following figure illustrates the structure of an EAPoL packet.

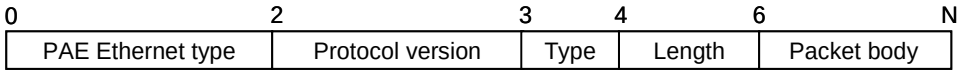


Figure 1-3 The format of an EAPoL packet

In an EAPoL packet:

- The PAE Ethernet type field holds the protocol identifier. The identifier for 802.1x is 0x888E.
- The Protocol version field holds the version of the protocol supported by the sender of the EAPoL packet.
- The Type field can be one of the following:
  00: Indicates that the packet is an EAP-packet, which carries authentication information.
  01: Indicates that the packet is an EAPoL-start packet, which initiates the authentication.
  02: Indicates that the packet is an EAPoL-logoff packet, which sends logging off requests.
  03: Indicates that the packet is an EAPoL-key packet, which carries key information.
  04: Indicates that the packet is an EAPoL-encapsulated-ASF-Alert packet, which is used to support the alerting messages of ASF (alerting standards forum).
- The Length field indicates the size of the Packet body field. A value of 0 indicates that the Packet Body field does not exist.
- The Packet body field differs with the Type field.

Note that EAPoL-Start, EAPoL-Logoff, and EAPoL-Key packets are only transmitted between the supplicant system and the authenticator system. EAP-packets are encapsulated by RADIUS protocol to allow them successfully reach the authentication servers. Network management-related information (such as alarming information) is encapsulated in EAPoL-Encapsulated-ASF-Alert packets, which are terminated by authenticator systems.

II. The format of an EAP packet

For an EAPoL packet with the value of the Type field being EAP-packet, its Packet body field is an EAP packet, whose format is illustrated in Figure 1-4.

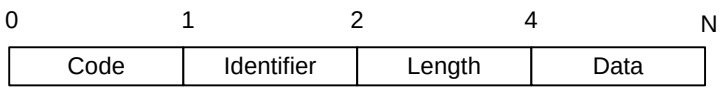


Figure 1-4 The format of an EAP packet

In an EAP packet:

- The Code field indicates the EAP packet type, which can be Request, Response, Success, or Failure.
- The Identifier field is used to match a Response packets with the corresponding Request packet.
- The Length field indicates the size of an EAP packet, which includes the Code, Identifier, Length, and Data fields.
- The Data field differs with the Code field.

A Success or Failure packet does not contain the Data field, so the Length field of it is 4.

Figure 1-5 shows the format of the Data field of a Request packet or a Response packet.

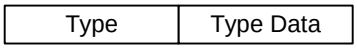


Figure 1-5 The format of the Data field of a Request packet or a Response packet

- The Type field indicates the EAP authentication type. A value of 1 indicates Identity and that the packet is used to query the identity of the peer. A value of 4 represents MD5-Challenge (similar to PPP CHAP) and indicates that the packet includes query information.
- The Type Date field differs with types of Request and Response packets.

III. Newly added fields for EAP authentication

Two fields, EAP-message and Message-authenticator, are added to a RADIUS protocol packet for EAP authentication. (Refer to the Introduction to RADIUS protocol section in the *AAA,RADIUS,HWTACACS and EAD Operation* part for information about the format of a RADIUS protocol packet.)

The EAP-message field, whose format is shown in Figure 1-6, is used to encapsulate EAP packets. The maximum size of the string field is 253 bytes. EAP packets with their size larger than 253 bytes are fragmented and are encapsulated in multiple EAP-message fields. The type code of the EAP-message field is 79.

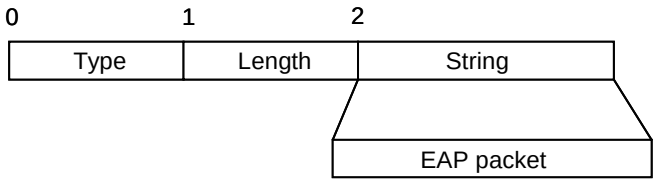


Figure 1-6 The format of an EAP-message field

The Message-authenticator field, whose format is shown in Figure 1-7, is used to prevent unauthorized interception to access requesting packets during authentications using CHAP, EAP, and so on. A packet with the EAP-message field must also have the

Message-authenticator field. Otherwise, the packet is regarded as invalid and is discarded.

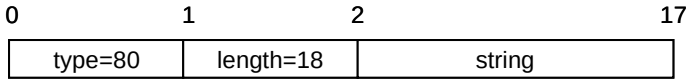


Figure 1-7 The format of an Message-authenticator field

1.1.4 802.1x Authentication Procedure

A H3C3600 series Ethernet switch can authenticate supplicant systems in EAP terminating mode or EAP relay mode.

I. EAP relay mode

This mode is defined in 802.1x. In this mode, EAP-packets are encapsulated in higher level protocol (such as EAPoR) packets to enable them to successfully reach the authentication server. Normally, this mode requires that the RADIUS server support the two newly-added fields: the EAP-message field (with a value of 79) and the Message-authenticator field (with a value of 80).

Four authentication ways, namely EAP-MD5, EAP-TLS (transport layer security), EAP-TTLS, and PEAP (protected extensible authentication protocol), are available in the EAP relay mode.

- EAP-MD5 authenticates the supplicant system. The RADIUS server sends MD5 keys (contained in EAP-request/MD5 challenge packets) to the supplicant system, which in turn encrypts the passwords using the MD5 keys.
- EAP-TLS authenticates both the supplicant system and the RADIUS server by checking their security licenses to prevent data from being stolen.
- EAP-TTLS is a kind of extended EAP-TLS. EAP-TLS implements bidirectional authentication between the client and authentication server. EAP-TTLS transmit message using a tunnel established using TLS.
- PEAP creates and uses TLS security channels to ensure data integrity and then performs new EAP negotiations to verify supplicant systems.

Figure 1-8 describes the basic EAP-MD5 authentication procedure.

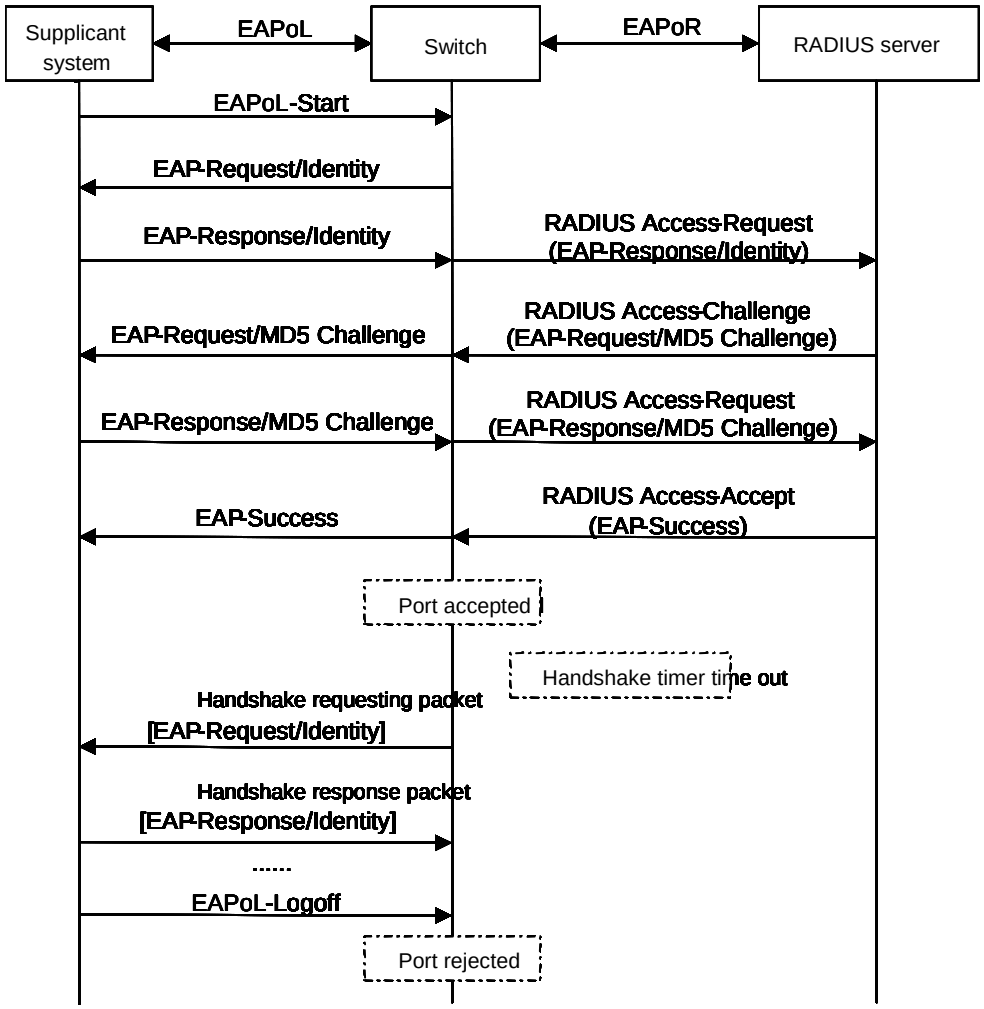


Figure 1-8 802.1x authentication procedure (in EAP relay mode)

The detailed procedure is as follows.

- A supplicant system launches an 802.1x client to initiate an access request by sending an EAPoL-start packet to the switch, with its user name and password provided. The 802.1x client program then forwards the packet to the switch to start the authentication process.
- Upon receiving the authentication request packet, the switch sends an EAP-request/identity packet to ask the 802.1x client for the user name.
- The 802.1x client responds by sending an EAP-response/identity packet to the switch with the user name contained in it. The switch then encapsulates the packet in a RADIUS Access-Request packet and forwards it to the RADIUS server.
- Upon receiving the packet from the switch, the RADIUS server retrieves the user name from the packet, finds the corresponding password by matching the user name in its database, encrypts the password using a randomly-generated key, and sends the key to the switch through an RADIUS access-challenge packet. The switch then sends the key to the 802.1x client.

- Upon receiving the key (encapsulated in an EAP-request/MD5 challenge packet) from the switch, the client program encrypts the password of the supplicant system with the key and sends the encrypted password (contained in an EAP-response/MD5 challenge packet) to the RADIUS server through the switch. (Normally, the encryption is irreversible.)
- The RADIUS server compares the received encrypted password (contained in a RADIUS access-request packet) with the locally-encrypted password. If the two match, it will then send feedbacks (through a RADIUS access-accept packet and an EAP-success packet) to the switch to indicate that the supplicant system is authenticated.
- The switch changes the state of the corresponding port to accepted state to allow the supplicant system to access the network.
- The supplicant system can also terminate the authenticated state by sending EAPoL-Logoff packets to the switch. The switch then changes the port state from accepted to rejected.

Note:

In EAP relay mode, packets are not modified during transmission. Therefore if one of the four ways are used (that is, PEAP, EAP-TLS, EAP-TTLS or EAP-MD5) to authenticate, ensure that the authenticating ways used on the supplicant system and the RADIUS server are the same. However for the switch, you can simply enable the EAP relay mode by using the **dot1x authentication-method eap** command.

II. EAP terminating mode

In this mode, EAP packet transmission is terminated at authenticator systems and the EAP packets are converted to RADIUS packets. Authentication and accounting are carried out through RADIUS protocol.

In this mode, PAP or CHAP is employed between the switch and the RADIUS server. Figure 1-9 illustrates the authentication procedure (assuming that CHAP is employed between the switch and the RADIUS server).

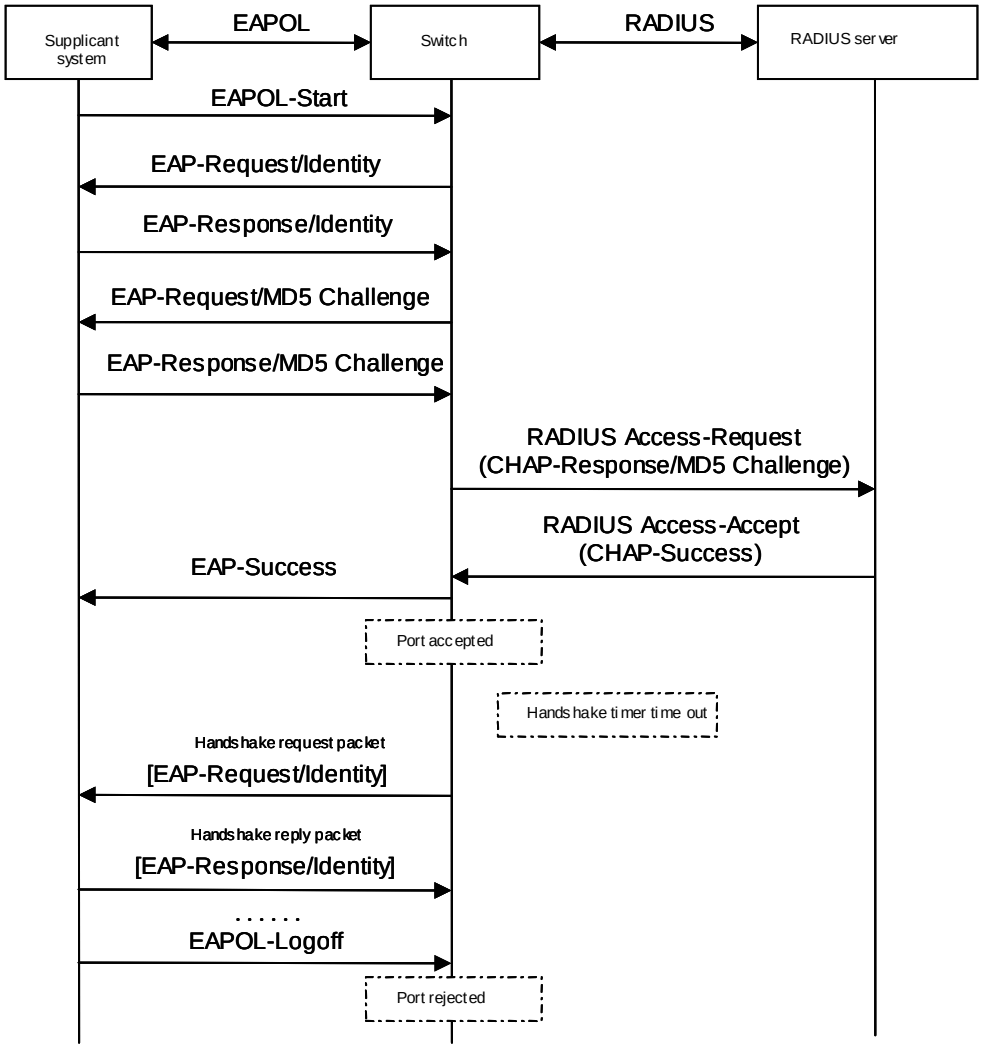


Figure 1-9 802.1x authentication procedure (in EAP terminating mode)

The authentication procedure in EAP terminating mode is the same as that in the EAP relay mode except that the randomly-generated key in the EAP terminating mode is generated by the switch, and that it is the switch that sends the user name, the randomly-generated key, and the supplicant system-encrypted password to the RADIUS server for further authentication.

1.1.5 Timers Used in 802.1x

In 802.1 x authentication, the following timers are used to ensure that the supplicant system, the switch, and the RADIUS server interact in an orderly way.

- Handshake timer (**handshake-period**). This timer sets the handshake-period and is triggered after a supplicant system passes the authentication. It sets the interval for a switch to send handshake request packets to online users. If you set the number of retries to N by using the **dot1x retry** command, an online user is

considered offline when the switch does not receive response packets from it in a period N times of the handshake-period.

- Quiet-period timer (**quiet-period**). This timer sets the quiet-period. When a supplicant system fails to pass the authentication, the switch quiets for the set period (set by the quiet-period timer) before it processes another authentication request re-initiated by the supplicant system.
- RADIUS server timer (**server-timeout**). This timer sets the server-timeout period. After sending an authentication request packet to the RADIUS server, a switch sends another authentication request packet if it does not receive the response from the RADIUS server when this timer times out.
- Supplicant system timer (**supp-timeout**). This timer sets the supp-timeout period and is triggered by the switch after the switch sends a request/challenge packet to a supplicant system. The switch sends another request/challenge packet to the supplicant system if the switch does not receive the response from the supplicant system when this timer times out.
- Transmission timer (**tx-period**). This timer sets the tx-period and is triggered by the switch in two cases. The first case is when the client requests for authentication. The switch sends a unicast request/identity packet to a supplicant system and then triggers the transmission timer. The switch sends another request/identity packet to the supplicant system if it does not receive the reply packet from the supplicant system when this timer times out. The second case is when the switch authenticates the 802.1x client who cannot request for authentication actively. The switch sends multicast request/identity packets periodically through the port enabled with 802.1x function. In this case, this timer sets the interval to send the multicast request/identity packets.
- Client version request timer (**ver-period**). This timer sets the version period and is triggered after a switch sends a version request packet. The switch sends another version request packet if it does receive version response packets from the supplicant system when the timer expires.

1.1.6 802.1x Implementation on an S3600 Series Switch

In addition to the earlier mentioned 802.1x features, an S3600 series switch is also capable of the following:

- Checking supplicant systems for proxies, multiple network adapters, and so on (This function needs the cooperation of a CAMS server.)
- Checking client version
- The Guest VLAN function

I. Checking the supplicant system

An S3600 series switch checks:

- Supplicant systems logging on through proxies

- Supplicant systems logging on through IE proxies
- Whether or not a supplicant system logs in through more than one network adapters (that is, whether or not more than one network adapters are active in a supplicant system when the supplicant system logs in).

In response to any of the three cases, a switch can optionally take the following measures:

- Only disconnects the supplicant system but sends no Trap packets, which can be achieved by using the **dot1x supp-proxy-check logoff** command.
- Sends Trap packets without disconnecting the supplicant system, which can be achieved by using the **dot1x supp-proxy-check trap** command.

This function needs the cooperation of 802.1x client and a CAMS server.

- The 802.1x client needs to capable of detecting multiple network adapters, proxies, and IE proxies.
- The CAMS server is configured to disable the use of multiple network adapters, proxies, or IE proxies.

By default, an 802.1x client program allows use of multiple network adapters, proxies, and IE proxies. In this case, if the CAMS server is configured to disable use of multiple network adapters, proxies, or IE proxies, it prompts the 802.1x client to disable use of multiple network adapters, proxies, or IE proxies through messages after the supplicant system passes the authentication.

🕮 **Note:**

- The client-checking function needs the support of H3C's 802.1x client program.
- To implement the proxy detecting function, you need to enable the function on both the 802.1x client program and the CAMS server in addition to enabling the client version detecting function on the switch by using the **dot1x version-check** command.

II. Checking the client version

With the 802.1x client version-checking function enabled, a switch checks the version and validity of an 802.1x client to prevent unauthorized users or users with earlier versions of 802.1x client from logging in.

This function makes the switch to send version-requesting packets again if the 802.1x client fails to send version-reply packet to the switch when the version-checking timer times out.

Note:

The 802.1x client version-checking function needs the support of H3C's 802.1x client program.

III. The Guest VLAN function

The Guest VLAN function enables supplicant systems that that are not authenticated to access network resources in a restrained way.

The Guest VLAN function enables supplicant systems that do not have 802.1x client installed to access specific network resources. It also enables supplicant systems that are not authenticated to upgrade their 802.1x client programs.

With this function enabled:

- The switch multicasts trigger packets through all the 802.1x-enabled ports.
- After the maximum number retries have been made and there are still ports that have not sent any response back, the switch will then add these ports to the Guest VLAN.
- Users belonging to the Guest VLAN can access the resources of the Guest VLAN without being authenticated. But they need to be authenticated when accessing external resources.

Normally, the Guest VLAN function is coupled with the dynamic VLAN delivery function.

Refer to *AAA&RADIUS&RADIUS&HWTACACS&EAD Operation Manual* for detailed information about the dynamic VLAN delivery function.

1.2 802.1x Configuration

802.1x provides a solution for authenticating users. To implement this solution, you need to execute 802.1x-related commands. You also need to configure AAA schemes on switches and specify the authentication scheme (RADIUS authentication scheme or local authentication scheme).

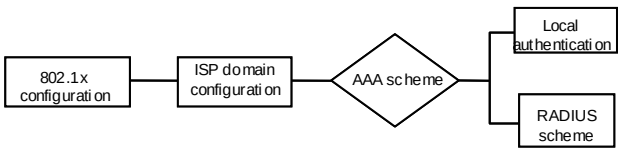


Figure 1-10 802.1x configuration

- 802.1x users use domain names to associate with the ISP domains configured on switches
- Configure the AAA scheme (a local authentication scheme or the RADIUS scheme) to be adopted in the ISP domain.

- If you specify to adopt the RADIUS scheme, the supplicant systems are authenticated by a remote RADIUS server. In this case, you need to configure user names and passwords on the RADIUS server and perform RADIUS client-related configuration on the switches.
- If you specify to adopt a local authentication scheme, you need to configure user names and passwords manually on the switches. Users can pass the authentication through 802.1x client if they provide the user names and passwords that match those configured on the switches.
- You can also specify to adopt RADIUS authentication scheme, with a local authentication scheme as a backup. In this case, the local authentication scheme is adopted when the RADIUS server fails.

Refer to the *AAA&RADIUS&RADIUS&HWTACACS&EAD Operation Manual* for detailed information about AAA scheme configuration.

1.3 Basic 802.1x Configuration

To utilize 802.1x features, you need to perform basic 802.1x configuration.

1.3.1 Prerequisites

- Configure ISP domain and the AAA scheme to be adopted. You can specify a RADIUS scheme or a local scheme.
- Ensure that the service type is configured as **lan-access** (by using the **service-type** command) if local authentication scheme is adopted.

1.3.2 Configuring Basic 802.1x Functions

Table 1-1 Configure basic 802.1x functions

Operation	Command	Description
Enter system view	**system-view**	—
Enable 802.1x globally	**dot1x**	Required By default, 802.1x is disabled globally.
Enable 802.1x for specified ports	Use the following command in system view: **dot1x** [**interface** *interface-list*]	Required By default, 802.1x is disabled on all ports.
	Use the following command in port view: **dot1x**	

Operation	Command	Description
Set port access control mode for specified ports	**dot1x port-control** { **authorized-force** | **unauthorized-force** | **auto** } [**interface** *interface-list*]	Optional By default, an 802.1x-enabled port operates in the **auto** mode.
Set port access method for specified ports	**dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*]	Optional The default port access method is MAC-address-based (that is, the **macbased** keyword is used by default).
Set authentication method for 802.1x users	**dot1x authentication-method** { **chap** | **pap** | **eap** }	Optional By default, a switch performs CHAP authentication in EAP terminating mode.

Caution:

- 802.1x-related configurations can all be performed in system view. Port access control mode and port access method can also be configured in port view.
- If you perform a configuration in system view and do not specify the *interface-list* argument, the configuration applies to all ports. Configurations performed in Ethernet port view apply to the current Ethernet port only. In this case, the *interface-list* argument is not needed.
- 802.1x configurations take effect only after you enable 802.1x both globally and for specified ports.
- When a device operates as an authentication server, its authentication method for 802.1x users cannot be configured as EAP.

1.4 Timer and Maximum User Number Configuration

Table 1-2 Configure 802.1x timers and the maximum number of users

Operation	Command	Description
Enter system view	**system-view**	—
Set the maximum number of concurrent on-line users for specified ports	In system view: **dot1x max-user** *user-number* [**interface** *interface-list*]	Optional By default, a port can accommodate up to 256 users at a time.
	In port view: **dot1x max-user** *user-number*	
Set the maximum retry times to send request packets	**dot1x retry** *max-retry-value*	Optional By default, the maximum retry times to send a request packet is 2. That is, the authenticator system sends a request packet to a supplicant system for up to two times by default.
Set 802.1x timers	**dot1x timer** { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* | **ver-period** *ver-period-value* }	Optional The settings of 802.1x timers are as follows. • *handshake-period-value:* 15 seconds • *quiet-period-value:* 60 seconds • *server-timeout-value:* 100 seconds • *supp-timeout-value:* 30 seconds • *tx-period-value:* 30 seconds • *ver-period-value:* 30 seconds
Trigger the quiet-period timer	**dot1x quiet-period**	Optional By default, the quiet-period timer is disabled.

Note:

- As for the **dot1x max-user** command, if you execute it in system view without specifying the *interface-list* argument, the command applies to all ports. You can also use this command in port view. In this case, this command applies to the current port only and the *interface-list* argument is not needed.
- As for the configuration of 802.1x timers, the default values are recommended.

1.5 Advanced 802.1x Configuration

Advanced 802.1x configurations, as listed below, are all optional.

- Configuration concerning CAMS, including multiple network adapters detecting, proxy detecting, and so on.
- Client version checking configuration
- DHCP –triggered authentication
- Guest VLAN configuration

1.5.1 Prerequisites

Basic 802.1x configuration is performed.

1.5.2 Configuring Proxy Checking

This function needs the cooperation of 802.1x client program and CAMS server, as listed below.

- The 802.1x client needs to capable of detecting multiple network adapters, proxies, and IE proxies.
- The CAMS server is configured to disable the use of multiple network adapters, proxies, or IE proxies.

By default, an 802.1x client program allows use of multiple network adapters, proxies, and IE proxies. In this case, if the CAMS server is configured to disable use of multiple network adapters, proxies, or IE proxies, it prompts the 802.1x client to disable use of multiple network adapters, proxies, or IE proxies through messages after the supplicant system passes the authentication.

Table 1-3 Configure proxy checking

Operation	Command	Description
Enter system view	**system-view**	—
Enable proxy checking function globally	**dot1x supp-proxy-check** { **logoff** | **trap** }	Required By default, the 802.1x proxy checking function is globally disabled.
Enable proxy checking for a port/specified ports	In system view: **dot1x supp-proxy-check** { **logoff** | **trap** } [**interface** *interface-list*]	Required By default, the 802.1x proxy checking is disabled on a port.
	In port view: **dot1x supp-proxy-check** { **logoff** | **trap** }	

Note:

- The proxy checking function needs the cooperation of H3C's 802.1x client program.
- The configuration listed in Table 1-3 takes effect only when it is performed on CAMS as well as on the switch. In addition, the client version checking function needs to be enabled on the switch too (by using the **dot1x version-check** command).

1.5.3 Configuring Client Version Checking

Table 1-4 Configure client version checking

Operation	Command	Description
Enter system view	**system-view**	—
Enable 802.1x client version checking	**dot1x version-check** [**interface** *interface-list*]	Required By default, 802.1x client version checking is disabled on a port.
Set the maximum number of retires to send version checking request packets	**dot1x retry-version-max** *max-retry-version-value*	Optional By default, the maximum number of retires to send version checking request packets is 3.
Set the client version checking period timer	**dot1x timer ver-period** *ver-period-value*	Optional By default, the timer is set to 30 seconds.

Note:

As for the **dot1x version-user** command, if you execute it in system view without specifying the *interface-list* argument, the command applies to all ports. You can also execute this command in port view. In this case, this command applies to the current port only and the *interface-list* argument is not needed.

1.5.4 Enabling DHCP-triggered Authentication

After performing the following configuration, 802.1X allows running DHCP on access users, and users are authenticated when they apply for dynamic IP addresses through DHCP.

Table 1-5 Enable DHCP-triggered authentication

Operation	Command	Description
Enter system view	**system-view**	—
Enable DHCP-triggered authentication	**dot1x dhcp-launch**	Optional By default, DHCP-triggered authentication is disabled.

1.5.5 Configuring Guest VLAN

Table 1-6 Configure Guest VLAN

Operation	Command	Description
Enter system view	**system-view**	—
Configure port access method	**dot1x port-method portbased**	Required The default port access method is MAC-address-based. That is, the **macbased** keyword is used by default.
Enable the Guest VLAN function	**dot1x guest-vlan** *vlan-id* [**interface** *interface-list*]	Required By default, the Guest VLAN function is disabled.

Caution:

- The Guest VLAN function is available only when the switch operates in the port-based authentication mode.
- Only one Guest VLAN can be configured for each switch.

1.6 Displaying and Debugging 802.1x

After performing the above configurations, you can display and verify the 802.1x-related configuration by executing the **display** command in any view.

You can clear 802.1x-related statistics information by executing the **reset** command in user view.

Table 1-7 Display and debug 802.1x

Operation	Command	Description
Display the configuration, session, and statistics information about 802.1x	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]	This command can be executed in any view.
Clear 802.1x-related statistics information	**reset dot1x statistics** [**interface** *interface-list*]	Execute this command in user view.

1.7 Configuration Example

1.7.1 802.1x Configuration Example

I. Network requirements

- Authenticate users on all ports to control their accesses to the Internet. The switch operates in MAC address-based access control mode.
- All supplicant systems that pass the authentication belong to the default domain named “aabbcc.net”. The domain can accommodate up to 30 users. As for authentication, a supplicant system is authenticated locally if the RADIUS server fails. And as for accounting, a supplicant system is disconnected by force if the RADIUS server fails. The name of an authenticated supplicant system is not suffixed with the domain name. A connection is terminated if the total size of the data passes through it during a period of 20 minutes is less than 2,000 bytes.
- The switch is connected to a server comprising of two RADIUS servers whose IP addresses are 10.11.1.1 and 10.11.1.2. The RADIUS server with an IP address of 10.11.1.1 operates as the primary authentication server and the secondary accounting server. The other operates as the secondary authentication server and

primary accounting server. The password for the switch and the authentication RADIUS servers to exchange message is “name”. And the password for the switch and the accounting RADIUS servers to exchange message is “money”. The switch sends another packet to the RADIUS servers again if it sends a packet to the RADIUS server and does not receive response for 5 seconds, with the maximum number of retries of 5. And the switch sends a real-time accounting packet to the RADIUS servers once in every 15 minutes. A user name is sent to the RADIUS servers with the domain name truncated.

- The user name and password for local 802.1x authentication are “localuser” and “localpass” (in plain text) respectively. The idle disconnecting function is enabled.

II. Network diagram

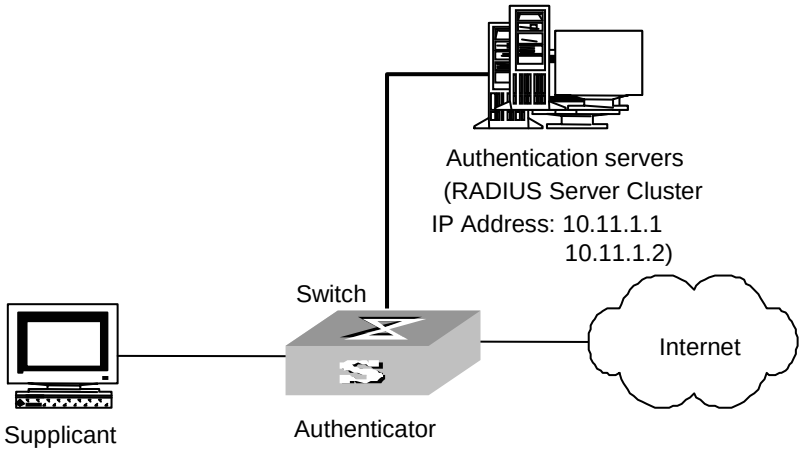


Figure 1-11 Network diagram for AAA configuration with 802.1x and RADIUS enabled

III. Configuration procedure

Note:

Following configuration covers the major AAA/RADIUS configuration commands. Refer to *AAA,RADIUS,HWTACACS and EAD Operation Manual* for the information about these commands. Configuration on the client and the RADIUS servers is omitted.

Enable 802.1x globally.

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] dot1x
```

Enable 802.1x for Ethernet1/0/1 port.

```
[H3C] dot1x interface Ethernet 1/0/1
```

Set the access control method to be MAC-address-based (This operation can be omitted, as MAC-address-based is the default).

```
[H3C] dot1x port-method macbased interface Ethernet 1/0/1
```

Create a RADIUS scheme named “radius1” and enter RADIUS scheme view.

```
[H3C] radius scheme radius1
```

Assign IP addresses to the primary authentication and accounting RADIUS servers.

```
[H3C-radius-radius1] primary authentication 10.11.1.1
[H3C-radius-radius1] primary accounting 10.11.1.2
```

Assign IP addresses to the secondary authentication and accounting RADIUS server.

```
[H3C-radius-radius1] secondary authentication 10.11.1.2
[H3C-radius-radius1] secondary accounting 10.11.1.1
```

Set the password for the switch and the authentication RADIUS servers to exchange messages.

```
[H3C-radius-radius1] key authentication name
```

Set the password for the switch and the accounting RADIUS servers to exchange messages.

```
[H3C-radius-radius1] key accounting money
```

Set the interval and the number of the retries for the switch to send packets to the RADIUS servers.

```
[H3C-radius-radius1] timer 5
[H3C-radius-radius1] retry 5
```

Set the timer for the switch to send real-time accounting packets to the RADIUS servers.

```
[H3C-radius-radius1] timer realtime-accounting 15
```

Configure to send the user name to the RADIUS server with the domain name truncated.

```
[H3C-radius-radius1] user-name-format without-domain
[H3C-radius-radius1] quit
```

Create the domain named “aabbcc.net” and enter its view.

```
[H3C] domain enable aabbcc.net
```

Specify to adopt radius1 as the RADIUS scheme of the user domain. If RADIUS server is invalid, specify to adopt the local authentication scheme.

```
[H3C-isp-aabbcc.net] scheme radius-scheme radius1 local
```

Specify the maximum number of users the user domain can accommodate to 30.

```
[H3C-isp-aabbcc.net] access-limit enable 30
```

Enable the idle disconnecting function and set the related parameters.

```
[H3C-isp-aabbcc.net] idle-cut enable 20 2000
[H3C-isp-aabbcc.net] quit
```

Set the default user domain to be “aabbcc.net”.

```
[H3C] domain default enable aabbcc.net
```

Create a local access user account.

```
[H3C] local-user localuser
[H3C-luser-localuser] service-type lan-access
[H3C-luser-localuser] password simple localpass
```

Chapter 2 HABP Configuration

2.1 Introduction to HABP

With 802.1x enabled, a switch authenticates and then authorizes 802.1x-enabled ports. Packets can be forwarded only by authorized ports. For ports connected to the switch and are not authenticated and authorized by 802.1x, their received packets will be filtered. This means that users cannot manage the attached switches. Huawei authentication bypass protocol (HABP) is designed to address this problem.

An HABP packet carries the MAC addresses of the attached switches with it. It can bypass the 802.1x authentications when traveling between HABP-enabled switches, through which management devices can obtain the MAC addresses of the attached switches and thus the management of the attached switches is feasible.

HABP is implemented by HABP server and HABP client. Normally, an HABP server sends HABP request packets regularly to HABP clients to collect the MAC addresses of the attached switches. HABP clients respond to the HABP request packets and forward the HABP request packets to lower-level switches. HABP servers usually reside on management devices and HABP clients usually on attached switches.

For ease of switch management, it is recommended that you enable HABP for 802.1x-enabled switches.

2.2 HABP Server Configuration

With the HABP server launched, a management device sends HABP request packets regularly to the attached switches to collect their MAC addresses. You need also to configure the interval on the management device for an HABP server to send HABP request packets.

Table 2-1 Configure an HABP server

Operation	Command	Description
Enter system view	**system-view**	—
Enable HABP	**habp enable**	Required HABP is enabled by default.
Configure the current switch to be an HABP server	**habp server vlan** *vlan-id*	Required By default, a switch operates as an HABP client after you enable HABP on the switch. If you want to use the switch as a management switch, you need to configure the switch to be an HABP server.

Operation	Command	Description
Configure the interval to send HABP request packets.	**habp timer** *interval*	Optional The default interval for an HABP server to send HABP request packets is 20 seconds.

2.3 HABP Client Configuration

HABP clients reside on switches attached to HABP servers. After you enable HABP for a switch, the switch operates as an HABP client by default. So you only need to enable HABP on a switch to make it an HABP client.

Table 2-2 Configure an HABP client

Operation	Command	Description
Enter system view	**system-view**	—
Enable HABP	**habp enable**	Optional HABP is enabled by default. And a switch operates as an HABP client after you enable HABP for it.

2.4 Displaying HABP

After performing the above configuration, you can display and verify your HABP-related configuration by execute the **display** command in any view.

Table 2-3 Display HABP

Operation	Command	Description
Display HABP configuration and status	**display habp**	These commands can be executed in any view.
Display the MAC address table maintained by HABP	**display habp table**	
Display statistics on HABP packets	**display habp traffic**	

Table of Contents

Chapter 1 AAA & RADIUS & HWTACACS Configuration 1-1
1.1 Overview 1-1
1.1.1 Introduction to AAA 1-1
1.1.2 Introduction to ISP Domain 1-2
1.1.3 Introduction to RADIUS 1-2
1.1.4 Introduction to HWTACACS 1-7
1.2 Configuration Task 1-11
1.3 AAA Configuration 1-13
1.3.1 Configuration Prerequisites 1-13
1.3.2 Creating an ISP Domain 1-14
1.3.3 Configuring the Attributes of an ISP Domain 1-14
1.3.4 Configuring an AAA Scheme for an ISP Domain 1-15
1.3.5 Configuring Dynamic VLAN Assignment 1-18
1.3.6 Configuring the Attributes of a Local User 1-20
1.3.7 Cutting Down User Connections Forcibly 1-22
1.4 RADIUS Configuration 1-22
1.4.1 Creating a RADIUS Scheme 1-23
1.4.2 Configuring RADIUS Authentication/Authorization Servers 1-24
1.4.3 Configuring RADIUS Accounting Servers 1-25
1.4.4 Configuring Shared Keys for RADIUS Messages 1-26
1.4.5 Configuring Maximum Number of Transmission Attempts of RADIUS Request 1-27
1.4.6 Configuring to Support a Type of RADIUS Server 1-28
1.4.7 Configuring the Status of RADIUS Servers 1-28
1.4.8 Configuring the Attributes for Data to be Sent to RADIUS Servers 1-29
1.4.9 Configuring Local RADIUS Authentication Server 1-30
1.4.10 Configuring the Timers of RADIUS Servers 1-31
1.4.11 Enabling the Sending of Trap Message When a RADIUS Server is Down 1-32
1.4.12 Enabling the User Re-Authentication at Restart Function 1-33
1.5 HWTACACS Configuration 1-34
1.5.1 Creating a HWTACAS Scheme 1-34
1.5.2 Configuring HWTACACS Authentication Servers 1-35
1.5.3 Configuring HWTACACS Authorization Servers 1-36
1.5.4 Configuring HWTACACS Accounting Servers 1-37
1.5.5 Configuring Shared Keys for HWTACACS Messages 1-37
1.5.6 Configuring the Attributes for Data to be Sent to TACACS Servers 1-38
1.5.7 Configuring the Timers of TACACS Servers 1-39
1.6 Displaying and Maintaining AAA & RADIUS & HWTACACS Information 1-40
1.7 AAA & RADIUS & HWTACACS Configuration Example 1-42

1.7.1 Remote RADIUS Authentication of Telnet/SSH Users 1-42
1.7.2 Local Authentication of FTP/Telnet Users 1-44
1.7.3 HWTACACS Authentication and Authorization of Telnet Users 1-45
1.8 Troubleshooting AAA & RADIUS & HWTACACS Configuration 1-46
1.8.1 Troubleshooting RADIUS Configuration 1-46
1.8.2 Troubleshooting HWTACACS Configuration 1-47

Chapter 2 EAD Configuration 2-1
2.1 Introduction to EAD 2-1
2.2 Typical Network Application of EAD 2-1
2.3 EAD Configuration 2-2
2.4 EAD Configuration Example 2-3

Chapter 1 AAA & RADIUS & HWTACACS Configuration

1.1 Overview

1.1.1 Introduction to AAA

AAA is an acronym for the three security functions: authentication, authorization and accounting. It provides a uniform framework for you to configure the three security functions to implement network security management.

The network security mentioned here mainly refers to access control. It mainly controls:

- Which users can access the network,
- Which services are available to the users who can access the network, and
- How to charge the users who are using network resources.

Accordingly, AAA provides the following three functions:

I. Authentication

AAA supports the following authentication methods:

- None authentication: Users are trusted and are not checked for their validity. Generally, this method is not recommended.
- Local authentication: User information (including user name, password, and some other attributes) is configured on this device, and users are authenticated on this device instead of on a remote device. Local authentication is fast and requires lower operational cost, but has the deficiency that information storage capacity is limited by device hardware.
- Remote authentication: Users are authenticated remotely through RADIUS or HWTACACS protocol. This device (for example, a H3C series switch) acts as the client to communicate with the RADIUS or TACACS server. For RADIUS protocol, you can use extended RADIUS protocol as well as standard RADIUS protocol.

II. Authorization

AAA supports the following authorization methods:

- Direct authorization: Users are trusted and directly authorized.
- Local authorization: Users are authorized according to the related attributes configured for their local accounts on this device.
- RADIUS authorization: Users are authorized after they pass RADIUS authentication. In RADIUS protocol, authentication and authorization are

combined together, and authorization cannot be performed alone without authentication.

- HWTACACS authorization: Users are authorized by a TACACS server.

III. Accounting

AAA supports the following accounting methods:

- None accounting: No accounting is performed for users.
- Remote accounting: User accounting is performed on a remote RADIUS or TACACS server.

Generally, AAA adopts client/server structure, where the client acts as the managed resource and the server stores user information. This structure has good scalability and facilitates the centralized management of user information.

1.1.2 Introduction to ISP Domain

An Internet service provider (ISP) domain is a group of users who belong to the same ISP. For a user name in the format of userid@isp-name, the isp-name following the "@" character is the ISP domain name. The access device uses userid as the user name for authentication, and isp-name as the domain name.

In a multi-ISP environment, the users connected to the same access device may belong to different domains. Since the users of different ISPs may have different attributes (such as different forms of user name and password, different service types/access rights), it is necessary to distinguish the users by setting ISP domains.

You can configure a set of ISP domain attributes (including AAA policy, RADIUS scheme, and so on) for each ISP domain independently in ISP domain view.

1.1.3 Introduction to RADIUS

AAA is a management framework. It can be implemented by not only one protocol. But in practice, the most commonly used protocol for AAA is RADIUS.

I. What is RADIUS

RADIUS (remote authentication dial-in user service) is a distributed information exchange protocol based on client/server structure. It can prevent unauthorized access to your network and is commonly used in network environments where both high security and remote user access service are required.

The RADIUS service involves three components:

- Protocol: Based on the UDP/IP layer, RFC 2865 and 2866 define the message format and message transfer mechanism of RADIUS, and define 1812 as the authentication port and 1813 as the accounting port.

- Server: RADIUS Server runs on a computer or workstation at the center. It stores and maintains user authentication information and network service access information.
- Client: RADIUS Client runs on dial-in access server devices throughout the network.

RADIUS is based on client/server model. A switch acting as a RADIUS client passes user information to a specified RADIUS server, and takes appropriate action (such as establishing/terminating user connection) depending on the responses returned from the server. The RADIUS server receives user connection requests, authenticates users, and returns all required information to the switch.

Generally, a RADIUS server maintains the following three databases (see Figure 1-1):

- Users: This database stores information about users (such as user name, password, protocol adopted and IP address).
- Clients: This database stores information about RADIUS clients (such as shared key).
- Dictionary: The information stored in this database is used to interpret the attributes and attribute values in the RADIUS protocol.

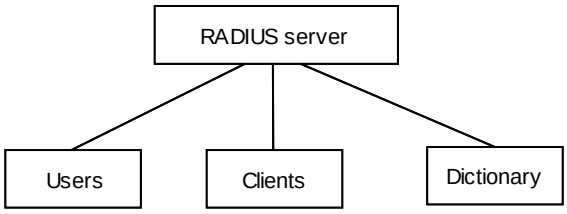


Figure 1-1 Databases in a RADIUS server

In addition, a RADIUS server can act as a client of some other AAA server to provide authentication or accounting proxy service.

II. Basic message exchange procedure in RADIUS

The messages exchanged between a RADIUS client (a switch, for example) and a RADIUS server are verified through a shared key. This enhances the security. The RADIUS protocol combines the authentication and authorization processes together by sending authorization information along with the authentication response message. Figure 1-2 depicts the message exchange procedure between user, switch and RADIUS server.

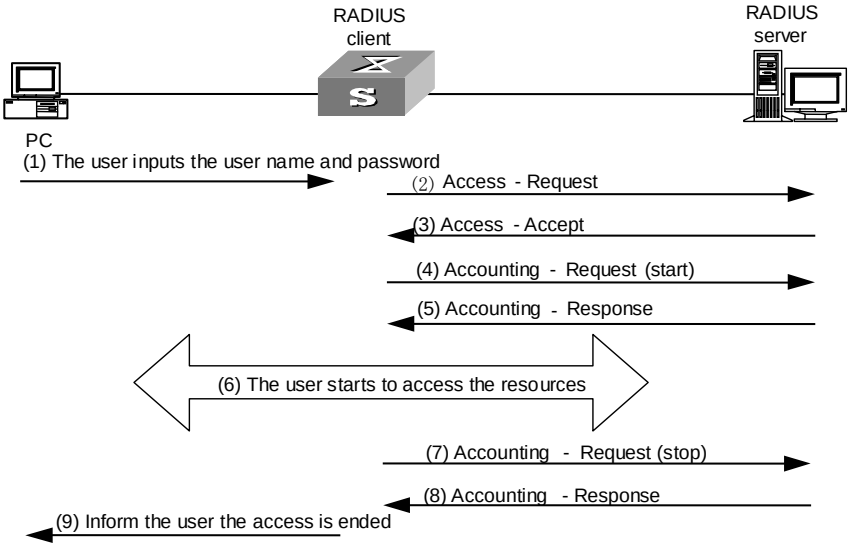


Figure 1-2 Basic message exchange procedure of RADIUS

The basic message exchange procedure of RADIUS is as follows:

1) The user enters the user name and password.
2) The RADIUS client receives the user name and password, and then sends an authentication request (Access-Request) to the RADIUS server.
3) The RADIUS server compares the received user information with that in the Users database to authenticate the user. If the authentication succeeds, the RADIUS server sends back to the RADIUS client an authentication response (Access-Accept), which contains the user's access right information. If the authentication fails, the server returns an Access-Reject response.
4) The RADIUS client accepts or denies the user depending on the received authentication result. If it accepts the user, the RADIUS client sends a start-accounting request (Accounting-Request, with the Status-Type attribute value = start) to the RADIUS server.
5) The RADIUS server returns a start-accounting response (Accounting-Response).
6) The user starts to access network resources.
7) The RADIUS client sends a stop-accounting request (Accounting-Request, with the Status-Type attribute value = stop) to the RADIUS server.
8) The RADIUS server returns a stop-accounting response (Accounting-Response).
9) The access to network resources is ended.

III. RADIUS message format

RADIUS messages are transported over UDP, which does not guarantee reliable delivery of messages between RADIUS server and client. As a remedy, RADIUS adopts the following mechanisms: timer management, retransmission, and backup server. Figure 1-3 depicts the format of RADIUS messages.

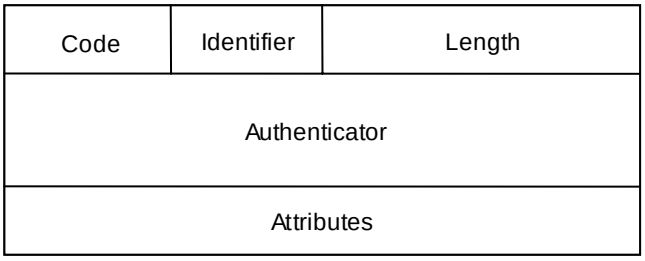


Figure 1-3 RADIUS message format

1) The Code field (one byte) decides the type of RADIUS message, as shown in Table 1-1.

Table 1-1 Description on the major values of the Code field

Code	Message type	Message description
1	Access-Request	Direction: client->server. The client transmits this message to the server to determine if the user can access the network. This message carries user information. It must contain the User-Name attribute and may contain the following attributes: NAS-IP-Address, User-Password and NAS-Port.
2	Access-Accept	Direction: server->client. The server transmits this message to the client if all the attribute values carried in the Access-Request message are acceptable (that is, the user passes the authentication).
3	Access-Reject	Direction: server->client. The server transmits this message to the client if any attribute value carried in the Access-Request message is unacceptable (that is, the user fails the authentication).
4	Accounting-Request	Direction: client->server. The client transmits this message to the server to request the server to start or end the accounting (whether to start or to end the accounting is determined by the Acct-Status-Type attribute in the message). This message carries almost the same attributes as those carried in the Access-Request message.
5	Accounting-Response	Direction: server->client. The server transmits this message to the client to notify the client that it has received the Accounting-Request message and has correctly recorded the accounting information.

2) The Identifier field (one byte) is used to match requests and responses. It changes whenever the content of the Attributes field change, and whenever a valid response has been received for a previous request, but remains unchanged for message retransmission.
3) The Length field (two bytes) specifies the total length of the message (including the Code, Identifier, Length, Authenticator and Attributes fields). The bytes beyond the length are regarded as padding and are ignored upon reception. If a received message is shorter than what the Length field indicates, it is discarded.
4) The Authenticator field (16 bytes) is used to authenticate the response from the RADIUS server; and is used in the password hiding algorithm. There are two kinds of authenticators: Request Authenticator and Response Authenticator.
5) The Attributes field contains specific authentication/authorization/accounting information to provide the configuration details of a request or response message. This field contains a list of field triplet (Type, Length and Value):

- The Type field (one byte) specifies the type of an attribute. Its value ranges from 1 to 255. Table 1-2 lists the attributes that are commonly used in RADIUS authentication/authorization.
- The Length field (one byte) specifies the total length of the attribute in bytes (including the Type, Length and Value fields).
- The Value field (up to 253 bytes) contains the information of the attribute. Its format is determined by the Type and Length fields.

Table 1-2 RADIUS attributes

Type field value	Attribute type	Type field value	Attribute type
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-ID	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group

Type field value	Attribute type	Type field value	Attribute type
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-ID	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

The RADIUS protocol has good scalability. Attribute 26 (Vender-Specific) defined in this protocol allows a device vendor to extend RADIUS to implement functions that are not defined in standard RADIUS.

Figure 1-4 depicts the format of attribute 26. The Vendor-ID field used to identify a vendor occupies four bytes, where the first byte is 0, and the other three bytes are defined in RFC 1700. Here, the vendor can encapsulate multiple customized sub-attributes (containing vendor-specific Type, Length and Value) to implement a RADIUS extension.

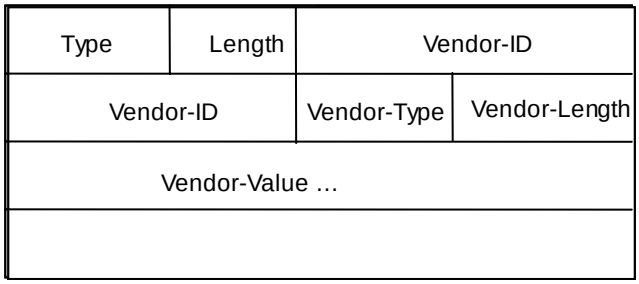


Figure 1-4 Vendor-specific attribute format

1.1.4 Introduction to HWTACACS

I. What is HWTACACS

HWTACACS (Huawei terminal access controller access control system) is an enhanced security protocol based on TACACS (RFC 1492). Similar to the RADIUS protocol, it implements AAA for different types of users (such as PPP, VPDN, and terminal users) through communicating with TACACS server in client-server mode.

Compared with RADIUS, HWTACACS provides more reliable transmission and encryption, and therefore is more suitable for security control. Table 1-3 lists the primary differences between HWTACACS and RADIUS.

Table 1-3 Differences between HWTACACS and RADIUS

HWTACACS	RADIUS
Adopts TCP, providing more reliable network transmission.	Adopts UDP.
Encrypts the entire message except the HWTACACS header.	Encrypts only the password field in authentication message.
Separates authentication from authorization. For example, you can use one TACACS server for authentication and another TACACS server for authorization.	Combines authentication and authorization.
Is more suitable for security control.	Is more suitable for accounting.
Supports configuration command authorization.	Does not support.

In a typical HWTACACS application (as shown in Figure 1-5), a dial-up or terminal user needs to log into the switch to perform some operations. As a HWTACACS client, the switch sends the username and password to the TACACS server for authentication. After passing authentication and being authorized, the user successfully logs into the switch to perform operations.

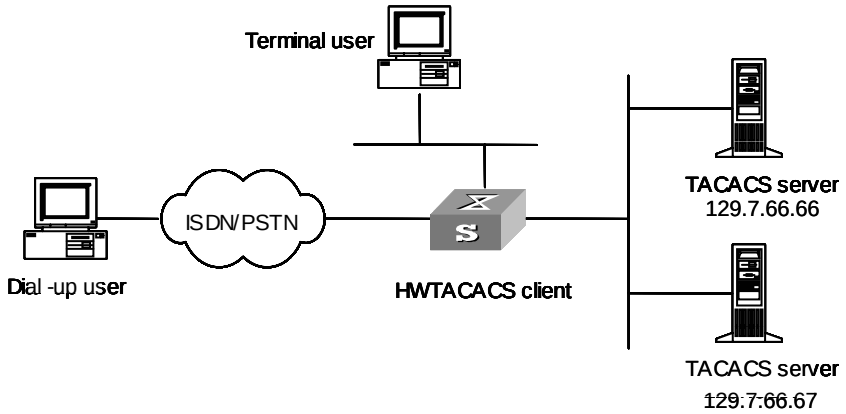


Figure 1-5 Network diagram for a typical HWTACACS application

II. Basic message exchange procedure in HWTACACS

The following text takes telnet user as an example to describe how HWTACACS implements authentication, authorization, and accounting for a user. Figure 1-6 illustrates the basic message exchange procedure:

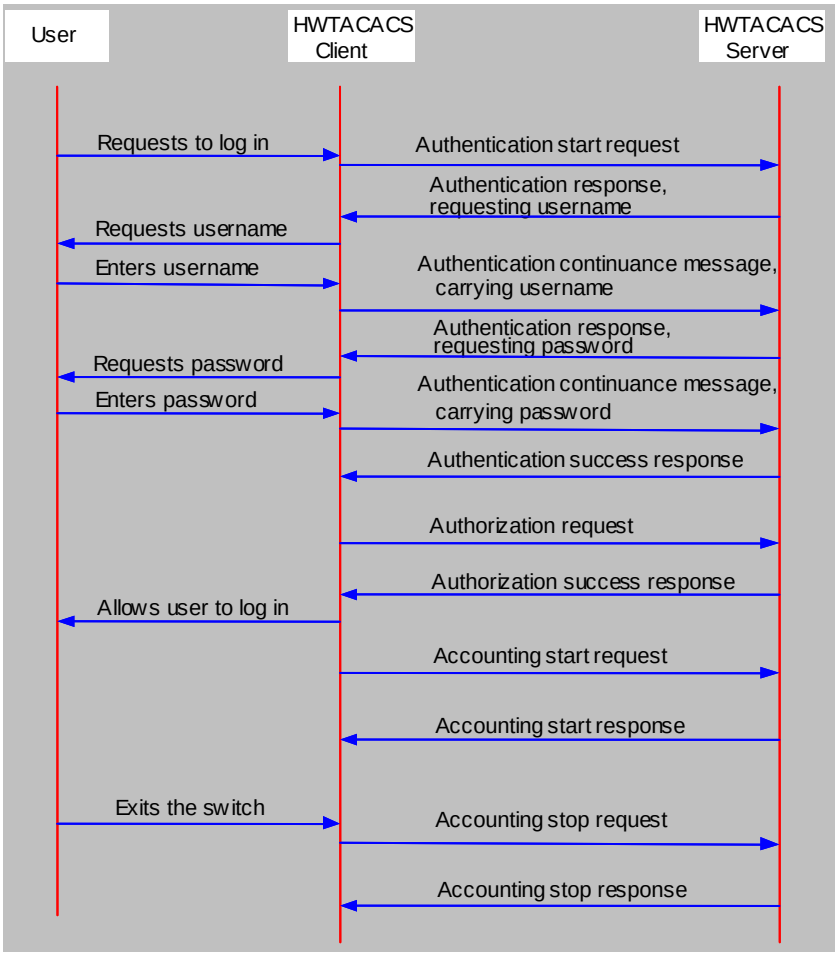


Figure 1-6 AAA implementation procedure for a telnet user

The basic message exchange procedure is as follows:

1) A user sends a login request to the switch acting as a TACACS client, which then sends an authentication start request to the TACACS.
2) The TACACS server returns an authentication response, asking for the username. Upon receiving the response, the TACACS client requests the user for the username.
3) After receiving the username from the user, the TACACS client sends an authentication continuance message carrying the username.
4) The TACACS server returns an authentication response, asking for the password. Upon receiving the response, the TACACS client requests the user for the login password.
5) After receiving the password, the TACACS client sends an authentication continuance message carrying the password to the TACACS server.
6) The TACACS server returns an authentication response, indicating that the user has passed the authentication.
7) The TACACS client sends a user authorization request to the TACACS server.

8) The TACACS server returns an authorization response, indicating that the user has passed the authorization.
9) After receiving the response indicating an authorization success, the TACACS client pushes the configuration interface of the switch to the user.
10) The TACACS client sends an accounting start request to the TACACS server.
11) The TACACS server returns an accounting response, indicating that it has received the accounting start request.
12) The user logs out; the TACACS client sends an accounting stop request to the TACACS server.
13) The TACACS server returns an accounting response, indicating that it has received the accounting stop request.

1.2 Configuration Task

Table 1-4 Configuration tasks

Configuration task		Description	Related section
AAA configuration	Creating an ISP domain	Required	Section 1.3.2 “Creating an ISP Domain”
	Configuring the attributes of an ISP domain	Optional	Section 1.3.3 “Configuring the Attributes of an ISP Domain”
	Configuring an AAA scheme for an ISP domain	Required If local authentication is adopted, refer to section 1.3.6 “Configuring the Attributes of a Local User”. If RADIUS authentication is adopted, refer to section 1.4 “RADIUS Configuration”.	Section 1.3.4 “Configuring an AAA Scheme for an ISP Domain”
	Configuring dynamic VLAN assignment	Optional	Section 1.3.5 “Configuring Dynamic VLAN Assignment”
	Configuring the attributes of a local user	Optional	Section 1.3.6 “Configuring the Attributes of a Local User”
	Cutting down user connections forcibly	Optional	Section 1.3.7 “Cutting Down User Connections Forcibly”

Configuration task		Description	Related section
RADIUS configuration	Creating a RADIUS scheme	Required	Section 1.4.1 “Creating a RADIUS Scheme”
	Configuring RADIUS authentication/authorization servers	Required	Section 1.4.2 “Configuring RADIUS Authentication/Authorization Servers”
	Configuring RADIUS accounting servers	Required	Section 1.4.3 “Configuring RADIUS Accounting Servers”
	Configuring shared keys for RADIUS messages	Optional	Section 1.4.4 “Configuring Shared Keys for RADIUS Messages”
	Configuring the maximum number of transmission attempts of a RADIUS request	Optional	Section 1.4.5 “Configuring Maximum Number of Transmission Attempts of RADIUS Request”
	Configuring to support a type of RADIUS server	Optional	Section 1.4.6 “Configuring to Support a Type of RADIUS Server”
	Configuring the status of RADIUS servers	Optional	Section 1.4.7 “Configuring the Status of RADIUS Servers”
	Configuring the attributes for data to be sent to RADIUS servers	Optional	Section 1.4.8 “Configuring the Attributes for Data to be Sent to RADIUS Servers”
	Configuring local RADIUS authentication server	Optional	Section 1.4.9 “Configuring Local RADIUS Authentication Server”
	Configuring the timers of RADIUS servers	Optional	Section 1.4.10 “Configuring the Timers of RADIUS Servers”
	Enabling the sending of trap message when a RADIUS server is down	Optional	Section 1.4.11 “Enabling the Sending of Trap Message When a RADIUS Server is Down”
	Enabling the user re-authentication at restart function	Optional	Section 1.4.12 “Enabling the User Re-Authentication at Restart Function”

Configuration task		Description	Related section
HWTACACS configuration	Creating a HWTACAS scheme	Required	Section 1.5.1 “Creating a HWTACAS Scheme”
	Configuring HWTACACS authentication servers	Required	Section 1.5.2 “Configuring HWTACACS Authentication Servers”
	Configuring HWTACACS authorization servers	Required	Section 1.5.3 “Configuring HWTACACS Authorization Servers”
	Configuring HWTACACS accounting servers	Optional	Section 1.5.4 “Configuring HWTACACS Accounting Servers”
	Configuring shared keys for HWTACACS messages	Optional	Section 1.5.5 “Configuring Shared Keys for HWTACACS Messages”
	Configuring the attributes for data to be sent to TACACS servers	Optional	Section 1.5.6 “Configuring the Attributes for Data to be Sent to TACACS Servers”
	Configuring the timers of TACACS servers	Optional	Section 1.5.7 “Configuring the Timers of TACACS Servers”

1.3 AAA Configuration

The purpose of AAA configuration is to provide network access services to legal users and at the same time protect your network device against unauthorized access. If you need to use ISP domains to implement AAA management on access users, you should first configure ISP domains.

1.3.1 Configuration Prerequisites

If you want to adopt remote AAA method, you must first create a RADIUS or HWTACACS scheme.

- RADIUS scheme (**radius-scheme**): You can reference a configured RADIUS scheme to provide AAA services. For the configuration of RADIUS scheme, refer to section 1.4 "RADIUS Configuration".
- HWTACACS scheme (**hwtacacs-scheme**): You can reference a configured HWTACACS scheme to implement AAA services. For the configuration of HWTACACS scheme, refer to section 1.5 "HWTACACS Configuration".

1.3.2 Creating an ISP Domain

Table 1-5 Create an ISP domain

Operation	Command	Description
Enter system view	**system-view**	—
Create an ISP domain and enter its view, enter the view of an existing ISP domain, or set an ISP domain as the default ISP domain	**domain** { *isp-name* | **default** { **disable** | **enable** *isp-name* } }	Required If no ISP domain is set as the default ISP domain, the ISP domain "system" is used as the default ISP domain.

1.3.3 Configuring the Attributes of an ISP Domain

Table 1-6 Configure the attributes of an ISP domain

Operation	Command	Description
Enter system view	**system-view**	—
Create an ISP domain and enter its view, or enter the view of an existing ISP domain	**domain** *isp-name*	Required
Set the status of the ISP domain	**state** { **active** | **block** }	Optional By default, an ISP domain is in the **active** state, that is, all the users in the domain are allowed to request network service.
Set the maximum number of access users that can be contained in the ISP domain	**access-limit** { **disable** | **enable** *max-user-number* }	Optional By default, there is no limit on the number of access users that can be contained in an ISP domain.
Set the user idle-cut function	**idle-cut** { **disable** | **enable** *minute flow* }	Optional By default, the user idle-cut function is disabled.
Set the accounting-optional switch	**accounting optional**	Optional By default, the accounting-optional switch is closed.

Operation	Command	Description
Set the messenger function	**messenger time** { **enable** *limit interval* | **disable** }	Optional By default, the messenger function is disabled.
Set the self-service server location function	**self-service-url** { **disable** | **enable** *url-string* }	Optional By default, the self-service server location function is disabled.

Caution:

- On an S3600 series switch, each access user belongs to an ISP domain. You can configure up to 16 ISP domains on the switch. When a user logs in, if no ISP domain name is carried in the user name, the switch assumes that the user belongs to the default ISP domain.
- If the system does not find any available accounting server or fails to communicate with any accounting server when it performs accounting for a user, it will not disconnect the user as long as the **accounting optional** command has been executed, though it cannot perform accounting for the user in this case.
- The self-service server location function needs the cooperation of a self-service-supported RADIUS server (such as CAMS, that is, comprehensive access management server). Through self-service, users can manage and control their account or card numbers by themselves. A server installed with the self-service software is called a self-service server.

Note:

H3C's CAMS Server is a service management system used to manage networks and secure networks and user information. With the cooperation of other networking devices (such as switches) in a network, a CAMS server can implement the AAA functions and right management.

1.3.4 Configuring an AAA Scheme for an ISP Domain

You can configure an AAA scheme in one of the following two ways:

I. Configuring a combined AAA scheme

You can use the **scheme** command to specify an AAA scheme for an ISP domain. If you specify a RADIUS or HWTACACS scheme, the authentication, authorization and accounting will be uniformly implemented by the RADIUS or TACACS server(s) specified in the RADIUS or HWTACACS scheme. In this way, you cannot specify different schemes for authentication, authorization and accounting respectively.

Table 1-7 Configure a combined AAA scheme

Operation	Command	Description
Enter system view	**system-view**	—
Create an ISP domain and enter its view, or enter the view of an existing ISP domain	**domain** *isp-name*	Required
Configure an AAA scheme for the ISP domain	**scheme** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] }	Required By default, an ISP domain uses the **local** AAA scheme.
Configure an RADIUS scheme for the ISP domain	**radius-scheme** *radius-scheme-name*	Optional This command has the same function as the **scheme radius-scheme** command.

Caution:

- You can execute the **scheme radius-scheme** *radius-scheme-name* command to adopt an already configured RADIUS scheme to implement all the three AAA functions. If you adopt the local scheme, only the authentication and authorization functions are implemented, the accounting function cannot be implemented.
- If you execute the **scheme radius-scheme** *radius-scheme-name* **local** command, the local scheme is used as the secondary scheme in case no RADIUS server is available. That is, if the communication between the switch and a RADIUS server is normal, no local authentication is performed; otherwise, local authentication is performed.
- If you execute the **scheme hwtacacs-scheme** *hwtacacs-scheme-name* **local** command, the local scheme is used as the secondary scheme in case no TACACS server is available. That is, if the communication between the switch and a TACACS server is normal, no local authentication is performed; otherwise, local authentication is performed.
- If you execute the **scheme local** or **scheme none** command to adopt **local** or **none** as the primary scheme, the local authentication is performed or no authentication is performed. In this case you cannot specify any RADIUS scheme at the same time.

II. Configuring separate AAA schemes

You can use the **authentication**, **authorization**, and **accounting** commands to specify a scheme for each of the three AAA functions (authentication, authorization and accounting) respectively. The following gives the implementations of this separate way for the services supported by AAA.

- For terminal users

Authentication: RADIUS, local, HWTACACS or none.

Authorization: none or HWTACACS.

Accounting: RADIUS, HWTACACS or none.

You can use an arbitrary combination of the above implementations for your AAA scheme configuration.

- For FTP users

Only authentication is supported for FTP users.

Authentication: RADIUS, local, or RADIUS-local.

Perform the following configuration in ISP domain view.

Table 1-8 Configure separate AAA schemes

Operation	Command	Description
Enter system view	**system-view**	—
Create an ISP domain and enter its view, or enter the view of an existing ISP domain	**domain** *isp-name*	Required
Configure an authentication scheme for the ISP domain	**authentication** { **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** }	Optional By default, no separate authentication scheme is configured.
Configure an authorization scheme for the ISP domain	**authorization** { **none** | **hwtacacs-scheme** *hwtacacs-scheme-name* }	Optional By default, no separate authorization scheme is configured.
Configure an accounting scheme for the ISP domain	**accounting** { **none** | **radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name* }	Optional By default, no separate accounting scheme is configured.

Note:

- If a combined AAA scheme is configured as well as the separate authentication, authorization and accounting schemes, the separate ones will be adopted in precedence.
- RADIUS scheme and local scheme do not support the separation of authentication and authorization. Therefore, pay attention when you make authentication and authorization configuration for a domain: When the **scheme radius-scheme** or **scheme local** command is executed and the **authentication** command is not executed, the authorization information returned from the RADIUS or local scheme still takes effect even if the **authorization none** command is executed.

1.3.5 Configuring Dynamic VLAN Assignment

The dynamic VLAN assignment feature enables a switch to dynamically add the switch ports of successfully authenticated users to different VLANs according to the attributes assigned by the RADIUS server, so as to control the network resources that different users can access.

Currently, the switch supports the following two types of assigned VLAN IDs: integer and string.

- Integer: If the RADIUS authentication server assigns integer type of VLAN IDs, you can set the VLAN assignment mode to integer on the switch (this is also the default mode on the switch). Then, upon receiving an integer ID assigned by the RADIUS authentication server, the switch adds the port to the VLAN whose VLAN ID is equal to the assigned integer ID. If no such a VLAN exists, the switch first creates a VLAN with the assigned ID, and then adds the port to the newly created VLAN.
- String: If the RADIUS authentication server assigns string type of VLAN IDs, you can set the VLAN assignment mode to string on the switch. Then, upon receiving a string ID assigned by the RADIUS authentication server, the switch compares the ID with existing VLAN names on the switch. If it finds a match, it adds the port to the corresponding VLAN. Otherwise, the VLAN assignment fails and the user fails the authentication.

In actual applications, to use this feature together with Guest VLAN, you should better set port control to port-based mode.

Table 1-9 Configure dynamic VLAN assignment

Operation	Command	Description
Enter system view	**system-view**	—
Create an ISP domain and enter its view	**domain** *isp-name*	—
Set the VLAN assignment mode	**vlan-assignment-mode** { **integer** | **string** }	Optional By default, the VLAN assignment mode is integer.
Create a VLAN and enter its view	**vlan** *vlan-id*	—
Set a VLAN name for VLAN assignment	**name** *string*	This operation is required if the VLAN assignment mode is set to string.

Caution:

- In string mode, if the VLAN ID assigned by the RADIUS server is a character string containing only digits (for example, 1024), the switch first regards it as an integer VLAN ID: the switch transforms the string to an integer value and judges if the value is in the valid VLAN ID range; if it is, the switch adds the authenticated port to the VLAN with the integer value as the VLAN ID (VLAN 1024, for example).
- To implement dynamic VLAN assignment on a port where both MSTP and 802.1x are enabled, you must set the MSTP port to an edge port.

1.3.6 Configuring the Attributes of a Local User

When **local** scheme is chosen as the AAA scheme, you should create local users on the switch and configure the relevant attributes.

The local users are users set on the switch, with each user uniquely identified by a user name. To make a user who is requesting network service pass local authentication, you should add an entry in the local user database on the switch for the user.

Table 1-10 Configure the attributes of a local user

Operation	Command	Description
Enter system view	**system-view**	—
Set the password display mode of all local users	**local-user password-display-mode** { **cipher-force** | **auto** }	Optional By default, the password display mode of all access users is **auto**, indicating the passwords of access users are displayed in the modes set by the **password** command.
Add a local user and enter local user view	**local-user** *user-name*	Required By default, there is no local user in the system.
Set a password for the local user	**password** { **simple** | **cipher** } *password*	Optional
Set the status of the local user	**state** { **active** | **block** }	Optional By default, the user is in **active** state, that is, the user is allowed to request network services.

Operation	Command	Description
Authorize the user to access specified type(s) of service	**service-type** { **ftp** | **lan-access** | { **telnet** | **ssh** | **terminal** }* [**level** *level*] }	Required By default, the system does not authorize the user to access any service.
Set the privilege level of the user	**level** *level*	Optional By default, the privilege level of the user is 0.
Set the attributes of the user whose service type is lan-access	**attribute** { **ip** *ip-address* | **mac** *mac-address* | **idle-cut** *second* | **access-limit** *max-user-number* | **vlan** *vlan-id* | **location** { **nas-ip** *ip-address* **port** *port-number* | **port** *port-number* } }*	Optional When binding the user to a remote port, you must use **nas-ip** *ip-address* to specify a remote access server IP address (here, *ip-address* is 127.0.0.1 by default, representing this device). When binding the user to a local port, you need not use **nas-ip** *ip-address*.

Caution:

- The following characters are not allowed in the *user-name* string: /:*?<>. And you cannot input more than one "@" in the string.
- After the **local-user password-display-mode cipher-force** command is executed, any password will be displayed in cipher mode even though you specify to display a user password in plain text by using the **password** command.
- If a user name and password is required for user authentication (RADIUS authentication as well as local authentication), the command level that a user can access after login is determined by the privilege level of the user. For SSH users using RSA shared key for authentication, the commands they can access are determined by the levels set on their user interfaces.
- If the configured authentication method is none or password authentication, the command level that a user can access after login is determined by the level of the user interface.

1.3.7 Cutting Down User Connections Forcibly

Table 1-11 Cut down user connections forcibly

Operation	Command	Description
Enter system view	**system-view**	—
Cut down user connections forcibly	**cut connection** { **all** | **access-type** { **dot1x** | **mac-authentication** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlan-id* | **ucibindex** *ucib-index* | **user-name** *user-name* }	Required

Note:

You can use the **display connection** command to view the connections of Telnet users, but you cannot use the **cut connection** command to cut down their connections.

1.4 RADIUS Configuration

The RADIUS protocol configuration is performed on a RADIUS scheme basis. In an actual network environment, you can either use a single RADIUS server or two RADIUS servers (primary and secondary servers with the same configuration but different IP addresses) in a RADIUS scheme. After creating a new RADIUS scheme, you should configure the IP address and UDP port number of each RADIUS server you want to use in this scheme. These RADIUS servers fall into two types: authentication/authorization, and accounting. And for each type of server, you can configure two servers in a RADIUS scheme: primary server and secondary server. A RADIUS scheme has some parameters such as IP addresses of the primary and secondary servers, shared keys, and types of the RADIUS servers.

In an actual network environment, you can configure the above parameters as required. But you should configure at least one authentication/authorization server and one accounting server, and you should keep the RADIUS server port settings on the switch consistent with those on the RADIUS servers.

Note:

Actually, the RADIUS protocol configuration only defines the parameters for information exchange between switch and RADIUS server. To make these parameters take effect, you must reference the RADIUS scheme configured with these parameters in an ISP domain view (refer to section 1.3 "AAA Configuration").

1.4.1 Creating a RADIUS Scheme

The RADIUS protocol configuration is performed on a RADIUS scheme basis. You should first create a RADIUS scheme and enter its view before performing other RADIUS protocol configurations.

Table 1-12 Create a RADIUS scheme

Operation	Command	Description
Enter system view	**system-view**	—
Enable RADIUS authentication and accounting ports	**radius client enable**	Optional By default, RADIUS authentication and accounting ports are enabled.
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.

Caution:

A RADIUS scheme can be referenced by multiple ISP domains simultaneously.

1.4.2 Configuring RADIUS Authentication/Authorization Servers

Table 1-13 Configure RADIUS authentication/authorization servers

Operation	Command	Description
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the IP address and port number of the primary RADIUS authentication/authorization server	**primary authentication** *ip-address* [*port-number*]	Required By default, the IP address and UDP port number of the primary server are 0.0.0.0 and 1812 respectively.
Set the IP address and port number of the secondary RADIUS authentication/authorization server	**secondary authentication** *ip-address* [*port-number*]	Optional By default, the IP address and UDP port number of the secondary server are 0.0.0.0 and 1812 respectively.

Caution:

- The authentication response sent from the RADIUS server to the RADIUS client carries authorization information. Therefore, you need not (and cannot) specify a separate RADIUS authorization server.
- In an actual network environment, you can specify one server as both the primary and secondary authentication/authorization servers, as well as specifying two RADIUS servers as the primary and secondary authentication/authorization servers respectively.
- The IP address and port number of the primary authentication server used by the default RADIUS scheme "system" are 127.0.0.1 and 1645.

1.4.3 Configuring RADIUS Accounting Servers

Table 1-14 Configure RADIUS accounting servers

Operation	Command	Description
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the accounting-optional switch	**accounting optional**	You must select one from the two operations. By default, the accounting-optional switch is closed, that is, accounting is required.
Set the IP address and port number of the primary RADIUS accounting server	**primary accounting** *ip-address* [*port-number*]	By default, the IP address and UDP port number of the primary accounting server are 0.0.0.0 and 1813.
Set the IP address and port number of the secondary RADIUS accounting server	**secondary accounting** *ip-address* [*port-number*]	Optional By default, the IP address and UDP port number of the secondary accounting server are 0.0.0.0 and 1813.
Enable stop-accounting request buffering	**stop-accounting-buffer enable**	Optional By default, stop-accounting request buffering is enabled.
Set the maximum number of transmission attempts of a buffered stop-accounting request.	**retry stop-accounting** *retry-times*	Optional By default, the system tries at most 500 times to transmit a buffered stop-accounting request.
Set the maximum allowed number of continuous real-time accounting failures	**retry realtime-accounting** *retry-times*	Optional By default, the maximum allowed number of continuous real-time accounting failures is five. If five continuous failures occur, the switch cuts down the user connection.

Caution:

- In an actual network environment, you can specify one server as both the primary and secondary accounting servers, as well as specifying two RADIUS servers as the primary and secondary accounting servers respectively. In addition, because RADIUS adopts different UDP ports to exchange authentication/authorization messages and accounting messages, you must set a port number for accounting different from that set for authentication/authorization.
- With stop-accounting request buffering enabled, the switch first buffers the stop-accounting request that gets no response from the RADIUS accounting server, and then retransmits the request to the RADIUS accounting server until it gets a response, or the maximum number of transmission attempts is reached (in this case, it discards the request).
- You can set the maximum allowed number of continuous real-time accounting failures. If the number of continuously failed real-time accounting requests to the RADIUS server reaches the set maximum number, the switch cuts down the user connection.
- The IP address and port number of the primary accounting server of the default RADIUS scheme "system" are 127.0.0.1 and 1646 respectively.
- Currently, RADIUS does not support the accounting of FTP users.

1.4.4 Configuring Shared Keys for RADIUS Messages

Both RADIUS client and server adopt MD5 algorithm to encrypt RADIUS messages before they are exchanged between the two parties. The two parties verify the validity of the RADIUS messages received from each other by using the shared keys that have been set on them, and can accept and respond to the messages only when both parties have the same shared key.

Table 1-15 Configure shared keys for RADIUS messages

Operation	Command	Description
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set a shared key for RADIUS authentication/authorization messages	**key authentication** *string*	Required

Operation	Command	Description
Set a shared key for RADIUS accounting messages	**key accounting** *string*	Required

Caution:

The authentication/authorization shared key and the accounting shared key you set on the switch must be respectively consistent with the shared key on the authentication/authorization server and the shared key on the accounting server.

1.4.5 Configuring Maximum Number of Transmission Attempts of RADIUS Request

The communication in RADIUS is unreliable because this protocol uses UDP packets to carry its data. Therefore, it is necessary for the switch to retransmit a RADIUS request if it gets no response from the RADIUS server after the response timeout timer expires. If the switch gets no answer after it has tried the maximum number of times to transmit the request, the switch considers that the request fails.

Table 1-16 Configure the maximum transmission attempts of a RADIUS request

Operation	Command	Description
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the maximum number of transmission attempts of a RADIUS request	**retry** *retry-times*	Optional By default, the system can try three times to transmit a RADIUS request.

1.4.6 Configuring to Support a Type of RADIUS Server

Table 1-17 Configure to support a type of RADIUS server

Operation	Command	Description
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Configure the switch to support a type of RADIUS server	**server-type** { **extended** | **standard** }	Optional

1.4.7 Configuring the Status of RADIUS Servers

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme:

When the switch fails to communicate with the primary server due to some server trouble, the switch will turn to the secondary server and exchange messages with the secondary server.

After the primary server remains in the block state for a set time (set by the **timer quiet** command), the switch will try to communicate with the primary server again when it receives a RADIUS request. If it finds that the primary server has recovered, the switch immediately restores the communication with the primary server instead of communicating with the secondary server, and at the same time restores the status of the primary server to active while keeping the status of the secondary server unchanged.

When both the primary and secondary servers are in active or block state, the switch sends messages only to the primary server.

Table 1-18 Set the status of RADIUS servers

Operation	Command	Description
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.

Operation	Command	Description
Set the status of the primary RADIUS authentication/authorization server	**state primary authentication** { **block** | **active** }	Optional By default, the primary RADIUS servers in the default RADIUS scheme "system" are in the **active** state, the secondary servers in the scheme are in the **block** state, and all RADIUS servers in all other RADIUS schemes are in the **block** state.
Set the status of the primary RADIUS accounting server	**state primary accounting** { **block** | **active** }	
Set the status of the secondary RADIUS authentication/authorization server	**state secondary authentication** { **block** | **active** }	
Set the status of the secondary RADIUS accounting server	**state secondary accounting** { **block** | **active** }	

1.4.8 Configuring the Attributes for Data to be Sent to RADIUS Servers

Table 1-19 Configure the attributes for data to be sent to RADIUS servers

Operation	Command	Description
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the format of the user names to be sent to RADIUS server	**user-name-format** { **with-domain** | **without-domain** }	Optional By default, the user names sent from the switch to RADIUS server carry ISP domain names.
Set the units of data flows to RADIUS servers	**data-flow-format data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }	Optional By default, in a RADIIUS scheme, the data unit and packet unit for outgoing RADIUS flows are byte and one-packet respectively.

Operation	Command	Description
Set the source IP address of outgoing RADIUS messages	RADIUS scheme view **nas-ip** *ip-address*	Optional By default, no source IP address is set; and the IP address of the corresponding outbound interface is used as the source IP address.
	System view **radius nas-ip** *ip-address*	

Caution:

- Generally, the access users are named in the *userid@isp-name* format. Here, *isp-name* behind the @ character represents the ISP domain name, by which the device determines which ISP domain a user belongs to. However, some old RADIUS servers cannot accept the user names that carry ISP domain names. In this case, it is necessary to remove domain names from user names before sending the user names to RADIUS server. For this reason, the **user-name-format** command is designed for you to specify whether or not ISP domain names are carried in the user names to be sent to RADIUS server.
- For a RADIUS scheme, if you have specified to remove ISP domain names from user names, you should not use this RADIUS scheme in more than one ISP domain. Otherwise, such errors may occur: the RADIUS server regards two different users having the same name but belonging to different ISP domains as the same user (because the usernames sent to it are the same).
- In the default RADIUS scheme "system", ISP domain names are removed from user names by default.

1.4.9 Configuring Local RADIUS Authentication Server

Table 1-20 Configure local RADIUS authentication server

Operation	Command	Description
Enter system view	**system-view**	—
Enable UDP port for local RADIUS authentication server	**local-server enable**	Optional By default, the UDP port for local RADIUS authentication server is enabled.

Operation	Command	Description
Configure local RADIUS authentication server	**local-server nas-ip** *ip-address* **key** *password*	Required By default, local RADIUS authentication server is configured with an NAS IP address of 127.0.0.1.

Caution:

- If you adopt the local RADIUS authentication server function, the UDP port number of the authentication/authorization server must be 1645, the UDP port number of the accounting server must be 1646, and the IP addresses of the servers must be set to the addresses of this switch.
- The message encryption key set by the **local-server nas-ip** *ip-address* **key** *password* command must be identical with the authentication/authorization message encryption key set by the **key authentication** command in the RADIUS scheme view of the RADIUS scheme on the specified NAS that uses this switch as its authentication server.
- Acting as local RADIUS authentication server, the switch can provide authentication service to up to 16 network access servers (NAS) (including the switch itself) at the same time.

1.4.10 Configuring the Timers of RADIUS Servers

After sending out a RADIUS request (authentication/authorization request or accounting request) to a RADIUS server, the switch waits for a response from the server. The maximum time that the switch can wait for the response is called the response timeout time of RADIUS servers, and the corresponding timer in the switch system is called the response timeout timer of RADIUS servers. If the switch gets no answer within the response timeout time, it needs to retransmit the request to ensure that the user can obtain RADIUS service.

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme:

When the switch fails to communicate with the primary server due to some server trouble, the switch will turn to the secondary server and exchange messages with the secondary server.

After the primary server remains in the block state for a specific time (set by the **timer quiet** command), the switch will try to communicate with the primary server again when it has a RADIUS request. If it finds that the primary server has recovered, the switch

immediately restores the communication with the primary server instead of communicating with the secondary server, and at the same time restores the status of the primary server to active while keeping the status of the secondary server unchanged.

To control the interval at which users are charged in real time, you can set the real-time accounting interval. After the setting, the switch periodically sends online users' accounting information to RADIUS server at the set interval.

Table 1-21 Set the timers of RADIUS servers

Operation	Command	Description
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the response timeout time of RADIUS servers	**timer response-timeout** *seconds*	Optional By default, the response timeout time of RADIUS servers is three seconds.
Set the time that the switch waits before it try to re-communicate with primary server and restore the status of the primary server to active	**timer quiet** *minutes*	Optional By default, the switch waits five minutes before it restores the status of the primary server to active.
Set the real-time accounting interval	**timer realtime-accounting** *minutes*	Optional By default, the real-time accounting interval is 12 minutes.

1.4.11 Enabling the Sending of Trap Message When a RADIUS Server is Down

Table 1-22 Enable the sending of trap message when a RADIUS server is down

Operation	Command	Description
Enter system view	**system-view**	—
Enable the sending of trap message when a RADIUS server is down	**radius trap** { **authentication-server-down** | **accounting-server-down** }	Optional By default, the switch does not send trap message when a RADIUS server is down.

Note:

- This configuration takes effect on all RADIUS schemes.
- The switch considers a RADIUS server as being down if it has tried the configured maximum times to send a message to the RADIUS server but does not receive any response.

1.4.12 Enabling the User Re-Authentication at Restart Function

Note:

The user re-authentication at restart function applies to the environment where the RADIUS authentication/authorization and accounting server is CAMS.

In an environment that a CAMS server is used to implement AAA functions, if the switch reboots after an exclusive user (a user whose concurrent online number is set to 1 on the CAMS) gets authenticated and authorized and begins being charged, the switch will give a prompt that the user has already been online when the user re-logs into the network before the CAMS performs online user detection, and the user cannot get authenticated. In this case, the user can access the network again only when the CAMS administrator manually removes the user's online information.

The user re-authentication at restart function is designed to resolve this problem. After this function is enabled, every time the switch restarts:

1) The switch generates an Accounting-On message, which mainly contains the following information: NAS-ID, NAS-IP-address (source IP address), and session ID.
2) The switch sends the Accounting-On message to the CAMS at regular intervals.
3) Once the CAMS receives the Accounting-On message, it sends a response to the switch. At the same time it finds and deletes the original online information of the users who were accessing the network through the switch before the restart according to the information (NAS-ID, NAS-IP-address and session ID) contained in the message, and ends the accounting for the users depending on the last accounting update message.
4) Once the switch receives the response from the CAMS, it stops sending Accounting-On messages.

5) If the switch does not receive any response from the CAMS after it has tried the configured maximum number of times to send the Accounting-On message, it will not send the Accounting-On message any more.

Note:

The switch can automatically generate the main attributes (NAS-ID, NAS-IP-address and session ID) contained in Accounting-On messages. However, you can also manually configure the NAS-IP-address with the **nas-ip** command. If you choose to manually configure the attribute, be sure to configure an appropriate valid IP address. If this attribute is not configured, the switch will automatically choose the IP address of a VLAN interface as the NAS-IP-address.

Table 1-23 Enable the user re-authentication at restart function

Operation	Command	Description
Enter system view	**system-view**	—
Enter RADIUS scheme view	**radius scheme** *radius-scheme-name*	—
Enable the user re-authentication at restart function	**accounting-on enable** [**send** *times* | **interval** *interval*]	By default, this function is disabled. If you use this command without any parameter, the system will try at most 15 times to send an Accounting-On message at the interval of three seconds.

1.5 HWTACACS Configuration

1.5.1 Creating a HWTACAS Scheme

The HWTACACS protocol configuration is performed on a scheme basis. Therefore, you must create a HWTACACS scheme and enter HWTACACS view before performing other configuration tasks.

Table 1-24 Create a HWTACACS scheme

Operation	Command	Description
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.

Caution:

- The system supports up to 16 HWTACACS schemes. You can delete a HWTACACS scheme only when it is not referenced.
- If the Fabric function is enabled on the switch, you cannot create any HWTACACS scheme, because the two are exclusive to each other.

1.5.2 Configuring HWTACACS Authentication Servers

Table 1-25 Configure HWTACACS authentication servers

Operation	Command	Description
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the IP address and port number of the primary TACACS authentication server	**primary authentication** *ip-address* [*port*]	Required By default, the IP address of the primary authentication server is 0.0.0.0, and the port number is 0.
Set the IP address and port number of the secondary TACACS authentication server	**secondary authentication** *ip-address* [*port*]	Required By default, the IP address of the secondary authentication server is 0.0.0.0, and the port number is 0.

Caution:

- You are not allowed to configure the same IP address for both primary and secondary authentication servers. If you do this, the system will prompt that the configuration fails.
- You can remove an authentication server setting only when there is no active TCP connection that is sending authentication messages to the server.

1.5.3 Configuring HWTACACS Authorization Servers

Table 1-26 Configure TACACS authorization servers

Operation	Command	Description
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the IP address and port number of the primary TACACS authorization server	**primary authorization** *ip-address* [*port*]	Required By default, the IP address of the primary authorization server is 0.0.0.0, and the port number is 0.
Set the IP address and port number of the secondary TACACS authorization server	**secondary authorization** *ip-address* [*port*]	Required By default, the IP address of the secondary authorization server is 0.0.0.0, and the port number is 0.

Caution:

- You are not allowed to configure the same IP address for both primary and secondary authorization servers. If you do this, the system will prompt that the configuration fails.
- You can remove a server only when it is not used by any active TCP connection for sending authorization messages.

1.5.4 Configuring HWTACACS Accounting Servers

Table 1-27 Configure HWTACACS accounting servers

Operation	Command	Description
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the IP address and port number of the primary TACACS accounting server	**primary accounting** *ip-address* [*port*]	Required By default, the IP address of the primary accounting server is 0.0.0.0, and the port number is 0.
Set the IP address and port number of the secondary TACACS accounting server	**secondary accounting** *ip-address* [*port*]	Required By default, the IP address of the secondary accounting server is 0.0.0.0, and the port number is 0.
Enable the stop-accounting message retransmission function and set the maximum number of transmission attempts of a buffered stop-accounting message	**retry stop-accounting** *retry-times*	Optional By default, the stop-accounting messages retransmission function is enabled and the system can transmit a buffered stop-accounting request for 100 times.

Caution:

- You are not allowed to configure the same IP address for both primary and secondary accounting servers. If you do this, the system will prompt that the configuration fails.
- You can remove a server only when it is not used by any active TCP connection for sending accounting messages.

1.5.5 Configuring Shared Keys for HWTACACS Messages

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.

The TACACS client and server adopt MD5 algorithm to encrypt HWTACACS messages before they are exchanged between the two parties. The two parties verify the validity of the HWTACACS messages received from each other by using the shared keys that have been set on them, and can accept and respond to the messages only when both parties have the same shared key.

Table 1-28 Configure shared keys for HWTACACS messages

Operation	Command	Description
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set a shared key for HWTACACS authentication, authorization or accounting messages	**key** { **accounting** | **authorization** | **authentication** } *string*	Required By default, no such key is set.

1.5.6 Configuring the Attributes for Data to be Sent to TACACS Servers

Table 1-29 Configure the attributes for data to be sent to TACACS servers

Operation	Command	Description
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the format of the user names to be sent to TACACS server	**user-name-format** { **with-domain** | **without-domain** }	Optional By default, the user names sent from the switch to TACACS server carry ISP domain names.
Set the units of data flows to TACACS servers	**data-flow-format data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** }	Optional By default, in a TACACS scheme, the data unit and packet unit for outgoing HWTACACS flows are byte and one-packet respectively.
	data-flow-format packet { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }	

Operation	Command	Description
Set the source IP address of outgoing HWTACACS messages	HWTACACS scheme view **nas-ip** *ip-address*	Optional By default, no source IP address is set; the IP address of the corresponding outbound interface is used as the source IP address.
	System view **hwtacacs nas-ip** *ip-address*	

Caution:

Generally, the access users are named in the *userid@isp-name* format. Where, *isp-name* behind the @ character represents the ISP domain name. If the TACACS server does not accept the user names that carry ISP domain names, it is necessary to remove domain names from user names before they are sent to TACACS server.

1.5.7 Configuring the Timers of TACACS Servers

Table 1-30 Configure the timers of TACACS servers

Operation	Command	Description
Enter system view	**system-view**	—
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the response timeout time of TACACS servers	**timer response-timeout** *seconds*	Optional By default, the response timeout time is five seconds.
Set the time that the switch must wait before it can restore the status of the primary server to active	**timer quiet** *minutes*	Optional By default, the switch must wait five minutes before it can restore the status of the primary server to active.
Set the real-time accounting interval	**timer realtime-accounting** *minutes*	Optional By default, the real-time accounting interval is 12 minutes.

Caution:

- To control the interval at which users are charge in real time, you can set the real-time accounting interval. After the setting, the switch periodically sends online users' accounting information to the TACACS server at the set interval.
- The real-time accounting interval must be a multiple of 3.
- The setting of real-time accounting interval somewhat depends on the performance of the TACACS client and server devices: A shorter interval requires higher device performance.

1.6 Displaying and Maintaining AAA & RADIUS & HWTACACS Information

After the above configurations, you can execute the **display** commands in any view to view the configuration result and operation status of AAA, RADIUS and HWTACACS and verify your configuration.

You can use the **reset** command in user view to clear the corresponding statistics.

Table 1-31 Display AAA information

Operation	Command	Description
Display configuration information about one specific or all ISP domains	**display domain** [*isp-name*]	You can execute the **display** command in any view.
Display information about user connections	**display connection** [**access-type** { **dot1x** | **mac-authentication** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name* | **vlan** *vlan-id* | **ucibindex** *ucib-index* | **user-name** *user-name*]	
Display information about local users	**display local-user** [**domain** *isp-name* | **idle-cut** { **disable** | **enable** } | **vlan** *vlan-id* | **service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name*]	

Table 1-32 Display and maintain RADIUS protocol information

Operation	Command	Description
Display RADIUS message statistics about local RADIUS authentication server	**display local-server statistics**	You can execute the **display** command in any view.
Display configuration information about one specific or all RADIUS schemes	**display radius scheme** [*radius-scheme-name*]	
Display RADIUS message statistics	**display radius statistics**	
Display buffered non-response stop-accounting requests	**display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }	
Delete buffered non-response stop-accounting requests	**reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }	You can execute the **reset** command in user view.
Clear RADIUS message statistics	**reset radius statistics**	

Table 1-33 Display and maintain HWTACACS protocol information

Operation	Command	Description
Display the configuration or statistic information about one specific or all HWTACACS schemes	**display hwtacacs** [*hwtacacs-scheme-name* [**statistics**]]	You can execute the **display** command in any view.
Display buffered non-response stop-accounting requests	**display stop-accounting-buffer** { **hwtacacs-scheme** *hwtacacs-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }	

Operation	Command	Description
Clear HWTACACS message statistics	**reset hwtacacs statistics** { **accounting** | **authentication** | **authorization** | **all** }	You can execute the **reset** command in user view.
Delete buffered non-response stop-accounting requests	**reset stop-accounting-buffer** { **hwtacacs-scheme** *hwtacacs-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }	

1.7 AAA & RADIUS & HWTACACS Configuration Example

1.7.1 Remote RADIUS Authentication of Telnet/SSH Users

Note:

The configuration procedure for remote authentication of SSH users by RADIUS server is similar to that for Telnet users. The following text only takes Telnet users as example to describe the configuration procedure for remote authentication.

I. Network requirements

In the network environment shown in Figure 1-7, you are required to configure the switch so that the Telnet users logging into the switch are authenticated by the RADIUS server.

- A RADIUS server with IP address 10.110.91.164 is connected to the switch. This server will be used as the authentication server.
- On the switch, set the shared key it uses to exchange messages with the authentication RADIUS server to "expert".

You can use a CAMS server as the RADIUS server. You can select standard or extended as the server-type in a RADIUS scheme.

On the RADIUS server:

- Set the shared key it uses to exchange messages with the switch to "expert".
- Set the authentication port number.
- Add Telnet user names and login passwords.

The Telnet user names added to the RADIUS server must be in the format of *userid@isp-name* if you have configured the switch to include domain names in the user names to be sent to the RADIUS server in the RADIUS scheme.

II. Network diagram

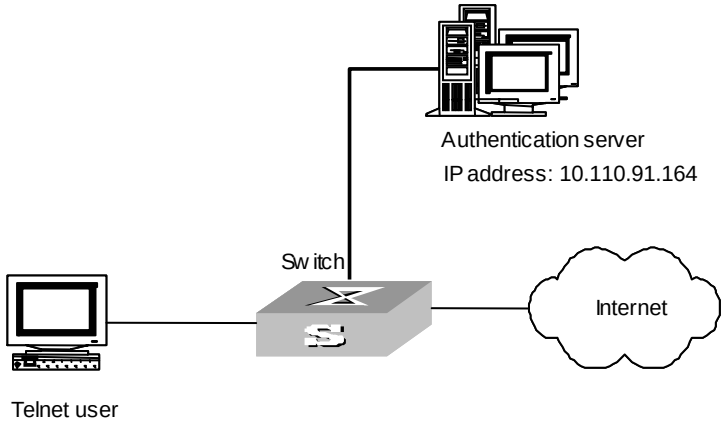


Figure 1-7 Remote RADIUS authentication of Telnet users

III. Configuration procedure

Enter system view.

```
<H3C> system-view
[H3C]
```

Adopt AAA authentication for Telnet users.

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
[H3C-ui-vty0-4] quit
```

Configure an ISP domain.

```
[H3C] domain cams
[H3C-isp-cams] access-limit enable 10
[H3C-isp-cams] quit
```

Configure a RADIUS scheme.

```
[H3C] radius scheme cams
[H3C-radius-cams] accounting optional
[H3C-radius-cams] primary authentication 10.110.91.164 1812
[H3C-radius-cams] key authentication expert
[H3C-radius-cams] server-type Extended
[H3C-radius-cams] user-name-format with-domain
[H3C-radius-cams] quit
```

Associate the ISP domain with the RADIUS scheme.

```
[H3C] domain cams
[H3C-isp-cams] scheme radius-scheme cams
```

A Telnet user logging into the switch by a name in the format of *userid* @cams belongs to the cams domain and will be authenticated according to the configuration of the cams domain.

1.7.2 Local Authentication of FTP/Telnet Users

Note:

The configuration procedure for local authentication of FTP users is similar to that for Telnet users. The following text only takes Telnet users as example to describe the configuration procedure for local authentication.

I. Network requirements

In the network environment shown in Figure 1-8, you are required to configure the switch so that the Telnet users logging into the switch are authenticated locally.

II. Network diagram

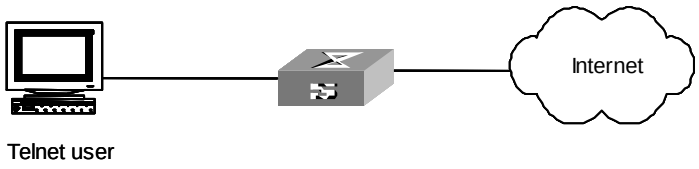


Figure 1-8 Local authentication of Telnet users

III. Configuration procedure

Method 1: Using local authentication scheme.

Enter system view.

```
<H3C> system-view
[H3C]
```

Adopt AAA authentication for Telnet users.

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
[H3C-ui-vty0-4] quit
```

Create and configure a local user named "telnet".

```
[H3C] local-user telnet
[H3C-luser-telnet] service-type telnet
[H3C-luser-telnet] password simple h3c
[H3C-luser-telnet] attribute idle-cut 300 access-limit 5
```

```
[H3C-luser-telnet] quit
[H3C] domain system
[H3C-isp-system] scheme local
```

A Telnet user logging into the switch with the name telnet@system belongs to the "system" domain and will be authenticated according to the configuration of the "system" domain.

Method 2: using local RADIUS server

This method is similar to the remote authentication method described in section 1.7.1 . You only need to change the server IP address, the authentication password, and the UDP port number of the authentication server to 127.0.0.1, h3c, and 1645 respectively in the configuration step "Configure a RADIUS scheme" in section 1.7.1 , and configure local users (whether the names of local users carry domain names should be consistent with the configuration in the RADIUS scheme).

1.7.3 HWTACACS Authentication and Authorization of Telnet Users

I. Network requirements

You are required to configure the switch so that the Telnet users logging into the switch are authenticated and authorized by the TACACS server.

A TACACS server with IP address 10.110.91.164 is connected to the switch. This server will be used as the authentication and authorization server. On the switch, set both authentication and authorization shared keys that are used to exchange messages with the TACACS server to "expert". Configure the switch to strip domain names off user names before sending user names to the TACACS server.

Configure the shared key to “expert” on the TACACS server for exchanging messages with the switch.

II. Network diagram

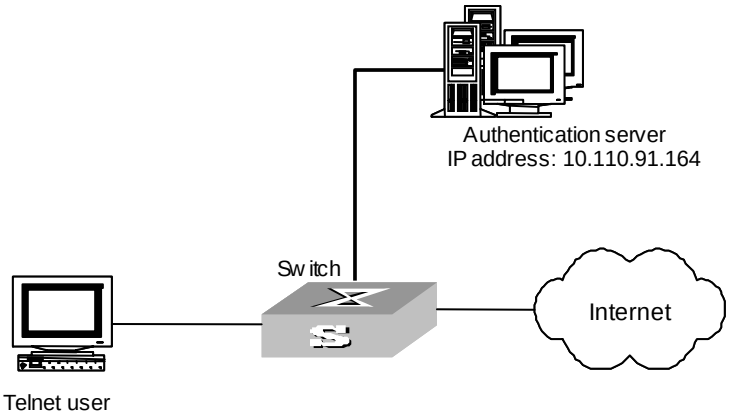


Figure 1-9 Remote HWTACACS authentication and authorization of Telnet users

III. Configuration procedure

Add a Telnet user.

(Omitted here)

Configure a HWTACACS scheme.

```
<H3C> system-view
[H3C] hwtacacs scheme hwtac
[H3C-hwtacacs-hwtac] primary authentication 10.110.91.164 49
[H3C-hwtacacs-hwtac] primary authorization 10.110.91.164 49
[H3C-hwtacacs-hwtac] key authentication expert
[H3C-hwtacacs-hwtac] key authorization expert
[H3C-hwtacacs-hwtac] user-name-format without-domain
[H3C-hwtacacs-hwtac] quit
```

Configure the domain name of the HWTACACS scheme to hwtac.

```
[H3C] domain hwtacacs
[H3C-isp-hwtacacs] scheme hwtacacs-scheme hwtac
```

1.8 Troubleshooting AAA & RADIUS & HWTACACS Configuration

1.8.1 Troubleshooting RADIUS Configuration

The RADIUS protocol operates at the application layer in the TCP/IP protocol suite. This protocol prescribes how the switch and the RADIUS server of the ISP exchange user information with each other.

Symptom 1: User authentication/authorization always fails.

Possible reasons and solutions:

- The user name is not in the userid@isp-name format, or the default ISP domain is not correctly specified on the switch — Use the correct user name format, or set a default ISP domain on the switch.
- The user is not configured in the database of the RADIUS server — Check the database of the RADIUS server, make sure that the configuration information about the user exists.
- The user input an incorrect password — Be sure to input the correct password.
- The switch and the RADIUS server have different shared keys — Compare the shared keys at the two ends, make sure they are identical.
- The switch cannot communicate with the RADIUS server (you can determine by pinging the RADIUS server from the switch) — Take measures to make the switch communicate with the RADIUS server normally.

Symptom 2: RADIUS packets cannot be sent to the RADIUS server.

Possible reasons and solutions:

- The communication links (physical/link layer) between the switch and the RADIUS server is disconnected/blocked — Take measures to make the links connected/unblocked.
- None or incorrect RADIUS server IP address is set on the switch — Be sure to set a correct RADIUS server IP address.
- One or all AAA UDP port settings are incorrect — Be sure to set the same UDP port numbers as those on the RADIUS server.

Symptom 3: The user passes the authentication and gets authorized, but the accounting information cannot be transmitted to the RADIUS server.

Possible reasons and solutions:

- The accounting port number is not properly set — Be sure to set a correct port number for RADIUS accounting.
- The switch requests that both the authentication/authorization server and the accounting server use the same device (with the same IP address), but in fact they are not resident on the same device — Be sure to configure the RADIUS servers on the switch according to the actual situation.

1.8.2 Troubleshooting HWTACACS Configuration

See the previous section if you encounter an HWTACACS fault.

Chapter 2 EAD Configuration

2.1 Introduction to EAD

Endpoint admission defense (EAD) is an attack defense solution. Using this solution, you can enhance the active defense capability of network endpoints, prevents viruses and worms from spreading on the network, and protects the entire network by limiting the access rights of insecure endpoints.

With the cooperation of switch, AAA sever, security policy server and security client, EAD is able to evaluate the security compliance of network endpoints and dynamically control their access rights.

With EAD, a switch:

- Verifies the validity of the session control packets it receives according to the source IP addresses of the packets: It regards only those packets sourced from authentication or security policy server as valid.
- Dynamically adjusts the VLAN, rate, packet scheduling priority and access control list (ACL) for user terminals according to session control packets, whereby to control the access rights of users dynamically.

2.2 Typical Network Application of EAD

EAD checks the security status of users before they can access the network, and forcibly implements user access control policies according to the check results. In this way, it can isolate the users that are not compliant with security standard and force these users to update their virus databases and install system patches. Figure 2-1 shows a typical network application of EAD.

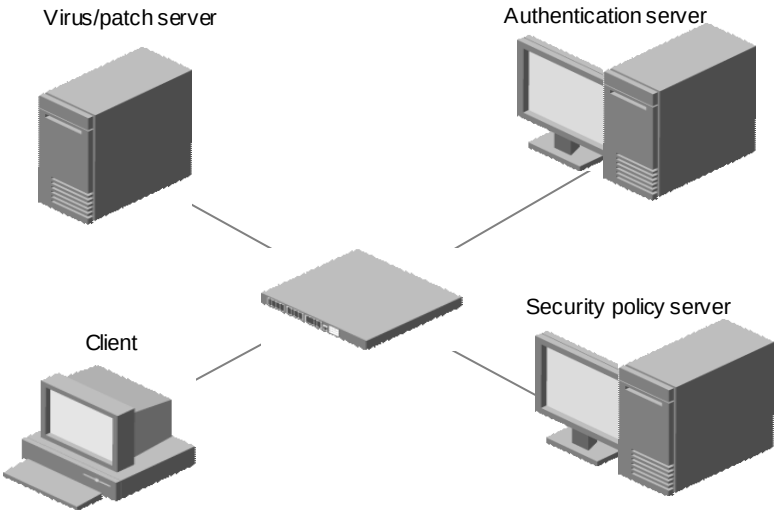


Figure 2-1 Typical network application of EAD

After a client passes the authentication, the security Client (software installed on the client PC) interacts with the security policy server to check the security status of the client. If the client is not compliant with the security standard, the security policy server issues an ACL to the switch, which then inhibits the client from accessing any parts of the network except for the virus/patch server.

After the client is patched and compliant with the required security standard, the security policy server reissues an ACL to the switch, which then assigns access right to the client so that the client can access more network resources.

2.3 EAD Configuration

The EAD configuration includes:

- Configuring the attributes of access users (such as user name, user type, and password). For local authentication, you need to configure these attributes on the switch; for remote authentication, you need to configure these attributes on the AAA sever.
- Configuring RADIUS scheme.
- Configuring the IP address of the security policy server.
- Associating domain with RADIUS scheme.

EAD is commonly used in RADIUS authentication environment.

This section mainly describes the configuration of security policy server IP address. For other related configuration, refer to Chapter 1 “AAA & RADIUS & HWTACACS Configuration”.

Table 2-1 EAD configuration

Operation	Command	Description
Enter system view	**system-view**	—
Enter RADIUS scheme view	**radius scheme** *radius-scheme-name*	—
Configure the RADIUS server type to **extended**	**server-type extended**	Required
Configure the IP address of a security policy server	**security-policy-server** *ip-address*	Required Each RADIUS scheme supports up to eight IP addresses of security policy servers.

2.4 EAD Configuration Example

I. Network requirements

In Figure 2-2:

- A user is connected to Ethernet1/0/1 on the switch.
- The user adopts 802.1x client supporting H3C extended function.
- You are required to configure the switch to use RADIUS server for remote user authentication and use security policy server for EAD control on users.

The following are the configuration tasks:

- Connect the RADIUS authentication server 10.110.91.164 and the switch, and configure the switch to use port number 1812 to communicate with the server.
- Configure the authentication server type to **extended**.
- Configure the encryption password for exchanging messages between the switch and RADIUS server to “expert”.
- Configure the IP address 10.110.91.166 of the security policy server.

II. Network diagram

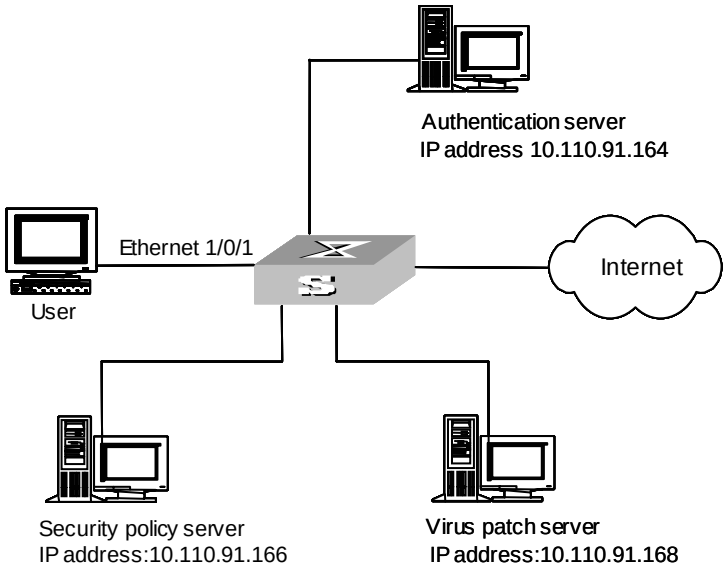


Figure 2-2 EAD configuration

III. Configuration procedure

Configure 802.1x on the switch. Refer to the 802.1x part in *H3C S3600 Series Ethernet Switches Operation Manual* for detailed description.

Configure a domain.

```
<H3C> system-view
[H3C] domain system
[H3C-isp-system] quit
```

Configure a RADIUS scheme.

```
[H3C] radius scheme cams
[H3C-radius-cams] primary authentication 10.110.91.164 1812
[H3C-radius-cams] accounting optional
[H3C-radius-cams] key authentication expert
[H3C-radius-cams] server-type extended
```

Configure the IP address of the security policy server.

```
[H3C-radius-cams] security-policy-server 10.110.91.166
```

Associate the domain with the RADIUS scheme.

```
[H3C-radius-cams] quit
[H3C] domain system
[H3C-isp-system] radius-scheme cams
```

Table of Contents

Chapter 1 VRRP Configuration 1-1
1.1 VRRP Overview 1-1
1.1.1 Virtual Router Overview 1-2
1.1.2 Introduction to Backup Group 1-4
1.1.3 Introduction to the Port Tracking Function 1-6
1.1.4 Auto Detect Implementation in VRRP 1-6
1.2 VRRP Configuration 1-7
1.2.1 Introduction to VRRP Configuration Tasks 1-7
1.2.2 Configuring a Virtual Router IP Address 1-7
1.2.3 Configuring Backup Group-Related Parameters 1-8
1.2.4 Configuring the Port Tracking Function 1-9
1.2.5 Configuring the Auto Detect Function for VRRP 1-9
1.3 Displaying and Debugging VRRP 1-10
1.4 VRRP Configuration Example 1-10
1.4.1 Single-VRRP Backup Group Configuration 1-10
1.4.2 VRRP Tracking Interface Configuration 1-12
1.4.3 Multiple-VRRP Backup Group Configuration 1-15
1.4.4 Port Tracking Configuration Example 1-16
1.4.5 VRRP Auto Detect Configuration Example 1-17
1.5 Troubleshooting VRRP 1-19

Chapter 1 VRRP Configuration

Note:

The S3600-EI series switches support the VRRP feature, but not the S3600-SI series.

1.1 VRRP Overview

Virtual router redundancy protocol (VRRP) is a fault-tolerant protocol.

As shown in Figure 1-1, in general,

- A default route (for example, the next hop address of the default route is 10.100.10.1, as shown in the following figure) is configured for every host on a network.
- The packets destined for the external network segments and sourced from these hosts go through the default routes to the Layer 3 Switch 1, implementing communication between these hosts and the external network.
- If Switch 1 fails, all the hosts on this segment taking Switch 1 as the next-hop through the default routes are cut off from the external network.

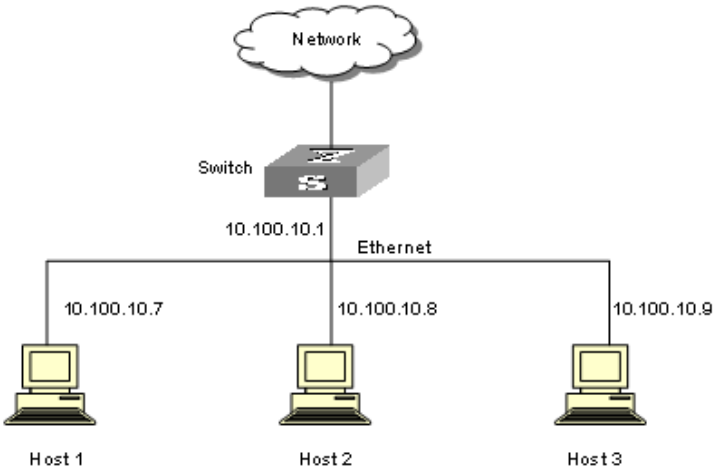


Figure 1-1 LAN networking

VRRP, designed for LANs with multicast and broadcast capabilities (such as Ethernet), settles the problem caused by switch failures.

VRRP combines a group of LAN switches, including a master switch and several backup switches, into a virtual router, or a backup group

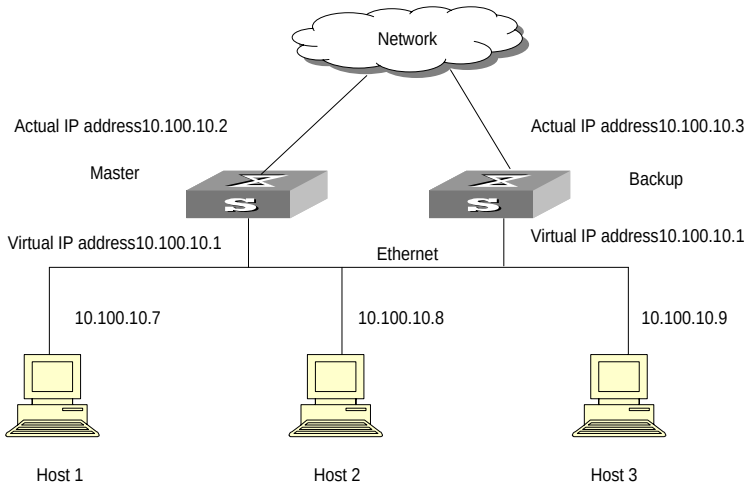


Figure 1-2 Virtual router

The switches in a backup group have the following features:

- This virtual router has its own IP address: 10.100.10.1 (which can be the interface address of a switch within the backup group).
- The switches within the backup group have their own IP addresses (such as 10.100.10.2 for the master switch and 10.100.10.3 for the backup switch).
- Hosts on the LAN only know the IP address of this virtual router, that is, 10.100.10.1, but not the specific IP addresses 10.100.10.2 of the master switch and 10.100.10.3 of the backup switch.
- Hosts in the LAN use the IP address of the virtual router (that is, 10.100.10.1) as their default next-hop IP addresses.

Therefore, hosts within the network will communicate with the other networks through this virtual router.

If the master switch in the backup group goes down, the backup switch with the highest priority functions as the new master switch to guarantee normal communication between the hosts and the external networks. This ensures the communications between the hosts and the external networks.

1.1.1 Virtual Router Overview

After you enable VRRP on the switches of a backup group, a virtual router is formed. You can perform related configuration on the virtual router.

I. Configuring a virtual router IP address

The IP address of the virtual router can be an unassigned IP address of the network segment where the backup group is located or the interface IP address of a member switch in the backup group. The virtual router IP address has the following features:

- You can specify the virtual router IP address as the IP address used by a member switch in the backup group. In this case, the switch is called an IP address owner.

- A backup group is established if it is assigned an IP address for the first time. If you then add other IP addresses to the backup group, the IP addresses are added to the virtual router IP address list of the backup group.
- The virtual router IP address and the IP addresses used by the member switches in a backup group must belong to the same network segment. If not, the backup group will be in the initial state (the state before you configure the VRRP on the switches of the group). In this case, VRRP does not take effect.
- A backup group is removed if all its virtual router IP addresses are removed. In this case, all the configurations performed for the backup group get ruined.

According to the standard VRRP, you will fail to use the **ping** command to ping the IP address of a virtual router. So the hosts connected to a switch in a backup group cannot judge with **ping** command whether an IP address is used by the backup group. If the IP address of a host is also used by the virtual router, all packets destined for the network segment will be forwarded to the host. In this case, data in this network segment cannot be forwarded properly.

Before enabling VRRP feature on an S3600 Ethernet switch, you can enable the switches in a backup group to respond the **ping** operations destined for the virtual router IP addresses. Therefore the above incident can be avoided. If VRRP is already enabled, the system does not support this configuration.

II. Mapping virtual IP addresses to MAC addresses

An S3600 Ethernet switch provides the following functions in addition to forwarding data correctly.

- You can map multiple virtual IP addresses of the backup group to a virtual MAC address as needed. You can also map virtual IP addresses to the MAC address of a switch routing interface.
- You need to map the IP addresses of the backup group to the MAC addresses before enabling VRRP feature on an S3600 Ethernet switch. If VRRP is already enabled, the system does not support this configuration.

By default, virtual router IP addresses are mapped to the virtual MAC address of a backup group.

Note:

When you map a virtual IP address to the virtual MAC address on an S3600 Ethernet switch, the number of backup groups that can be configured on a VLAN interface is determined by the chips used. Refer to device specification for details.

1.1.2 Introduction to Backup Group

I. Configurations available on switches in a backup group

VRRP can group switches in a LAN into a virtual router, which is also known as a backup group.

You can perform the following configuration on an S3600 Ethernet switch that belongs to a backup group.

Table 1-1 Configuration available on switches in a backup group

Configuration	Description	Related section
Configure switch priority	Required	Section 1.1.2 II. "Configuring switch priority"
Configure preemptive mode	Required	Section 1.1.2 III. "Configuring preemptive mode for a switch in a backup group"
Configure authentication type and authentication key	Optional	Section 1.1.2 IV. "Configuring authentication type and authentication key for a switch in a backup group"
Configure VRRP timer	Required	Section 1.1.2 V. "Configuring VRRP timer"
Configure the VLAN interfaces to be tracked for a backup group	Required	Section 1.1.2 VI. "Configuring the VLAN interfaces to be tracked for a backup group"

II. Configuring switch priority

You can configure the priority of a switch in a backup group. VRRP will determine the status of each switch in a backup group according to the priority of the switch. The master switch in a backup group is the one currently with the highest priority.

Switch priority ranges from 0 to 255 (a larger number indicates a higher switch priority) and defaults to 100. Note that only 1 through 254 are available to users. Switch priority of 255 is reserved for IP address owners.

Note:

The priority of the IP address owner is fixed to 255.

III. Configuring preemptive mode for a switch in a backup group

As long as a switch in the backup group becomes the master switch, other switches, even if they are configured with a higher priority later, do not preempt the master switch

unless they operate in preemptive mode. The switch operating in preemptive mode will become the master switch when it finds its priority is higher than that of the current master switch, and the former master switch becomes a backup switch accordingly.

You can configure an S3600 Ethernet switch to operate in preemptive mode. You can also set the delay period. A backup switch waits for a period of time (the delay period) before becoming a master switch. Setting a delay period aims at:

In an unstable network, backup switches in a backup group possibly cannot receive packets from the master in time due to network congestions even if the master operates properly. This causes the master of the backup group being determined frequently. With the configuration of delay period, the backup switch will wait for a while if it does not receive packets from the master switch in time. A new master is determined only after the backup switches do not receive packets from the master switch after the specified delay time.

IV. Configuring authentication type and authentication key for a switch in a backup group

VRRP provides the 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 adds the authentication key into the VRRP packets before transmitting them. 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 and be discarded. In this case, a simple authentication key should not exceed eight characters.

In a vulnerable network, the authentication type can be set to **md5**. The switch then uses the authentication type provided by the Authentication Header, and MD5 algorithm to authenticate the VRRP packets. In this case, you need to set an authentication key comprising up to eight characters or a 24-character encrypted string.

Packets that fail to pass the authentication are discarded. The switch then sends trap packets to the network management system.

V. Configuring VRRP timer

The master switch advertises its normal operation state to the switches within the VRRP backup group by sending VRRP packets once in each specified interval (determined by the *adver-interval* argument). If the backup switches do not receive VRRP packets from the master after a specific period (determined by the *master-down-interval* argument), they consider the master is down and initiates the process to determine the master switch.

You can adjust the frequency in which a master sends VRRP packets by setting the corresponding VRRP timers (that is, the *adver-interval* argument). The *master-down-interval* argument is usually three times of the *adver-interval* argument. Excessive network traffic or differences between the timers of different switches 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. If you configure the preemption delay for a backup switch, the switch preempts the master after the period specified by the preemption delay if it does not receive a VRRP packet from the master for the period specified by the *master-down-interval* argument.

VI. Configuring the VLAN interfaces to be tracked for a backup group

The VLAN interface tracking function expands the backup group function. With this function enabled, the backup group function is provided not only when the interface where the backup group resides fails, but also when other interfaces are unavailable. By executing the related command you can track an interface.

When a tracked VLAN interface goes down, the priority of the switch owning the interface will reduce automatically by a specified value (the *value-reduced* argument). If the switches with their priorities higher than that of the current master switch exist in the backup group, a new master switch will be then determined.

1.1.3 Introduction to the Port Tracking Function

VRRP backup group port tracking function can track the link state of the physical port, and decrease the priority of the switch when the physical port fails.

When the master's uplink physical port fails, the priority of the master switch is decreased by a set value. This in turn triggers the new master to be determined in the backup group.

1.1.4 Auto Detect Implementation in VRRP

Note:

Currently, auto detect implementation in VRRP is only supported on S3600-EI series switches.

You can control the priority of the VRRP backup group according to the auto detect result to enable automatic switch between the master switch and the standby switch as follows:

- Decrease the priority of a backup group when the result of the detecting group is **unreachable**.

- Restore the priority of a backup group when the result of the detecting group is **reachable**.

Refer to *Auto Detect Operation Manual* for information about auto detect.

1.2 VRRP Configuration

1.2.1 Introduction to VRRP Configuration Tasks

Table 1-2 VRRP configuration tasks

Configuration	Description	Related section
Configure a virtual router IP address	Required	Section 1.2.2 "Configuring a Virtual Router IP Address"
Configure backup group-related parameters	Required	Section 1.2.3 "Configuring Backup Group-Related Parameters"
VRRP backup group interface tracking configuration	Optional	Section 1.2.4 "Configuring the Port Tracking Function"
VRRP auto detect configuration	Optional	Section 1.2.5 "Configuring the Auto Detect Function for VRRP"

1.2.2 Configuring a Virtual Router IP Address

Table 1-3 lists the operations to configure a virtual router IP address (suppose you have correctly configured the relation between the port and VLAN):

Table 1-3 Configure a virtual router IP address

Operation	Command	Description
Enter system view	**system-view**	—
Configure that the virtual IP address can be pinged	**vrrp ping-enable**	Optional By default, the virtual IP address cannot be pinged.
Map the virtual router IP address to a MAC address	**vrrp method** { **real-mac** | **virtual-mac** }	Optional By default, the virtual IP address of a backup group is mapped to a virtual router IP address.
Create a VLAN	**vlan** *vlan-id*	— This operation creates the VLAN to which the backup group corresponds. The *vlan-id* argument is the ID of the VLAN.

Operation	Command	Description
Quit to system view	**quit**	—
Enter VLAN interface view	**interface vlan-interface** *vlan-id*	—
Configure a virtual router IP address	**vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*	Optional

1.2.3 Configuring Backup Group-Related Parameters

Table 1-4 lists the operations to configure a switch in a backup group.

Table 1-4 Configure backup group-related parameters

Operation	Command	Description
Enter system view	**system-view**	—
Create a VLAN	**vlan** *vlan-id*	—
Quit to system view	**quit**	—
Enter VLAN interface view	**interface vlan-interface** *valn-id*	—
Configure the priority of the backup group	**vrrp vrid** *virtual-router-id* **priority** *priority*	Optional By default, the priority of a backup group is 100.
Configure the preemptive mode and delay period for the backup group	**vrrp vrid** *virtual-router-id* **preempt-mode** [**timer delay** *delay-value*]	Optional By default, a backup group operates in the preemptive mode.
Configure the authentication type and authentication key	**vrrp authentication-mode** *authentication-type authentication-key*	Optional By default, a backup group does not perform authentication.
Configure the VRRP timer	**vrrp vrid** *virtual-router-id* **timer advertise** *adver-interval*	Optional By default, the interval for the master switch in a backup group to send VRRP packets is 1 second.
Specify the interface to be tracked	**vrrp vrid** *virtual-router-id* **track vlan-interface** vlan-id [**reduced** *value-reduced*]	Optional *value-reduced*: Value by which the priority is to be reduced. By default, this value is 10.

1.2.4 Configuring the Port Tracking Function

Table 1-5 Configure the VRRP backup group port tracking function

Operation	Command	Description
Enter system view	**system-view**	—
Create a VLAN	**vlan** *vlan-id*	Required
Add an Ethernet port to the VLAN	**port** *interface-type interface-number*	—
Quit to system view	**quit**	Quit the VLAN view to system view
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the port tracking function	**vrrp vlan-interface** *vlan-id* **vrid** *virtual-router-id* **track** [**reduced** *value-reduced*]	Required By default, the value by which the priority of an Ethernet port is decreased is 10.

Note:

- The port to be tracked can be in the VLAN which the VLAN interface of the backup group belongs to.
- Up to eight ports can be monitored simultaneously.

1.2.5 Configuring the Auto Detect Function for VRRP

Note:

You need to create the detecting group and perform VRRP-related configurations before the following operations. Refer to *Auto Detect Operation Manual* for the creation of a detecting group.

Table 1-6 Configure the auto detect function for VRRP

Operation	Command	Description
Enter system view	**system-view**	—
Enter VLAN interface view	**interface vlan-interface** *vlan-id*	—

Operation	Command	Description
Enable the auto detect function for VRRP	**vrrp vrid** *virtual-router-id* **track detect-group** *group-number* [**reduced** *value-reduced*]	Required

Note:

A detecting group can be used to detect up to eight Layer 3 interfaces.

1.3 Displaying and Debugging VRRP

After the above configurations, you can execute the **display** command in any view to view VRRP configuration and verify the configuration effect. And you can execute the **reset** command in user view to clear the VRRP statistics.

Table 1-7 Display and debug VRRP

Operation	Command	Description
Display VRRP state information and statistics information	**display vrrp** [**interface vlan-interface** *vlan-id* **| statistics** [**vlan-interface** *vlan-id*]] [*virtual-router-id*]	The **display** command can be executed in any view.
Clear VRRP statistics	**reset vrrp statistics** [**vlan-interface** *vlan-id*] [*virtual-router-id*]	The **reset** command can be executed in user view.

1.4 VRRP Configuration Example

1.4.1 Single-VRRP Backup Group Configuration

I. Network requirements

Host A uses the VRRP virtual router comprising switch A and switch B as its default gateway to visit host B on the Internet.

The information about the VRRP backup group is as follows:

- VRRP backup group ID: 1
- Virtual router IP address: 202.38.160.111
- Master switch: Switch A
- Backup switch: Switch B
- Preemptive mode: enabled

Table 1-8 Network description

Switch	Ethernet port connecting to Host A	IP address of the VLAN interface	Switch priority in the backup group	Preemptive mode
LSW-A	Ethernet 1/0/6	202.38.160.1/24	110	Enabled
LSW-B	Ethernet 1/0/5	202.38.160.2/24	100 (default)	Enabled

II. Network diagram

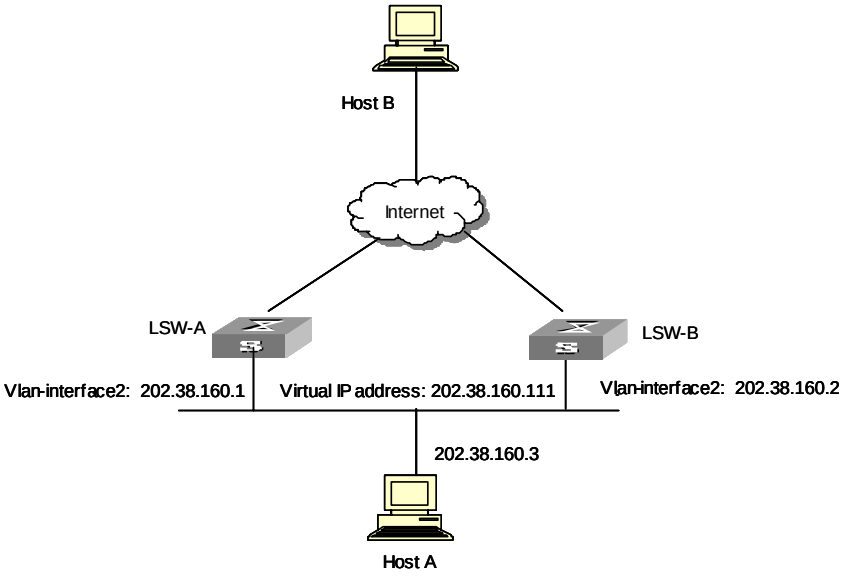


Figure 1-3 Network diagram for single-VRRP backup group configuration

III. Configuration procedure

- Configure Switch A.

Configure VLAN 2.

```
<LSW-A> system-view
[LSW-A] vlan 2
[LSW-A-vlan2] port Ethernet 1/0/6
[LSW-A-vlan2] quit
[LSW-A] interface Vlan-interface 2
[LSW-A-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
[LSW-A-Vlan-interface2] quit
```

Enable a backup group to respond to ping operations destined for its virtual router IP address.

```
[LSW-A] vrrp ping-enable
```

Create a backup group.

```
[LSW-A] interface vlan 2
[LSW-A-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Set the priority for the backup group.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 priority 110
```

Configure the preemptive mode for the backup group.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 preempt-mode
```

- Configure Switch B.

Configure VLAN 2.

```
<LSW-B> system-view
System View: return to User View with Ctrl+Z.
[LSW-B] vlan 2
[LSW-B-Vlan2] port Ethernet 1/0/5
[LSW-B-vlan2] quit
[LSW-B] interface Vlan-interface 2
[LSW-B-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
[LSW-B-Vlan-interface2] quit
```

Enable a backup group to respond to ping operations destined for its virtual router IP address.

```
[LSW-B] vrrp ping-enable
```

Create a backup group.

```
[LSW-B] interface vlan 2
[LSW-B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Configure the preemptive mode for the backup group.

```
[LSW-B-Vlan-interface2] vrrp vrid 1 preempt-mode
```

The IP address of the default gateway of Host A can be configured to be 202.38.160.111.

Normally, Switch A functions as the gateway, but when Switch A is turned off or fails, Switch B will function as the gateway instead.

Configure Switch A to operate in preemptive mode, so that it can resume its gateway function as the master switch after recovery.

1.4.2 VRRP Tracking Interface Configuration

I. Network requirements

Even when Switch A is still functioning, Switch B (with another link to connect with the outside) can function as a gateway when the interface on Switch A and connecting to

Internet does not function properly. This can be implemented by enabling the VLAN interface tracking function.

The VRRP backup group ID is set to 1, with configurations of authorization key and timer.

II. Network diagram

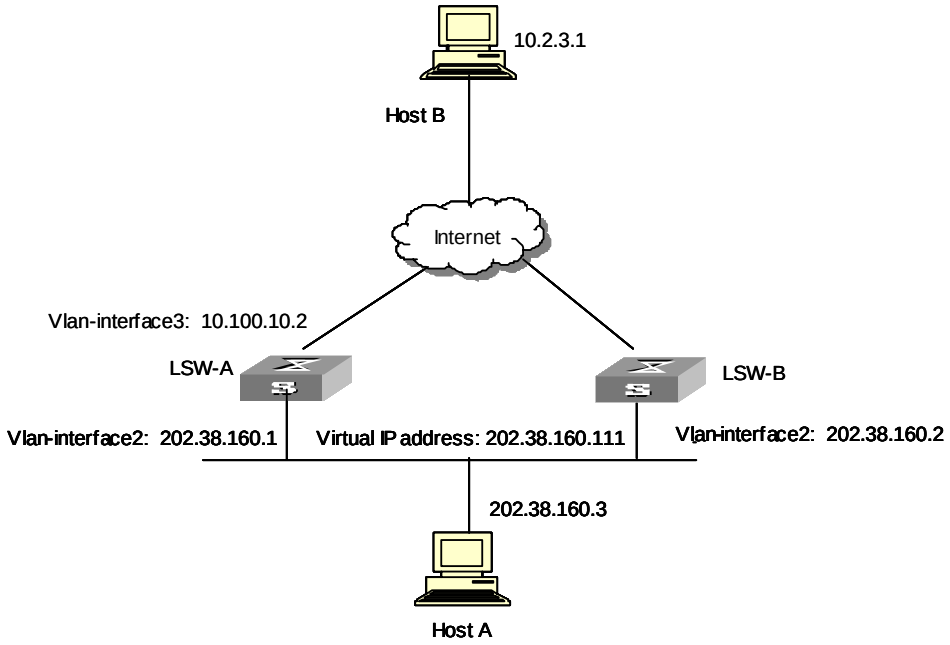


Figure 1-4 Network diagram for interface tracking configuration

III. Configuration procedure

- Configure Switch A.

Configure VLAN 2.

```
<LSW-A> system-view
System View: return to User View with Ctrl+Z.
[LSW-A] vlan 2
[LSW-A-vlan2] port Ethernet 1/0/6
[LSW-A-vlan2] quit
[LSW-A] interface Vlan-interface 2
[LSW-A-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
[LSW-A-Vlan-interface2] quit
```

Configure that the virtual router can be pinged.

```
[LSW-A] vrrp ping-enable
```

Create a backup group.

```
[LSW-A] interface Vlan-interface 2
[LSW-A-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Set the priority for the backup group.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 priority 110
```

Set the authentication type for the backup group to **md5,** and the password to abc123.

```
[LSW-A-Vlan-interface2] vrrp authentication-mode md5 abc123
```

Configure the master switch to send VRRP packets every 5 seconds.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

Set the tracked VLAN interface.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 track Vlan-interface 3 reduced 30
```

- Configure switch B.

Configure VLAN 2.

```
<LSW-B> system-view
System View: return to User View with Ctrl+Z.
[LSW-B] vlan 2
[LSW-B-vlan2] port Ethernet 1/0/5
[LSW-B-vlan2] quit
[LSW-B] interface Vlan-interface 2
[LSW-B-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
[LSW-B-Vlan-interface2] quit
```

Configure that the virtual router can be pinged.

```
[LSW-B] vrrp ping-enable
```

Create a backup group.

```
[LSW-B] interface Vlan-interface 2
[LSW-B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Configure the authentication key for the backup group.

```
[LSW-B-Vlan-interface2] vrrp authentication-mode md5 abc123
```

Configure the master to send VRRP packets every 5 seconds.

```
[LSW-B-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

Normally, Switch A functions as the gateway, but when VLAN-interface3 on Switch A goes 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 recovers, switch A will resume its gateway function as the master.

1.4.3 Multiple-VRRP Backup Group Configuration

I. Network requirements

A switch can function as backup switches of multiple backup groups.

Multiple-backup group configuration can implement load balancing. For example, Switch A operates as the master switch of backup group 1 and a backup switch in backup group 2. Similarly, Switch B operates as the master switch of backup group 2 and a backup switch in backup group 1. Some hosts in the network take virtual router 1 as the gateway, while others take virtual router 2 as the gateway. In this way, both load balancing and mutual backup are implemented.

II. Network diagram

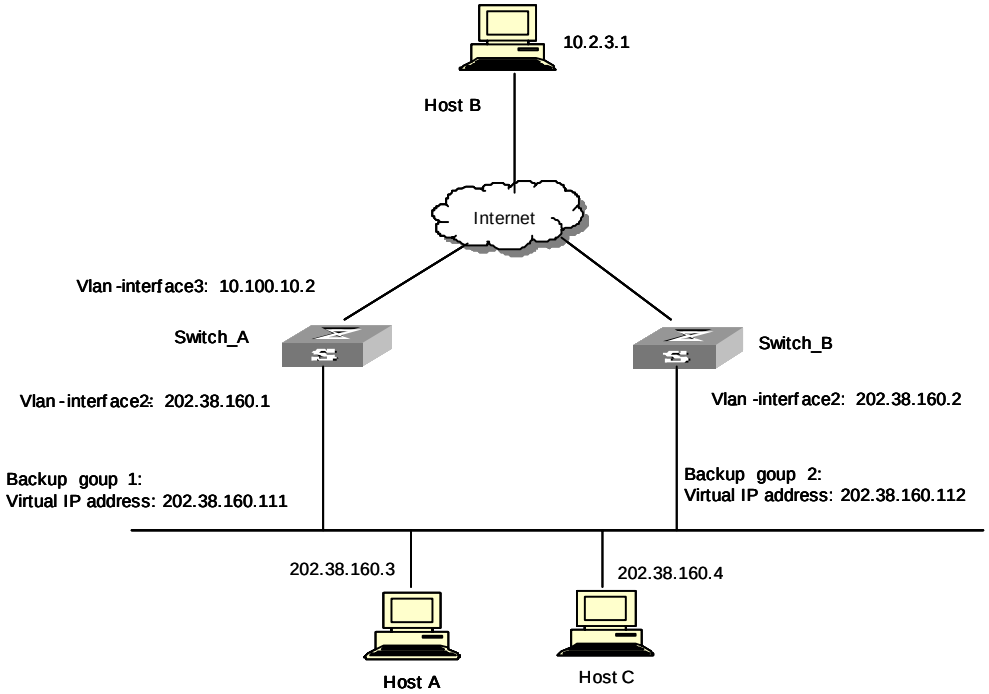


Figure 1-5 Network diagram for multiple-VRRP backup group configuration

III. Configuration procedure

- Configure Switch A.

Configure VLAN 2.

```
<LSW-A> system-view
System View: return to User View with Ctrl+Z.
[LSW-A] vlan 2
[LSW-A-vlan2] port Ethernet 1/0/6
[LSW-A-vlan2] quit
[LSW-A] interface Vlan-interface 2
[LSW-A-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
```

Create backup group 1.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Set the priority for backup group 1.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 priority 150
```

Create backup group 2.

```
[LSW-A-Vlan-interface2] vrrp vrid 2 virtual-ip 202.38.160.112
```

- Configure Switch B.

Configure VLAN 2.

```
<LSW-B> system-view
System View: return to User View with Ctrl+Z.
[LSW-B] vlan 2
[LSW-B-vlan2] port Ethernet 1/0/6
[LSW-B-vlan2] quit
[LSW-B] interface vlan-interface 2
[LSW-B-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
```

Create backup group 1.

```
[LSW-B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Create backup group 2.

```
[LSW-B-Vlan-interface2] vrrp vrid 2 virtual-ip 202.38.160.112
```

Set the priority for backup group 2.

```
[LSW-B-Vlan-interface2] vrrp vrid 2 priority 110
```

Note:

Normally, multiple backup groups are used in actual use.

1.4.4 Port Tracking Configuration Example

I. Network requirements

- Backup group 1 comprises two switches, which operate as the master switch and the backup switch.
- The actual IP addresses of the master and the backup switches are 10.100.10.2 and 10.100.10.3 respectively.
- The master switch is connected to the upstream network through its Ethernet1/0/1 port. The backup switch is connected to the upstream network through its Ethernet1/0/2 port.
- The virtual router IP address of the backup group is 10.100.10.1.

- Enable the port tracking function on Ethernet1/0/1 port of the master switch and specify that the priority of the master decreases by 50 when Ethernet1/0/1 port fails, which triggers new master switch being determined in the backup group 1.

II. Network diagram

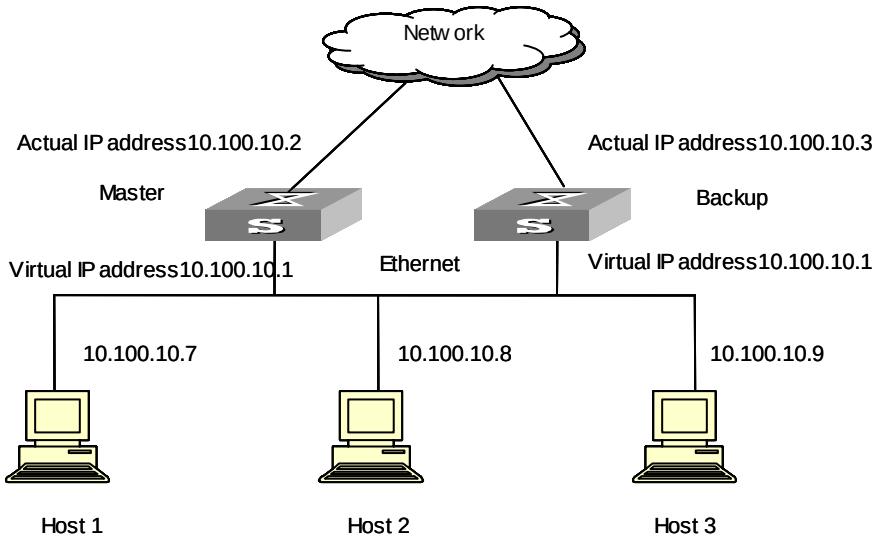


Figure 1-6 Network diagram for VRRP port tracking configuration

III. Configuration procedure

- Configure the master switch.

Enter system view.

```
<H3C> system-view
```

Create VLAN 2.

```
[H3C] vlan 2
[H3C-vlan2] port Ethernet1/0/1
[H3C-vlan2] quit
```

Enter Ethernet1/0/1 port view and enable the port tracking function.

```
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] vrrp vlan-interface 2 vrid 1 track reduced 50
```

1.4.5 VRRP Auto Detect Configuration Example

I. Network requirements

- Switch B and switch D form VRRP backup group 1, whose virtual IP address is 192.168.1.10. Normally, packets sourced from Switch A and destined for Switch C are forwarded by Switch B.

- When the connection between Switch B and Switch C fails, Switch D becomes the Master in backup group 1 automatically and the link from Switch D to Switch C, namely the secondary link, is enabled.

II. Network diagram

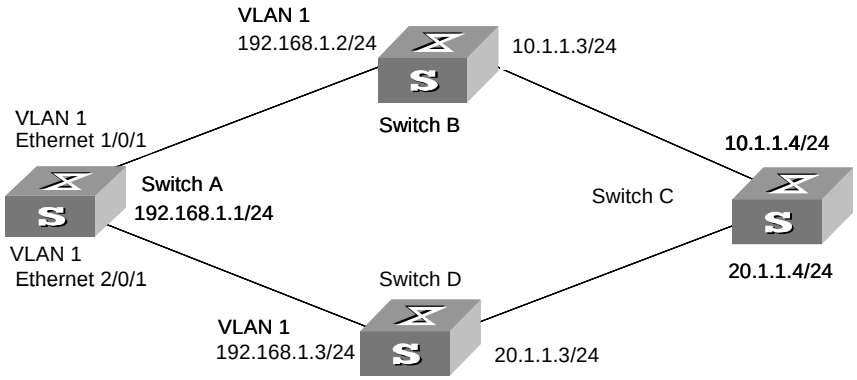


Figure 1-7 Network diagram for implementing the auto detect function in VRRP

III. Configuration procedure

- Configure Switch B.

Create detecting group 9.

```
<H3C B> system-view
[H3C B] detect-group 9
```

Specify to detect the reachability of the IP address 10.1.1.4, setting the detect number to 1.

```
[H3C B-detect-group-9] detect-list 1 ip address 10.1.1.4
[H3C B-detect-group-9] quit
```

Assign an IP address to VLAN-interface1.

```
[H3C B] interface vlan-interface 1
[H3C B-Vlan-interface1] ip address 192.168.1.2 24
```

Enable VRRP on VLAN-interface1 and assign a virtual IP address to the backup group.

```
[H3C B-Vlan-interface1] vrrp vrid 1 virtual-ip 192.168.1.10
```

Set the backup group priority of switch B to 110, and specify to decrease the priority by 20 when the result of detecting group 9 is **unreachable**.

```
[H3C B-Vlan-interface1] vrrp vrid 1 priority 110
[H3C B-Vlan-interface1] vrrp vrid 1 track detect-group 9 reduced 20
```

- Configure Switch D.

Assign an IP address to VLAN-interface1.

```
<H3C D> system-view
```

```
[H3C D] interface vlan-interface 1
[H3C D-Vlan-interface1] ip address 192.168.1.3 24
```

Crate a backup group on VLAN-interface1 and assign a virtual IP address to the backup group.

```
[H3C D-Vlan-interface1] vrrp vrid 1 virtual-ip 192.168.1.10
```

Set the backup group priority of Switch D to 100.

```
[H3C D-Vlan-interface1] vrrp vrid 1 priority 100
```

1.5 Troubleshooting VRRP

You can locate VRRP problems through the configuration and debugging information. Here are some possible failures you might meet and the corresponding troubleshooting methods.

I. Symptom 1: Frequent prompts of configuration errors on the console

This indicates that incorrect VRRP packets are received. It may be because of the inconsistent configuration of the switches within the backup group, or the attempt of other devices sending 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 taken.

II. Symptom 2: More than one master existing within a backup group

There are also 2 reasons. One is short coexistence of many master switches, which is normal and needs no manual intervention. Another is long coexistence of many master switches, which may be caused because the original master switch and other member switches in a backup group cannot receive VRRP packets from each other, or receive some illegal packets.

To solve such a problem, an attempt should be made to ping among these masters and if such an attempt fails, check the connectivity between related devices. If they can be pinged, check VRRP configuration. For the configuration of a VRRP backup group, complete consistency for the number of virtual IP addresses, each virtual IP address, timer interval and authentication type configured on each member switch must be guaranteed.

III. Symptom 3: VRRP state of a switch changes repeatedly

Such problems occur when the backup group timer interval is too short. They can be solved through prolonging the interval or configuring the preemption delay period.

Table of Contents

Chapter 1 Centralized MAC Address Authentication Configuration 1-1
1.1 Centralized MAC Address Authentication Overview 1-1
1.2 Centralized MAC Address Authentication Configuration 1-2
1.2.1 Enabling Centralized MAC Address Authentication Globally 1-2
1.2.2 Enabling Centralized MAC Address Authentication for a Port 1-2
1.2.3 Configuring Centralized MAC Address Authentication Mode 1-3
1.2.4 Configuring the ISP Domain for MAC Address Authentication Users 1-4
1.2.5 Configuring the Timers Used in Centralized MAC Address Authentication 1-4
1.3 Displaying and Debugging Centralized MAC Address Authentication 1-5
1.4 Centralized MAC Address Authentication Configuration Example 1-6

Chapter 1 Centralized MAC Address Authentication Configuration

1.1 Centralized MAC Address Authentication Overview

Centralized MAC address authentication is port- and MAC address-based authentication used to control user permissions to access a network. Centralized MAC address authentication can be performed without client-side software. With this type of authentication employed, a switch authenticates a user upon detecting the MAC address of the user for the first time.

Centralized MAC address authentication can be implemented in the following two modes:

- MAC address mode, where user MAC serves as both the user name and the password.
- Fixed mode, where user names and passwords are configured on a switch in advance. In this case, every user corresponds to a specific user name and password configured on the switch.

As for S3600 series Ethernet switches, authentication can be performed locally or on a RADIUS server.

1) When a RADIUS server is used for authentication, the switch serves as a RADIUS client. Authentication is carried out through the cooperation of switches and the RADIUS server.

- In MAC address mode, a switch sends user MAC addresses detected to the RADIUS server as both user names and passwords. The rest handling procedures are the same as that of the common RADIUS authentication.
- In fixed mode, a switch sends the user name and password previously configured for the user to be authenticated to the RADIUS server and replaces the calling-station-id field of the RADIUS packet with the MAC address of the user. The rest handling procedures are the same as that of the common RADIUS authentication.
- A user can access a network upon passing the authentication performed by the DADIUS server.

2) When authentications are performed locally, users are authenticated by switches. In this case,

- For MAC address mode, you can specify the format to enter the MAC addresses used as both user name and password by executing corresponding commands. That is, to specify whether or not MAC addresses are provided in the hyphened

form. The input format should be the same as the configured format, or else, the authentication will fail.

- For fixed mode, configure the local user names and passwords as those for fixed mode.
- The service type of a local user needs to be configured as lan-access.

1.2 Centralized MAC Address Authentication Configuration

The following are centralized MAC address authentication configuration tasks:

- Enabling Centralized MAC Address Authentication Globally
- Enabling Centralized MAC Address Authentication for a Port
- Configuring Centralized MAC Address Authentication Mode
- Configuring the ISP Domain for MAC Address Authentication Users
- Configuring the Timers Used in Centralized MAC Address Authentication

---

Caution:

The configuration of the maximum number of learned MAC addresses (refer to the **mac-address max-mac-count** command) is unavailable for the ports with centralized MAC address authentication enabled. Similarly, the centralized MAC address authentication is unavailable for the ports with the maximum number of learned MAC addresses configured.

1.2.1 Enabling Centralized MAC Address Authentication Globally

Table 1-1 Enable centralized MAC address authentication

Operation	Command	Description
Enter system view	**system-view**	—
Enable centralized MAC address authentication globally	**mac-authentication**	Required By default, centralized MAC address authentication is globally disabled.

1.2.2 Enabling Centralized MAC Address Authentication for a Port

You can enable centralized MAC address authentication for a port in system view or in Ethernet port view.

Table 1-2 Enable centralized MAC address authentication for a port in system view

Operation	Command	Description
Enter system view	**system-view**	—
Enable centralized MAC address authentication for specified ports	**mac-authentication interface** *interface-list*	Required By default, centralized MAC address authentication is disabled on a port.

Table 1-3 Enable centralized MAC address authentication for a port in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable centralized MAC address authentication for the current port	**mac-authentication**	Required By default, centralized MAC address authentication is disabled on a port.

Centralized MAC address authentication for a port can be configured but does not take effect before global centralized MAC address authentication is enabled. After global centralized MAC address authentication is enabled, ports enabled with the centralized MAC address authentication will perform the authentication immediately.

1.2.3 Configuring Centralized MAC Address Authentication Mode

Table 1-4 Configure centralized MAC address authentication mode

Operation	Command	Description
Enter system view	**system-view**	—
Configure centralized MAC address authentication mode as MAC address mode	**mac-authentication authmode usernameasmacaddress** [**usernameformat** { **with-hyphen** | **without-hyphen** }]	Optional By default, the MAC address mode is adopted.
Configure centralized MAC address authentication mode as fixed mode	**mac-authentication authmode usernamefixed**	Optional

Operation	Command	Description
Set a user name for fixed mode	**mac-authentication authusername** *username*	Required for fixed mode By default, the user name is mac and no password is needed.
Set the password for fixed mode	**mac-authentication authpassword** *password*	Optional

1.2.4 Configuring the ISP Domain for MAC Address Authentication Users

Table 1-5 lists the operations to configure the ISP domain for centralized MAC address authentication users.

Table 1-5 Configure the ISP domain for MAC address authentication users

Operation	Command	Description
Enter system view	**system-view**	—
Configure the ISP domain for MAC address authentication users	**mac-authentication domain** *isp-name*	Required By default, the "default domain" is used as the ISP domain.

1.2.5 Configuring the Timers Used in Centralized MAC Address Authentication

The following timers are used in centralized MAC address authentication:

- Offline detect timer, which sets the time interval for a switch to test whether a user goes offline. Upon detecting a user is offline, a switch notifies the RADIUS server of the user to trigger the RADIUS server to stop the accounting on the user.
- Quiet timer, which sets the quiet period for a switch. After a user fails to pass the authentication performed by a switch, the switch quiets for a specific period (the quiet period) before it authenticates users again.
- Server timeout timer. During authentication, the switch prohibits the user from accessing the network through the corresponding port if the connection between the switch and RADIUS server times out. In this case, the user can have it authenticated through another port of the switch.

Table 1-6 lists the operations to configure the timers used in centralized MAC address authentication.

Table 1-6 Configure the timers used in centralized MAC address authentication

Operation	Command	Description
Enter system view	**system-view**	—
Configure a timer used in centralized MAC address authentication	**mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }	Optional The default settings of the timers used in centralized MAC address authentication are as follows: • Offline detect timer: 300 seconds • Quiet timer: 60 seconds • Server timeout timer: 100 seconds

1.3 Displaying and Debugging Centralized MAC Address Authentication

After the above configuration, you can execute the **display** command in any view to display system running of centralized MAC address authentication configuration, and to verify the effect of the configuration. You can execute the **reset** command in user view to clear the statistics of centralized MAC address authentication.

Table 1-7 Display and debug centralized MAC address authentication

Operation	Command	Description
Display global or port information about centralized MAC address authentication	**display mac-authentication** [**interface** *interface-list*]	This command can be executed in any view.
Clear the statistics of global or port centralized MAC address authentication	**reset mac-authentication statistics [interface** *interface-type interface-number* **]**	This command is executed in user view

1.4 Centralized MAC Address Authentication Configuration Example

Note:

Centralized MAC address authentication configuration is similar to that of 802.1x. In this example, the differences between the two lie in:

- Centralized MAC address authentication needs to be enabled both globally and for a port.
- In MAC address mode, MAC address of locally authenticated user is used as both user name and password.
- In MAC address mode, MAC address of user authenticated by RADIUS server need to be configured as both user name and password on the RADIUS server.

The following section describes how to enable centralized MAC address authentication globally and for a port, and how to configure a local user. For other related configuration, refer to the configuration examples in “802.1x” Configuration.

Enable centralized MAC address authentication for Ethernet 1/0/2 port.

```
<H3C> system-view
[H3C] mac-authentication interface Ethernet 1/0/2
```

Configure centralized MAC address authentication mode as MAC address mode, and use hyphened MAC addresses as the user names and passwords for authentication.

```
[H3C] mac-authentication authmode usernameasmacaddress userformat with-hyphen
```

Add a local user.

- Configure the user name and password.

```
[H3C] local-user 00-e0-fc-01-01-01
[H3C-luser-00-e0-fc-01-01-01] password simple 00-e0-fc-01-01-01
```

- Set service type of the local user to lan-access.

```
[H3C-luser-00-e0-fc-01-01-01] service-type lan-access
```

Enable centralized MAC address authentication globally.

```
[H3C-luser-00-e0-fc-01-01-01] quit
[H3C] mac-authentication
```

Configure the domain name for centralized MAC address authentication users as aabbcc163.net.

```
[H3C] mac-authentication domain aabbcc163.net
```

For domain-related configuration, refer to the “802.1x” Configuration Example part of this manual.

Table of Contents

Chapter 1 ARP Configuration 1-1
1.1 Introduction to ARP 1-1
1.1.1 Necessity of the Address Resolution 1-1
1.1.2 ARP Packet Structure 1-1
1.1.3 ARP Table 1-2
1.1.4 ARP Implementation Procedure 1-3
1.1.5 Introduction to Gratuitous ARP 1-5
1.2 ARP Configuration 1-6
1.2.1 Adding a Static ARP Mapping Entry Manually 1-6
1.2.2 Configuring the ARP Aging Timer for Dynamic ARP Entries 1-7
1.2.3 Enabling the ARP Entry Checking Function 1-7
1.3 Gratuitous ARP Packet Configuration 1-8
1.3.1 Configuring Sending of Gratuitous ARP Packets 1-8
1.3.2 Configuring the Gratuitous ARP packet Learning Function 1-8
1.4 Displaying and Debugging ARP 1-8
Chapter 2 Resilient ARP Configuration 2-1
2.1 Introduction to Resilient ARP 2-1
2.2 Resilient ARP Configuration 2-1
2.3 Displaying Resilient ARP 2-2
2.4 Resilient ARP Configuration Example 2-2

Chapter 1 ARP Configuration

1.1 Introduction to ARP

Address resolution protocol (ARP) is used to map IP addresses to the corresponding MAC addresses so that packets can be delivered to their destinations correctly.

1.1.1 Necessity of the Address Resolution

After a packet is forwarded to the destination network, MAC address is necessary for the packet to reach the very device. So the destination IP address carried in a packet need to be translated into the corresponding MAC address.

1.1.2 ARP Packet Structure

ARP packets are classified as ARP request packets and ARP reply packets. Figure 1-1 illustrates the structure of these two types of ARP packets.

- As for an ARP request packet, all the fields except the hardware address of the receiver field are set. The hardware address of the receiver is what the sender request for.
- As for an ARP reply packets, all the fields are set.

<table>
<tr><td colspan="2">Hardware type (16 bits)</td></tr>
<tr><td colspan="2">Protocol type (16 bits)</td></tr>
<tr><td>Length of the hardware address</td><td>Length of protocol address</td></tr>
<tr><td colspan="2">Operator (16 bits)</td></tr>
<tr><td colspan="2">Hardware address of the sender</td></tr>
<tr><td colspan="2">IP address of the sender</td></tr>
<tr><td colspan="2">Hardware address of the receiver</td></tr>
<tr><td colspan="2">IP address of the receiver</td></tr>
</table>

Figure 1-1 Structure of an ARP request/reply packet

Table 1-1 describes the fields of an ARP packet.

Table 1-1 Description on the fields of an ARP packet

Field	Description
Hardware Type	Identifies the type of the hardware interface. Refer to Table 1-2 for the information about the field values.
Protocol type	Type of protocol address to be mapped. 0x0800 indicates an IP address.
Length of the hardware address	Hardware address length (in bytes)
Length of protocol address	Protocol address length (in bytes)
Operator	Indicates the type of a data packets, which can be: • 1: ARP request packets • 2: ARP reply packets • 3: RARP request packets • 4: RARP reply packets
Hardware address of the sender	Hardware address of the sender
IP address of the sender	IP address of the sender
Hardware address of the receiver	• For an ARP request packet, this field is null. • For an ARP reply packet, this field carries the hardware address of the receiver.
IP address of the receiver	IP address of the receiver

Table 1-2 Description on the values of the hardware type field

Value	Description
1	Ethernet
2	Experimental Ethernet
3	X.25
4	Proteon ProNET (Token Ring)
5	Chaos
6	IEEE802.X
7	ARC network

1.1.3 ARP Table

In an Ethernet, the MAC addresses of two hosts must be available for the two hosts to communicate with each other. Each host in an Ethernet maintains an ARP mapping table, where the latest used IP address-to-MAC address mapping entries are stored.

Note that this manual only introduces the basic implementation of the mapping table. Different products of different manufactures may provide more information about the mapping table. S3600 series Ethernet switches provide the **display arp** command to display the information about ARP mapping entries. Figure 1-2 shows the structure of an ARP mapping table.

	IF index	Physical address	IP address	Type
Entry 1				
Entry 2				
Entry 3				
Entry 4				
Entry 5				
…				
Entry n				

Figure 1-2 An ARP mapping table

Table 1-3 describes the APR mapping table fields.

Table 1-3 Description on the fields of an ARP table

Field	Description
IF index	Index of the physical interface/port on the device owning the physical address and IP address contained in the entry
Physical address	Physical address of the device, that is, the MAC address
IP address	IP address of the device
Type	Entry type, which can be: • 1: An entry falling out of the following three cases • 2: Invalid entry • 3: Dynamic entry • 4: Static entry

1.1.4 ARP Implementation Procedure

The ARP mapping table of a host is empty when the host is just started up. And when a dynamic ARP mapping entry is not in use for a specified period of time, it is removed from the ARP mapping table so as to save the memory space and shorten the interval

for the switch to look up entries in the ARP mapping table. For details, refer to Figure 1-3.

- 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 that of Host B is IP_B. To send a packet to Host B, Host A checks its own ARP mapping table first to see if the ARP entry corresponding to IP_B exists. If yes, Host A encapsulates the IP packet into a frame with the MAC address of Host B inserted to it and sends it to Host B.
- If the corresponding MAC address is not found in the ARP mapping table, Host A adds the packet in the transmission queue, creates an ARP request packet and broadcasts it throughout the Ethernet. As mentioned earlier, the ARP request packet contains the IP address of Host B, the IP address of Host A, and the MAC address of Host A. Since the ARP request packet is broadcasted, all hosts on the network segment can receive it. However, only the requested host (namely, Host B) processes the request.
- Host B saves the IP address and the MAC address carried in the request packet (that is, the IP address and the MAC address of the sender, Host A) to its ARP mapping table and then sends back an ARP reply packet to the sender (Host A), with its MAC address carried in the packet. Note that the ARP reply packet is a unicast packet instead of a broadcasted packet.
- Upon receiving the ARP reply packet, Host A extracts the IP address and the corresponding MAC address of Host B from the packet, adds them to its ARP mapping table, and then transmits all the packets in the queue with their destination being Host B.

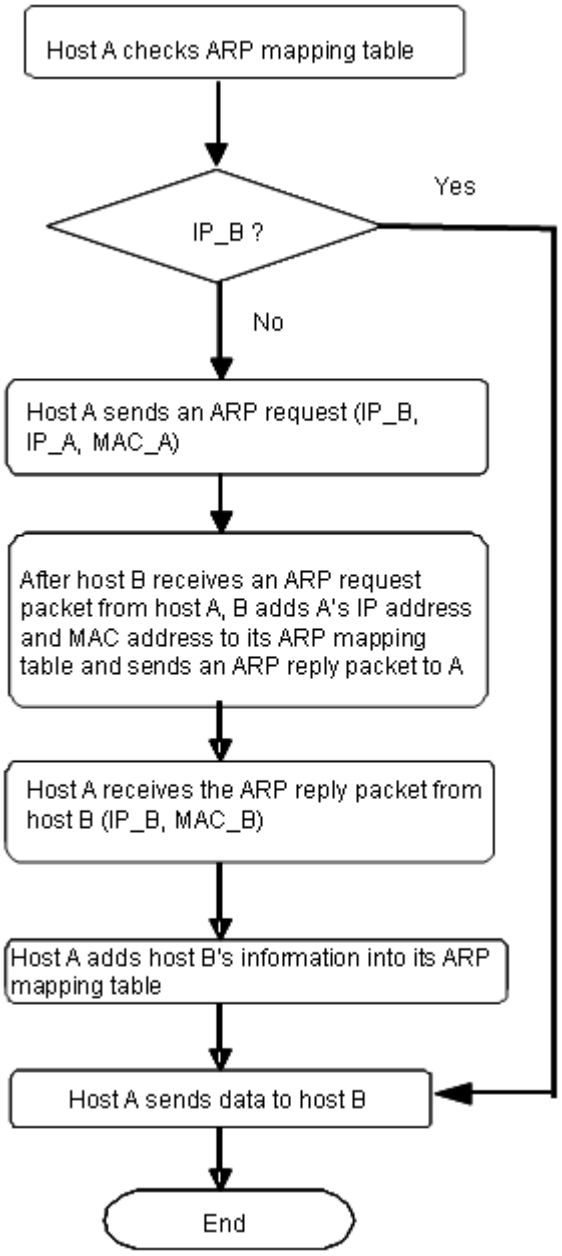


Figure 1-3 ARP work flow

Normally, a device automatically triggers the ARP calculation in the IP addressing process.

1.1.5 Introduction to Gratuitous ARP

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.

The gratuitous ARP packet learning function:

When the gratuitous ARP packet learning function is enabled on a switch and the switch receives a gratuitous ARP packet, the switch updates the existing ARP entry (contained in the cache of the switch) that matches the received gratuitous ARP packet using the hardware address of the sender carried in the gratuitous ARP packet. A switch operates like this whenever it receives a gratuitous ARP packet.

1.2 ARP Configuration

ARP entries in an S3600 series Ethernet switch can either be static entries or dynamic entries, as described in Table 1-4.

Table 1-4 ARP entries

ARP entry	Generation Method	Maintenance Mode
Static ARP entry	Manually configured	Manual maintenance
Dynamic ARP entry	Dynamically generated	ARP entries of this type age with time. The aging period is set by the ARP aging timer.

1.2.1 Adding a Static ARP Mapping Entry Manually

Table 1-5 Add a static ARP mapping entry manually

Operation	Command	Description
Enter system view	**system-view**	—
Add a static ARP mapping entry manually	**arp static** *ip-address mac-address* [*vlan-id interface-type interface-number*]	Required By default, the ARP mapping table is empty, and the address mapping entries are created dynamically by ARP.

Caution:

- Static ARP mapping entries are valid as long as the Ethernet switch operates. But some operations, which make the ARP entries invalid, result in ARP entries being removed, such as changing/removing a VLAN interface, removing a VLAN, or removing a port from a VLAN.
- As for the **arp static** command, the value of the *vlan-id* argument must be the ID of an existing VLAN, and the port identified by the *interface-type* and *interface-number* arguments must belong to the VLAN.
- Currently, static ARP mapping entries cannot be configured on aggregation ports.

1.2.2 Configuring the ARP Aging Timer for Dynamic ARP Entries

The ARP aging timer applies to all dynamic ARP mapping entries.

Table 1-6 Configure the ARP aging timer for dynamic ARP entries

Operation	Command	Description
Enter system view	**system-view**	—
Configure the ARP aging timer	**arp timer aging** *aging-time*	Optional By default, the ARP aging timer is set to 20 minutes.

1.2.3 Enabling the ARP Entry Checking Function

When multiple hosts share one multicast MAC address, you can specify whether or not to create ARP entries for the multicast MAC address by performing the operations listed in Table 1-7.

Table 1-7 Enable the ARP entry checking function

Operation	Command	Description
Enter system view	**system-view**	—
Enable the ARP entry checking function (that is, disable the switch from creating ARP entries for multicast MAC addresses)	**arp check enable**	Optional By default, the ARP entry checking function is enabled.

1.3 Gratuitous ARP Packet Configuration

1.3.1 Configuring Sending of Gratuitous ARP Packets

Sending of gratuitous ARP packets is enabled as long as an S3600 series switch operates. And no command is needed for this function.

1.3.2 Configuring the Gratuitous ARP packet Learning Function

Table 1-8 lists the operations to configure the gratuitous ARP packet learning function.

Table 1-8 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**	Required By default, the gratuitous ARP packet learning function is enabled.

1.4 Displaying and Debugging ARP

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

You can execute the **reset** command in user view to clear ARP mapping entries.

Table 1-9 Display and debug ARP

Operation	Command	Description
Display specific ARP mapping table entries	**display arp** [**static** | **dynamic** | *ip-address*]	These commands can be executed in any view.
Display the ARP mapping entries related to a specified string in a specified way	**display arp** [**dynamic** | **static** | { **begin** | **include** | **exclude** } *text*	
Display the number of the ARP mapping entries of a specified type	**display arp count** [[**dynamic** | **static**] [| { **begin** | **include** | **exclude** } *text*] | *ip-address*]	
Display the setting of the ARP aging timer	**display arp timer aging**	

Operation	Command	Description
Clear specific ARP mapping entries	**reset arp** [**dynamic** | **static** | **interface** *interface-type interface-number*]	Execute this command in user view.

Chapter 2 Resilient ARP Configuration

2.1 Introduction to Resilient ARP

In intelligent resilient framework (IRF) network application, normally you need to connect redundancy links between the fabric and other devices to support the resilient network. But if the connections inside the fabric break off, the fabric splits. In this case, the redundancy link may connect with two or more Layer 3 devices with the same configurations in the same network. Thus these devices operate the same routing function. Adopting the Resilient ARP function can avoid this. Resilient ARP can find whether there are the same Layer 3 devices in the network. If so, it keeps one device as the Layer 3 device, and changes the other devices to be the Layer 2 devices.

The state machine of Resilient ARP has six states which are Initialize, LisentForL3Master, L3Master, L3slave, L2Master, and L2slave. L3Master sends Resilient ARP packets periodically to notify other fabrics that the local fabric is in the Layer 3 state.

Resilient ARP implements the system state switching by sending/receiving Resilient ARP packets periodically, so as to determine a device to work as a Layer 3 device or a Layer 2 device.

2.2 Resilient ARP Configuration

Resilient ARP configuration includes:

- Enable/disable the Resilient ARP function.

When Resilient ARP function is enabled, the system can deal with the devices according to the current state. When the connections inside a fabric break off, Resilient ARP can send Resilient ARP packets through the VLAN interface where the redundancy link resides, so as to determine a device to work as a Layer 3 device or as a Layer 2 device.

- Configure the VLAN interface through which Resilient packets are sent.

You can use the following commands to configure the VLAN interface through which Resilient packets are sent. When no VLAN interface is specified, Resilient packets are sent through the default VLAN interface.

Table 2-1 Configure the Resilient ARP function

Operation	Command	Description
Enter system view	**system-view**	—
Enable the Resilient ARP function	**resilient-arp enable**	Required By default, the Resilient ARP function is enabled.
Configure the VLAN interface through which Resilient packets are sent	**resilient-arp interface vlan-interface** *vlan-id*	Optional By default, Resilient ARP packets are sent through the interface of VLAN 1(VLAN-interface1).

Note that the above configuration specifies the VLAN interface through which Resilient packets are sent, whereas all the VLAN interfaces can receive Resilient ARP packets.

2.3 Displaying Resilient ARP

After the above configuration, you can use the **display** command in any view to display the operation status, and verify the configuration effect through the displayed information.

Table 2-2 Display Resilient ARP

Operation	Command	Description
Display information about the Resilient ARP state	**display resilient-arp** [**unit** *unit-id*]	The **display** command can be executed in any view

2.4 Resilient ARP Configuration Example

I. Network requirements

There are four units in an IRF network: unit 1 to unit 4. Unit 1 and unit 3 connect to another switch (Switch) through link aggregation. If the connection between unit 1 and unit 3 and the connection between unit 2 and unit 4 break off, there will be two Layer 3 switches with the same configuration in the network. In this case, problems occur in packets forwarding between the fabric and the Switch. You can enable the Resilient ARP function for the fabric to avoid the problems. For security concerns, you need to enable MD5 authentication function. The ports through which unit 3 and unit 4 connect to the Switch belong to VLAN 2.

II. Network diagram

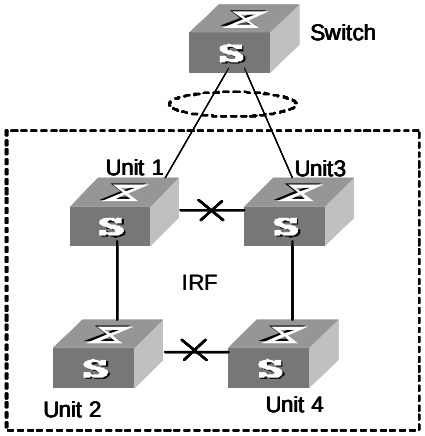


Figure 2-1 Network diagram for Resilient ARP

III. Configuration procedure

Enable the Resilient ARP function.

```
<H3C> system-view
[H3C] resilient-arp enable
```

Configure the Resilient ARP packets to be sent through the VLAN-interface2.

```
[H3C] resilient-arp interface Vlan-interface 2
```

Table of Contents

Chapter 1 DHCP Overview 1-1
1.1 Introduction to DHCP 1-1
1.2 DHCP IP Address Assignment 1-1
1.2.1 IP Address Assignment Policy 1-1
1.2.2 Obtaining IP Addresses Dynamically 1-2
1.2.3 Updating IP Address Lease 1-2
1.3 DHCP Packet Format 1-3
1.4 DHCP Packet Processing Modes 1-4
1.5 Protocol Specification 1-4
Chapter 2 DHCP Server Configuration 2-1
2.1 Introduction to DHCP Server 2-1
2.1.1 Usage of DHCP Server 2-1
2.1.2 IRF Support 2-1
2.1.3 DHCP Address Pool 2-2
2.1.4 DHCP IP Address Preferences 2-3
2.2 Global Address Pool-Based DHCP Server Configuration 2-4
2.2.1 Configuration Overview 2-4
2.2.2 Enabling DHCP 2-4
2.2.3 Configuring Global Address Pool Mode on Interface(s) 2-5
2.2.4 Configuring How to Assign IP Addresses in a Global Address Pool 2-6
2.2.5 Configuring DNS Services for the DHCP Server 2-9
2.2.6 Configuring DHCP Server to Assign WINS Server Addresses 2-10
2.2.7 Customizing DHCP Service 2-11
2.2.8 Configuring Gateway Addresses for DHCP Clients 2-11
2.2.9 Configuring Connection Between a DHCP Global Address Pool and a BIMS Server 2-12
2.3 Interface Address Pool-based DHCP Server Configuration 2-13
2.3.1 Configuration Overview 2-13
2.3.2 Enabling DHCP 2-14
2.3.3 Configuring to Assign the IP Addresses of Interface Address Pools to DHCP Clients 2-14
2.3.4 Configuring the Mode to Assign IP Addresses to DHCP Clients 2-15
2.3.5 Configuring DNS Services for the DHCP Server 2-17
2.3.6 Configuring DHCP Servers to Assign WINS Server Addresses 2-18
2.3.7 Customizing DHCP Service 2-20
2.3.8 Configuring Connection Between the DHCP Interface Address Pool and the BIMS Server 2-20
2.4 DHCP Security Configuration 2-21
2.4.1 Prerequisites 2-21

2.4.2 Configuring Private DHCP Server Detecting 2-21
2.4.3 Configuring IP Address Detecting 2-21
2.5 Option 82 Supporting Configuration 2-22
2.5.1 Introduction to DHCP-Server Option 82 2-22
2.5.2 Configuration Prerequisites 2-22
2.5.3 Configuring the Option 82 Supporting Function 2-22
2.6 Option 184 Supporting Configuration 2-23
2.6.1 Introduction to Option 184 2-23
2.6.2 Prerequisites 2-25
2.6.3 Configuring the Option 184 Supporting Function 2-25
2.6.4 Configuration Example 2-28
2.7 Displaying and Debugging a DHCP Server 2-30
2.8 DHCP Server Configuration Example 2-31
2.9 Troubleshooting a DHCP Server 2-33

Chapter 3 DHCP Relay Configuration 3-1
3.1 Introduction to DHCP Relay 3-1
3.1.1 Usage of DHCP Relay 3-1
3.1.2 DHCP Relay Fundamentals 3-1
3.1.3 Option 82 Supporting 3-2
3.2 DHCP Relay Configuration 3-4
3.2.1 DHCP Relay Configuration Tasks 3-4
3.2.2 Enabling DHCP 3-4
3.2.3 Configuring an Interface to Operate in DHCP Relay Mode 3-4
3.2.4 Configuring DHCP Relay Security 3-6
3.2.5 Configuring Option 82 Supporting 3-9
3.3 Displaying and Debugging DHCP Relay 3-10
3.4 DHCP Relay Configuration Example 3-10
3.5 Troubleshooting DHCP Relay 3-12

Chapter 4 DHCP Snooping Configuration 4-1
4.1 Introduction to DHCP Snooping 4-1
4.2 DHCP Snooping Configuration 4-3
4.3 Displaying DHCP Snooping 4-3
4.4 Configuration Example 4-4

Chapter 5 DHCP Accounting Configuration 5-1
5.1 Introduction to DHCP Accounting 5-1
5.1.1 DHCP Accounting Fundamentals 5-1
5.2 DHCP Accounting Configuration 5-1
5.2.1 Prerequisites 5-1
5.2.2 Configuring DHCP Accounting 5-2
5.2.3 DHCP Accounting Configuration Example 5-2

Chapter 1 DHCP Overview

1.1 Introduction to DHCP

With networks getting larger in size and more complicated in structure, lack of available IP addresses becomes the common situation the network administrators have to face, and network configuration becomes a tough task for the network administrators. With the emerging of wireless networks and the using of laptops, the position change of hosts and frequent change of IP addresses also require new technology. Dynamic host configuration protocol (DHCP) is developed in this background.

DHCP adopts a client/server model, where DHCP clients send requests to DHCP servers for configuration parameters; and the DHCP servers return the corresponding configuration information such as IP addresses to configure IP addresses dynamically.

A typical DHCP application includes one DHCP server and multiple clients (such as PCs and laptops), as shown in Figure 1-1.

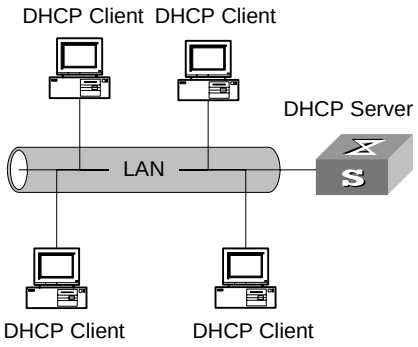


Figure 1-1 Typical DHCP application

1.2 DHCP IP Address Assignment

1.2.1 IP Address Assignment Policy

Currently, DHCP provides the following three IP address assignment policies to meet the requirements of different clients:

- Manual assignment. The administrator statically binds IP addresses to few clients with special uses (such as WWW server). Then the DHCP server assigns these fixed IP addresses to the clients.
- Automatic assignment. The DHCP server assigns IP addresses to DHCP clients. The IP addresses will be occupied by the DHCP clients permanently.

- Dynamic assignment. The DHCP server assigns IP addresses to DHCP clients for predetermined period of time. In this case, a DHCP client must apply for an IP address again at the expiration of the period. This policy applies to most clients.

1.2.2 Obtaining IP Addresses Dynamically

A DHCP client undergoes the following four phases to dynamically obtain an IP address from a DHCP server:

1) Discover: In this phase, the DHCP client tries to find a DHCP server by broadcasting a DHCP-DISCOVER packet.
2) Offer: In this phase, the DHCP server offers an IP address. After the DHCP server receives the DHCP-DISCOVER packet, it chooses an unassigned IP address according to the priority order of IP address assignment and then sends the IP address and other configuration information together in a DHCP-OFFER packet to the DHCP client. The sending mode is decided by the flag filed in the DHCP-DISCOVER packet, refer to section 1.3 "DHCP Packet Format" for detail.
3) Select: In this phase, the DHCP client selects an IP address. If more than one DHCP server sends DHCP-OFFER packets to the DHCP client, the DHCP client only accepts the DHCP-OFFER packet that first arrives, and then broadcasts a DHCP-REQUEST packet containing the assigned IP address carried in the DHCP-OFFER packet.
4) Acknowledge: In this phase, the DHCP servers acknowledge the IP address. Upon receiving the DHCP-REQUEST packet, only the selected DHCP server returns a DHCP-ACK packet to the DHCP client to confirm the assignment of the IP address to the client, or returns a DHCP-NAK packet to refuse the assignment of the IP address to the client. When the client receives the DHCP-ACK packet, it broadcasts an ARP packet with the assigned IP address as the destination address to detect the assigned IP address, and uses the IP address only if it does not receive any response within a specified period.

Note:

The IP addresses offered by other DHCP servers but not used by the DHCP client are still available to other clients.

1.2.3 Updating IP Address Lease

After a DHCP server dynamically assigns an IP address to a DHCP client, the IP address keeps valid only within a specified lease time and will be reclaimed by the DHCP server when the lease expires. If the DHCP client wants to use the IP address for a longer time, it must update the IP lease.

By default, a DHCP client updates its IP address lease automatically by unicasting a DHCP-REQUEST packet to the DHCP server when half of the lease time elapses. The DHCP server responds with a DHCP-ACK packet to notify the DHCP client of a new IP lease if the server can assign the same IP address to the client. Otherwise, the DHCP server responds with a DHCP-NAK packet to notify the DHCP client that the IP address will be reclaimed when the lease time expires.

If the DHCP client fails to update its IP address lease when half of the lease time elapses, it will update its IP address lease by broadcasting a DHCP-REQUEST packet to the DHCP servers again when seven-eighths of the lease time elapses. The DHCP server performs the same operations as those described above.

1.3 DHCP Packet Format

DHCP has eight types of packets. They have the same format, but the values of some fields in the packets are different. The DHCP packet format is based on that of the BOOTP packets. The following figure describes the packet format (the number in the brackets indicates the field length, in bytes):

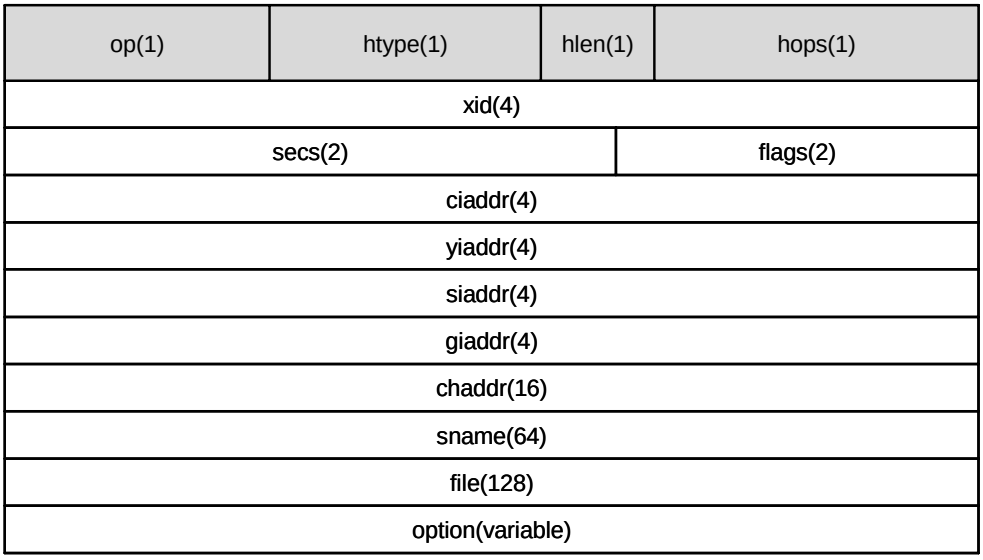


Figure 1-2 DHCP packet format

The fields are described as follows:

- op: Operation types of DHCP packets, 1 for request packets and 2 for response packets.
- htype, hlen: Hardware address type and length of the DHCP client.
- hops: Number of DHCP relays which a DHCP packet passes. For each DHCP relay that the DHCP request packet passes, the field value increases by 1.
- xid: Random number that the client selects when it initiates a request. The number is used to identify an address-requesting process.
- secs: Elapsed time after the DHCP client initiates a DHCP request.

- flags: The first bit is the broadcast response flag bit. It is used to identify that the DHCP response packet is sent in the unicast or broadcast mode. Other bits are reserved.
- ciaddr: IP address of a DHCP client.
- yiaddr: IP address that the DHCP server assigns to a client.
- siaddr: IP address of the DHCP server.
- giaddr: IP address of the first DHCP relay that the request packet sent by the DHCP client passes.
- chaddr: Hardware address of the DHCP client.
- sname: Name of the DHCP server.
- file: Path and name of the boot configuration file that the DHCP server specifies for the DHCP client.
- option: Optional variable-length fields, including packet type, valid lease time, IP address of a DNS server, and IP address of the WINS server.

1.4 DHCP Packet Processing Modes

After the DHCP is enabled on a device, the device processes the DHCP packet received from a DHCP client in one of the following three modes depending on your configuration:

- Global address pool: In response to the DHCP packets received from DHCP clients, the DHCP server picks IP addresses from its global address pools and assigns them to the DHCP clients.
- Interface address pool: In response to the DHCP packets received from DHCP clients, the DHCP server picks IP addresses from the interface address pools and assigns them to the DHCP clients. If there is no available IP address in the interface address pools, the DHCP server picks IP addresses from its global address pool that contains the interface address pool segment and assigns them to the DHCP clients.
- Relay: DHCP packets received from DHCP clients are forwarded to an external DHCP server, which assigns IP addresses to the DHCP clients.

You can specify the mode to process DHCP packets. For the configuration of the first two modes, see Chapter 2 DHCP Server Configuration. For the configuration of the trunk mode, see Chapter 3 DHCP Relay Configuration.

One interface only corresponds to one mode. In this case, the new configuration overwrites the previous one.

1.5 Protocol Specification

Protocol specifications related to DHCP include:

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions

- RFC1542: Clarifications and Extensions for the Bootstrap Protocol

Chapter 2 DHCP Server Configuration

Note:

The contents of this chapter are only applicable to the S3600-EI series among S3600 series switches.

2.1 Introduction to DHCP Server

2.1.1 Usage of DHCP Server

Generally, DHCP servers are used in the following networks to assign IP addresses:

- Large-sized networks, where manual configuration method bears heavy load and is difficult to manage the whole network in centralized way.
- Networks where the number of available IP addresses is less than that of the hosts. In this type of networks, IP addresses are not enough for all the hosts to obtain a fixed IP address, and the number of on-line users is limited (such is the case in an ISP network). In these networks, a great number of hosts must dynamically obtain IP addresses through DHCP.
- Networks where only a few hosts need fixed IP addresses and most hosts do not need fixed IP addresses.

2.1.2 IRF Support

In an IRF (intelligent resilient framework) system, DHCP servers operate in a centralized way to fit the IRF environment.

- DHCP servers run (as tasks) on all the units (including the master unit and the slave units) in a Fabric system. But only the one running on the master unit receives/sends packets and carries out all functions of a DHCP server. Those running on the slave units only operate as the backup tasks of the one running on the master unit.
- When a slave unit receives a DHCP-REQUEST packet, it redirects the packet to the DHCP server on the master unit, which returns a DHCP-ACK/DHCP-NAK packet to the DHCP client and at the same time backs up the related information to the slave units. In this way, when the current master unit fails, one of the slaves can change to the master and operates as the DHCP server immediately.
- DHCP is an UDP-based protocol operating at the application layer. When a DHCP server in a fabric system runs on a Layer 2 network device, DHCP packets are

directly forwarded by hardware instead of being delivered to the DHCP server, or being redirected to the master unit by UDP HELPER. This idles the DHCP server. DHCP packets can be redirected to the DHCP server on the master unit by UDP HELPER only when the Layer 2 device is upgraded to a Layer 3 device.

Caution:

- When you merge two or more IRF systems into one IRF system, a new master unit is elected, and the new IRF system adopts new configurations accordingly. This may result in the existing system configurations (including the address pools configured for the DHCP servers) being lost. As the new IRF system cannot inherit the original DHCP server configurations, you need to perform DHCP server configurations for it.
- When an IRF system is split into multiple new IRF systems, some of the new IRF systems may be degraded to Layer 2 devices. For a new IRF system degraded to Layer 2 device, although the original DHCP server still exists in the new system, it runs idle for being unable to receive any packets. When the IRF system restores to a Layer 3 device due to being merged into a new IRF system, it adopts the configurations on the new IRF system. And you need to perform DHCP server configurations if the new IRF system does not have DHCP server-related configurations.
- In an IRF system, the UDP HELPER function must be enabled on the DHCP servers that are in fabric state.

2.1.3 DHCP Address Pool

A DHCP address pool holds the IP addresses to be assigned to DHCP clients. When a DHCP server receives a DHCP request from a DHCP client, it selects an address pool depending on the configuration, picks an IP address from the pool and sends the IP address and other related parameters (such as the IP address of the DNS server, and the lease time of the IP address) to the DHCP client.

I. Types of address pool

The address pools of a DHCP server fall into two types: global address pool and interface address pool.

- A global address pool is created by executing the **dhcp server ip-pool** command in system view. It is valid on the current device.
- If an interface is configured with a valid unicast IP address, you can create an interface-based address pool for the interface by executing the **dhcp select interface** command in interface view. The IP addresses an interface address pool

holds belong to the network segment the interface resides in and are available to the interface only.

II. The structure of an address pool

The address pools of a DHCP server are hierarchically organized in a tree-like structure. The root holds the IP address of the natural network segment, the branches hold the subnet IP addresses, and the leaves holds the IP addresses that are manually bound to specific clients. The address pools that are of the same level are sorted by their configuration precedence order. Such a structure enables configurations to be inherited. That is, the configurations of the natural network segment can be inherited by its subnets, whose configurations in turn can be inherited by their client address. So, for the parameters that are common to the whole network segment or some subnets (such as domain name), you just need to configure them on the network segment or the corresponding subnets. The following is the details of configuration inheritance.

1) A newly created child address pool inherits the configurations of its parent address pool.
2) For an existing parent-child address pool pair, when you performs a new configuration on the parent address pool:

- The child address pool inherits the new configuration if there is no corresponding configuration on the child address pool.
- The child address pool does not inherit the new configuration if there is already a corresponding configuration on the child address pool.

2.1.4 DHCP IP Address Preferences

Interfaces of the DHCP server can work in the global address pool mode or in the interface address pool mode. If the DHCP server works in the interface address pool mode, it picks IP addresses from the interface address pools and assigns them to the DHCP clients. If there is no available IP address in the interface address pools, the DHCP server picks IP addresses from its global address pool that contains the interface address pool segment and assigns them to the DHCP clients.

A DHCP server assigns IP addresses in interface address pools or global address pools to DHCP clients in the following sequence:

- IP addresses that are statically bound to the MAC addresses of DHCP clients or client IDs
- IP addresses that are ever used by DHCP clients. That is, those in the assigned leases recorded by the DHCP server. If there is no record in the leases and the DHCP-DISCOVER packets sent by DHCP clients contain option 50 fields, the DHCP server assigns the IP address requested by option 50.
- The first IP address found among the available IP addresses in the DHCP address pool.

- If no IP address is available, the DHCP server queries lease-expired and conflicted IP addresses. If the DHCP server finds such IP addresses, it assigns them; otherwise the DHCP server does not assign an IP address.

2.2 Global Address Pool-Based DHCP Server Configuration

2.2.1 Configuration Overview

Table 2-1 Configure global address pool-based DHCP server

Configuration task		Description	Related section
Enable DHCP		Required	2.2.2 “Enabling DHCP”
Configure global address pool mode on interface(s)		Optional	2.2.3 “Configuring Global Address Pool Mode on Interface(s)”
Configure the interface(s) to operate in global address pool mode	Configure to bind IP address statically to a DHCP client	One of the two options is required. Only one mode can be selected for the same global address pool.	2.2.4 “Configuring How to Assign IP Addresses in a Global Address Pool”
	Configure to assign IP addresses dynamically		
Configure DNS services for the DHCP server		Optional	2.2.5 “Configuring DNS Services for the DHCP ”
Configure NetBIOS services for the DHCP server		Optional	2.2.6 “Configuring DHCP Server”
Customize DHCP service		Optional	2.2.7 “Customizing DHCP Service”
Configure the gateway IP address for DHCP clients		Optional	2.2.8 “Configuring Gateway Addresses for DHCP Clients”
Configure the connection between the DHCP global address pool and the BIMS server		Optional	2.2.9 “Configuring Connection Between a DHCP Global Address Pool and a BIMS Server”

2.2.2 Enabling DHCP

You need to enable DHCP before performing other DHCP-related configurations, which takes effect only after DHCP is enabled.

Table 2-2 Enable DHCP

Operation	Command	Description
Enter system view	**system-view**	—
Enable DHCP	**dhcp enable**	Required By default, DHCP is enabled

Note:

To improve security and avoid malicious attack to the unused SOCKETs, S3600 Ethernet switches provide the following functions:

- UDP 67 and UDP 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP 67 and UDP 68 ports are disabled when DHCP is disabled.

The corresponding implementation is as follows:

- After DHCP is enabled by executing the **dhcp enable** command, if the DHCP server and DHCP relay functions are not configured, UDP 67 and UDP 68 ports are kept disabled; if the DHCP server / DHCP relay function is configured, UDP 67 and UDP 68 ports are enabled.
- After DHCP is disabled by executing the **undo dhcp enable** command, even if the DHCP server and DHCP relay functions are configured, UDP 67 and UDP 68 ports will be disabled.

2.2.3 Configuring Global Address Pool Mode on Interface(s)

You can configure the global address pool mode on the specified or all interfaces of a DHCP server. After that, when the DHCP server receives DHCP packets from DHCP clients through these interfaces, it assigns IP addresses in the global address pool to the DHCP clients.

Table 2-3 Configure the global address pool mode on interface(s)

Operation		Command	Description
Enter system view		**system-view**	—
Configure the specified interface(s) or all the interfaces to operate in global address pool mode	Configure the current interface	**interface** *interface-type interface-number*	Optional By default, the interface operates in global address pool mode.
		dhcp select global	
		quit	
	Configure multiple interfaces simultaneously in system view	**dhcp select global** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

2.2.4 Configuring How to Assign IP Addresses in a Global Address Pool

You can specify to bind an IP address in a global address pool statically to a DHCP client or assign IP addresses in the pool dynamically to DHCP clients as needed. In a global address pool, you can only bind one IP address statically to a DHCP client and assign other IP addresses in the pool dynamically to DHCP clients.

For dynamic IP address assigning, you need to specify the range of the IP addresses to be dynamically assigned. But for static IP address binding, you can regard that the IP address statically bound to a DHCP client comes from a special DHCP address pool that contains only one IP address.

I. Configuring to assign IP addresses by static binding

Some DHCP clients, such as WWW servers, need fixed IP addresses. This can be achieved by binding IP addresses to the MAC addresses of these DHCP clients. When such a DHCP client applies for an IP address, the DHCP server searches for the IP address corresponding to the MAC address of the DHCP client and assigns the IP address to the DHCP client.

When some DHCP clients send DHCP-DISCOVER packets to the DHCP server to apply for IP addresses, they construct client IDs and add them in the DHCP-DISCOVER packets. The DHCP server finds the corresponding IP addresses based on the client IDs and assigns them to the DHCP clients.

Currently, only one IP address in a global DHCP address pool can be statically bound to a MAC address or a client ID.

Table 2-4 Configure to assign IP addresses by static binding

Operation		Command	Description
Enter system view		**system-view**	—
Create a DHCP address pool and enter DHCP address pool view		**dhcp server ip-pool** *pool-name*	Required By default, no global DHCP address pool is created.
Configure an IP address to be statically bound		**static-bind ip-address** *ip-address* [**mask** *mask*]	Required By default, no IP address is statically bound.
Bind an IP address to the MAC address of a DHCP client or a client ID statically	Configure the MAC address to which the IP address is to be statically bound	**static-bind mac-address** *mac-address*	One of these two options is required. By default, no MAC address or client ID to which an IP address is to be statically bound is configured.
	Configure the client ID to which the IP address is to be statically bound	**static-bind client-identifier** *client-identifier*	

Note:

- The **static-bind ip-address** command and the **static-bind mac-address** command or the **static-bind client-identifier** command must be coupled.
- In the same global DHCP address pool, if you configure the **static-bind client-identifier** command after configuring the **static-bind mac-address** command, the new configuration overwrites the previous one, and vice versa.
- In the same global DHCP address pool, if the **static-bind ip-address** command, the **static-bind mac-address** command, or the **static-bind client-identifier** is executed repeatedly, the new configuration overwrites the previous one.
- The IP address to be statically bound cannot be an interface IP address of the DHCP server; otherwise static binding does not take effect.
- A client can permanently use the statically-bound IP address that it has obtained. The IP address is not limited by the lease time of the IP addresses in the address pool.

Note:

To improve security and avoid malicious attack to the unused SOCKETs, S3600 Ethernet switches provide the following functions:

- UDP 67 and UDP 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP 67 and UDP 68 ports are disabled when DHCP is disabled.

The corresponding implementation is as follows:

- After a DHCP address pool is created by executing the **dhcp server ip-pool** command, the UDP 67 and UDP 68 ports used by DHCP are enabled.
- After a DHCP address pool is deleted by executing the **undo dhcp server ip-pool** command and all other DHCP functions are disabled, UDP 67 and UDP 68 ports used by DHCP are disabled accordingly.

II. Configuring to assign IP addresses dynamically

IP addresses dynamically assigned to DHCP clients (including those that are permanently leased and those that are temporarily leased) belong to addresses segments that are previously specified. Currently, an address pool can contain only one address segment, whose ranges are determined by the subnet mask.

To avoid IP address conflicts, the IP addresses to be dynamically assigned to DHCP clients are those that are not occupied by specific network devices (such as gateways and FTP servers).

The lease time can differ with address pools. But that of the IP addresses of the same address pool are the same. Lease time is not inherited, that is to say, the lease time of a child address pool is not affected by the configuration of the parent address pool.

Table 2-5 Configure to assign IP addresses dynamically

Operation	Command	Description
Enter system view	**system-view**	—
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no global DHCP address pool is created
Set the IP address segment whose IP address are to be assigned dynamically	**network** *ip-address* [**mask** *mask*]	Required By default, no IP address segment is set. That is, no IP address is available for being assigned
Configure the lease time	**expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }	Optional The default lease time is one day

Operation	Command	Description
Return to system view	**quit**	—
Specify the IP addresses that are not dynamically assigned	**dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]	Optional By default, all IP addresses in a DHCP address pool are available for being dynamically assigned

Note:

- In the same DHCP global address pool, the **network** command can be executed repeatedly. In this case, the new configuration overwrites the previous one.
- The **dhcp server forbidden-ip** command can be executed repeatedly. That is, you can configure multiple IP addresses that are not dynamically assigned to DHCP clients.
- If an IP address that is not to be automatically assigned has been configured as a statically-bound IP address, the DHCP server still assigns this IP address to the client whose MAC address has been bound.

2.2.5 Configuring DNS Services for the DHCP Server

If a host accesses the Internet through domain names, DNS (domain name system) is needed to translate the domain names into the corresponding IP addresses. To enable DHCP clients to access the Internet through domain names, a DHCP server is required to provide DNS server addresses while assigning IP addresses to DHCP clients. Currently, you can configure up to eight DNS server addresses for a DHCP address pool.

On a DHCP server, you can configure domain names to be used by DHCP clients for address pools. After you do this, the DHCP server provides the domain names together with the assigned IP addresses to the DHCP clients.

Table 2-6 Configure DNS services for the DHCP server

Operation	Command	Description
Enter system view	**system-view**	—
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no global DHCP address pool is created.

Operation	Command	Description
Configure a domain name for DHCP clients	**domain-name** *domain-name*	Required By default, no domain name is configured for DHCP clients.
Configure DNS server addresses for DHCP clients	**dns-list** *ip-address*&<1-8>	Required By default, no DNS server address is configured.

2.2.6 Configuring DHCP Server to Assign WINS Server Addresses

For Microsoft Windows-based DHCP clients that communicate through NetBIOS protocol, the host name-to-IP address translation is carried out by Windows internet naming service (WINS) servers. So you need to perform WINS-related configuration for most Windows-based hosts. Currently, you can configure up to eight WINS addresses for a DHCP address pool.

Host name-to-IP address mappings are needed for DHCP clients communicating through NetBIOS protocol. According to the way to establish the mapping, NetBIOS nodes fall into the following four categories:

- B-node. Nodes of this type establish their mappings through broadcasting (The character b stands for the word broadcast). The source node obtains the IP address of the destination node by sending the broadcast packet containing the host name of the destination node. After receiving the broadcast packet, the destination node returns its IP address to the source node.
- P-node. Nodes of this type establish their mappings by sending unicast packets to WINS servers. (The character p stands for peer-to-peer). The source node sends the unicast packet to the WINS server. After receiving the unicast packet, the WINS server returns the IP address corresponding to the destination node name to the source node.
- M-node. Nodes of this type are p-nodes mixed with broadcasting features (The character m stands for the word mixed), that is to say, this type of nodes obtain mappings by sending broadcast packets first. If they fail to obtain mappings, they send unicast packets to the WINS server to obtain mappings.
- H-node. Nodes of this type are b-nodes mixed with peer-to-peer features. (The character h stands for the word hybrid), that is to say, this type of nodes obtain mappings by sending unicast packets to WINS servers first. If they fail to obtain mappings, they send broadcast packets to obtain mappings.

Table 2-7 Configure DHCP server to assign WINS server addresses

Operation	Command	Description
Enter system view	**system-view**	—
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no global DHCP address pool is created.
Configure WINS server addresses for DHCP clients	**nbns-list** *ip-address*&<1-8>	Required By default, no WINS server address is configured.
Configure DHCP clients to be of a specific NetBIOS node type	**netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }	Optional By default, no NetBIOS node type of the DHCP client is specified and a DHCP client uses an h-node.

2.2.7 Customizing DHCP Service

With the evolution of DHCP, new options are constantly coming into being. You can add the new options as the properties of DHCP servers by performing the following configuration.

Table 2-8 Customize DHCP service

Operation	Command	Description
Enter system view	**system-view**	—
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no global DHCP address pool is created.
Configure customized options	**option** *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> }	Required By default, no customized option is configured.

2.2.8 Configuring Gateway Addresses for DHCP Clients

Gateways are necessary for DHCP clients to access servers/hosts outside the current network segment. After you configure gateway addresses on a DHCP server, the DHCP server provides the gateway addresses to DHCP clients as well while assigning IP addresses to them.

You can configure gateway addresses for address pools on a DHCP server. Currently, you can configure up to eight gateway addresses for a DHCP address pool.

Table 2-9 Configure gateway addresses for DHCP clients

Operation	Command	Description
Enter system view	**system-view**	—
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no global DHCP address pool is created.
Configure gateway addresses for DHCP clients	**gateway-list** *ip-address*&<1-8>	Required By default, no gateway address is configured.

2.2.9 Configuring Connection Between a DHCP Global Address Pool and a BIMS Server

Branch intelligent management system (BIMS) is a kind of network management software, provided by H3C Technologies Co., Ltd. With BIMS you can manage and monitor network devices that dynamically obtain IP addresses universally and effectively.

After configuring the connection between the DHCP global address pool and the BIMS server, you can enable the BIMS server to manage the devices that have obtained IP addresses from the global address pool.

Table 2-10 Configure connection between a DHCP global address pool and a BIMS server

Operation	Command	Description
Enter system view	**system-view**	—
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no DHCP global address pool is created.
Configure the connection between the DHCP global address pool and the BIMS server	**bims-server ip** *ip-address* [**port** *port-number*] **sharekey** *key*	Required By default, no connection between the DHCP global address pool and the BIMS server is configured.

2.3 Interface Address Pool-based DHCP Server Configuration

Caution:

In the interface address pool mode, after the addresses in the interface address pool have been assigned, the DHCP server picks IP addresses from the global interface address pool containing the segment of the interface address pool and assigns them to the DHCP clients. As a result, the IP addresses obtained from global address pools and those obtained from interface address pools are not in the same network segment, so the clients cannot interoperate with each other.

Therefore, in the interface address pool mode, if the IP addresses in the same address pool are required to be assigned to the clients on the same VLAN interface, the number of clients that obtain IP addresses automatically cannot exceed the number of the IP addresses that can be assigned in the interface address pool.

2.3.1 Configuration Overview

An interface address pool is created when the interface is assigned a valid unicast IP address and you execute the **dhcp select interface** command in interface view. The IP addresses contained in it belong to the network segment where the interface resides in and are available to the interface only.

You can perform certain configurations for DHCP address pools of an interface or multiple interfaces within specified interface ranges. Configuring for multiple interfaces eases configuration work load and makes you to configure in a more convenient way.

Table 2-11 Overview of interface address pool-based DHCP server configuration

Configuration task	Description	Related section
Enable DHCP	Required	2.3.2 “Enabling DHCP”
Configure to assign the IP addresses of the local interface-based address pools to DHCP clients	Required	2.3.3 “Configuring to Assign the IP Addresses of Interface Address Pools to DHCP Clients”

Configuration task		Description	Related section
Configure to assign IP addresses of DHCP interface address pool to DHCP clients	Configure to bind IP address statically to DHCP clients	You must choose at least one of the two options. And these two options can be configured at the same time.	2.3.4 "Configuring the Mode to Assign IP Addresses to DHCP Clients"
	Configure to assign IP addresses dynamically		
Configure DNS service for the DHCP server		Optional	2.3.5 "Configuring DNS Services for the DHCP Server"
Configure NetBIOS service for the DHCP server		Optional	2.3.6 "Configuring DHCP Servers"
Customize DHCP service		Optional	2.3.7 "Customizing DHCP Service"
Configure the connection between the DHCP interface address pool and the BIMS server		Optional	2.3.8 "Configuring Connection Between the DHCP Interface Address Pool and the BIMS Server"

2.3.2 Enabling DHCP

You need to enable DHCP before performing DHCP configurations. DHCP-related configurations are valid only when DHCP is enabled.

Table 2-12 Enable DHCP

Operation	Command	Description
Enter system view	**system-view**	—
Enable DHCP	**dhcp enable**	Required By default, DHCP is enabled

2.3.3 Configuring to Assign the IP Addresses of Interface Address Pools to DHCP Clients

If the DHCP server works in the interface address pool mode, it picks IP addresses from the interface address pools and assigns them to the DHCP clients. If there is no available IP address in the interface address pools, the DHCP server picks IP addresses from its global address pool that contains the interface address pool segment and assigns them to the DHCP clients.

Table 2-13 Configure to assign the IP addresses of interface address pools to DHCP clients

Operation		Command	Description
Enter system view		**system-view**	—
Configure to assign the IP addresses of interface address pools to DHCP clients	Configure the current interface	**interface** *interface-type interface-number*	Required By default, a DHCP server assigns the IP addresses of the global address pool to DHCP clients.
		dhcp select interface	
		quit	
	Configure multiple interfaces in system view	**dhcp select interface** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

Note:

To improve security and avoid malicious attack to the unused SOCKETs, S3600 Ethernet switches provide the following functions:

- UDP 67 and UDP 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP 67 and UDP 68 ports are disabled when DHCP is disabled.

The corresponding implementation is as follows:

- After a DHCP interface address pool is created by executing the **dhcp select interface** command, UDP 67 and UDP 68 ports used by DHCP are enabled.
- After a DHCP interface address pool is deleted by executing the **undo dhcp select interface** command and all other DHCP functions are disabled, UDP 67 and UDP 68 ports used by DHCP are disabled accordingly.

2.3.4 Configuring the Mode to Assign IP Addresses to DHCP Clients

IP addresses of an interface address pool can be statically bound to DHCP clients or dynamically allocated to DHCP clients.

I. Configuring to assign IP addresses by static binding

Some DHCP clients, such as WWW servers, need fixed IP addresses. This is achieved by binding IP addresses to the MAC addresses of these DHCP clients. When such a DHCP client applies for an IP address, the DHCP server finds the IP address corresponding to the MAC address of the DHCP client, and then assigns the IP address to the DHCP client.

When some DHCP clients send DHCP-DISCOVER packets to the DHCP server to apply for IP addresses, they construct client IDs and add them in the

DHCP-DISCOVER packets. The DHCP server finds the corresponding IP addresses based on the client IDs and assigns them to the DHCP clients.

Table 2-14 Configure to assign IP addresses by static binding

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Configure static binding	**dhcp server static-bind ip-address** *ip-address* { **client-identifier** *client-identifier* | **mac-address** *mac-address* }	Required By default, static binding is not configured

Note:

- The IP addresses statically bound in interface address pools and the interface IP addresses must be in the same segment.
- There is no limit to the number of IP addresses statically bound in an interface address pool, but the IP addresses statically bound in interface address pools and the interface IP addresses must be in the same segment.
- An IP address can be statically bound to only one MAC address or one client ID. A MAC address or client ID can be bound with only one IP address statically.
- The IP address to be statically bound cannot be an interface IP address of the DHCP server; otherwise the static binding does not take effect.

II. Configuring to assign IP addresses dynamically

As an interface-based address pool is created after the interface is assigned a valid unicast IP address, the IP addresses contained in the address pool belong to the network segment where the interface resides in and are available to the interface only. So specifying the range of the IP addresses to be dynamically assigned is unnecessary.

To avoid IP address conflicts, the IP addresses to be dynamically assigned to DHCP clients are those not occupied by specific network devices (such as gateways and FTP servers).

The lease time can differ with address pools. But that of the IP addresses of the same address pool are the same. Lease time is not inherited, that is to say, the lease time of a child address pool is not affected by the configuration of the parent address pool.

Table 2-15 Configure to assign IP addresses dynamically

Operation		Command	Description
Enter system view		**system-view**	—
Configure the lease time	Configure for the current interface	**interface** *interface-type interface-number*	Optional The default lease time is one day
		dhcp server expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }	
		quit	
	Configure multiple interfaces in system view	**dhcp server expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
Specify the IP addresses that are not dynamically assigned		**dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]	Optional By default, all IP addresses in a DHCP address pool are available for being dynamically assigned.

Note:

- The **dhcp server forbidden-ip** command can be executed repeatedly. That is, you can configure multiple IP addresses that are not dynamically assigned to DHCP clients.
- Use the **dhcp server forbidden-ip** command to configure the IP addresses that are not assigned dynamically in global address pools and interface address pools.
- If an IP address that is not to be automatically assigned has been configured as a statically-bound IP address, the DHCP server still assigns this IP address to the client whose MAC address has been bound.

2.3.5 Configuring DNS Services for the DHCP Server

If a host accesses the Internet through domain names, DNS is needed to translate the domain names into the corresponding IP addresses. To enable DHCP clients to access the Internet through domain names, a DHCP server is required to provide DNS server addresses while assigning IP addresses to DHCP clients. Currently, you can configure up to eight DNS server addresses for a DHCP interface address pool.

On the DHCP server, you can configure domain names to be used by DHCP clients for address pools. After you do this, the DHCP server provides the domain names to the DHCP clients while the DHCP server assigns IP addresses to the DHCP clients.

Table 2-16 Configure DNS services for the DHCP server

Operation		Command	Description
Enter system view		**system-view**	—
Configure a domain name for DHCP clients	Configure the current interface	**interface** *interface-type interface-number*	Required By default, no domain name is configured for DHCP clients.
		dhcp server domain-name *domain-name*	
		quit	
	Configure multiple interfaces in system view	**dhcp server domain-name** *domain-name* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
Configure DNS server addresses for DHCP clients	Configure the current interface	**interface** *interface-type interface-number*	Required By default, no DNS server address is configured.
		dhcp server dns-list *ip-address*&<1-8>	
		quit	
	Configure multiple interfaces in system view	**dhcp server dns-list** *ip-address*&<1-8> { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

2.3.6 Configuring DHCP Servers to Assign WINS Server Addresses

For Microsoft Windows-based DHCP clients that communicate through NetBIOS protocol, the host name-to-IP address translation is carried out by WINS servers. So you need to perform WINS-related configuration for most Windows-based hosts. Currently, you can configure up to eight WINS addresses for a DHCP address pool.

Host name-to-IP address mappings are needed for DHCP clients communicating through the NetBIOS protocol. According to the way to establish the mapping, NetBIOS nodes fall into the following four categories:

- B-node. Nodes of this type establish their mappings through broadcasting (The character b stands for the word broadcast). The source node obtains the IP address of the destination node by sending the broadcast packet containing the

host name of the destination node. After receiving the broadcast packet, the destination node returns its IP address to the source node.

- P-node. Nodes of this type establish their mappings by communicating with WINS servers (The character p stands for peer-to-peer). The source node sends the unicast packet to the WINS server. After receiving the unicast packet, the WINS server returns the IP address corresponding to the destination node name to the source node.
- M-node. Nodes of this type are p-nodes mixed with broadcasting features (The character m stands for the word mixed), that is to say, this type of nodes obtain mappings by sending broadcast packets first. If they fail to obtain mappings, they send unicast packets to the WINS server to obtain mappings.
- H-node. Nodes of this type are b-nodes mixed with peer-to-peer features (The character h stands for the word hybrid), that is to say, this type of nodes obtain mappings by sending unicast packets to WINS servers first. If they fail to obtain mappings, they send broadcast packets to obtain mappings.

Table 2-17 Configure DHCP servers to assign WINS server addresses

Operation		Command	Description
Enter system view		**system-view**	—
Configure WINS server addresses for DHCP clients	Configure the current interface	**interface** *interface-type interface-number*	Required By default, no WINS server address is configured
		dhcp server nbns-list *ip-address*&<1-8>	
		quit	
	Configure multiple interfaces in system view	**dhcp server nbns-list** *ip-address*&<1-8> { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
Configure NetBIOS node types for DHCP clients	Configure the current interface	**interface** *interface-type interface-number*	Required By default, no NetBIOS node type is specified and a DHCP client uses an h-node.
		dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }	
		quit	
	Configure multiple interfaces in system view	**dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

2.3.7 Customizing DHCP Service

With the evolution of DHCP, new options are constantly coming into being. You can add the new options as the properties of DHCP servers by performing the following configuration.

Table 2-18 Customize DHCP service

Operation		Command	Description
Enter system view		**system-view**	—
Configure customized options	Configure the current interface	**interface** *interface-type interface-number*	Required By default, no customized option is configured.
		dhcp server option *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> }	
		quit	
	Configure multiple interfaces in system view	**dhcp server option** *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

2.3.8 Configuring Connection Between the DHCP Interface Address Pool and the BIMS Server

After configuring the connection between the DHCP interface address pool and the BIMS server, you can enable the BIMS server to manage the devices that have obtained IP addresses from the interface address pool.

Table 2-19 Configure connection between the DHCP interface address pool and the BIMS server

Operation	Command	Description
Enter system view	**system-view**	—
Configure connection between the DHCP interface address pool and the BIMS server	**dhcp server bims-server ip** *ip-address* [**port** *port-number*] **sharekey** *key* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	Required By default, no connection between the DHCP interface address pool and the BIMS server is configured.

2.4 DHCP Security Configuration

DHCP security configuration is needed to ensure the security of DHCP service.

2.4.1 Prerequisites

Before configuring DHCP security, you should first complete the DHCP server configuration (either global address pool-based or interface address pool-based DHCP server configuration).

2.4.2 Configuring Private DHCP Server Detecting

A private DHCP server on a network also answers IP address request packets and assigns IP addresses to DHCP clients. However, the IP addresses they assigned may conflict with those of other hosts. As a result, users cannot normally access networks. This kind of DHCP servers are known as private DHCP servers.

With the private DHCP server detecting function enabled, when a DHCP client sends the DHCP-REQUEST packet, the DHCP server tracks the information (such as the IP address and interface) of the DHCP server which assigns the IP address to the client to enable the administrator to detect private DHCP servers in time and take proper measures.

Table 2-20 Enable detection of a private DHCP server

Operation	Command	Description
Enter system view	**system-view**	—
Enable the private DHCP server detecting function	**dhcp server detect**	Required By default, the private DHCP server detecting function is disabled.

2.4.3 Configuring IP Address Detecting

To avoid IP address conflicts caused by assigning the same IP address to multiple DHCP clients simultaneously, you can configure a DHCP server to detect an IP address before it assigns the address to a DHCP client.

IP address detecting is achieved by performing ping operations. To detect whether an IP address is currently in use, the DHCP server sends an ICMP packet with the IP address to be assigned as the destination and waits for a ping response. If the DHCP server receives no response within a specified time, it resends an ICMP packet. This procedure repeats until the DHCP server receives a response or the number of the ping operations reaches the specified maximum number. The DHCP server assigns the IP

address to the DHCP client only when no response is received during the whole course, thus ensuring that an IP address is assigned to one DHCP client exclusively.

Table 2-21 Configure IP address detecting

Operation	Command	Description
Enter system view	**system-view**	—
Set the maximum number of ping operations performed by a DHCP server	**dhcp server ping packets** *number*	Optional By default, a DHCP server performs the ping operation twice to test an IP address.
Set the response timeout time of each ping operation	**dhcp server ping timeout** *milliseconds*	Optional The default timeout time is 500 milliseconds.

2.5 Option 82 Supporting Configuration

2.5.1 Introduction to DHCP-Server Option 82

If a DHCP server supports option 82, after the DHCP server receives packets containing option 82 forwarded by the DHCP relay, the DHCP server processes the packets normally and assigns IP addresses for the clients.

If a DHCP server does not support option 82, after the DHCP server receives packets containing option 82 forwarded by the DHCP relay, the DHCP server does not process the packets.

For details of option 82, see section 3.1.3 "Option 82 Supporting".

2.5.2 Configuration Prerequisites

Before enabling option 82 for the DHCP server, you need to configure the DHCP server based on global address pools or interface address pools.

2.5.3 Configuring the Option 82 Supporting Function

Table 2-22 Enable the DHCP server to support option 82

Operation	Command	Description
Enter system view	**system-view**	—
Enable the DHCP server to support option 82	**dhcp server relay information enable**	Required By default, the DHCP server supports option 82

Note:

To enable option 82 normally, you need to perform corresponding configuration on both the DHCP server and the DHCP relay. For the configuration of the DHCP relay, see section 3.1.3 "Option 82 Supporting".

2.6 Option 184 Supporting Configuration

2.6.1 Introduction to Option 184

Option 184 is an RFC reserved option, and the information it carries can be customized. H3C defines four proprietary sub-options for this option, enabling the DHCP server to put the information required by a DHCP client in the response packet to the client.

I. Basic concept

The four sub-options of option 184 mainly carry information about voice. The following lists the sub-options and the carried information:

- option: An option in a DHCP message. This option may be a field in variable length. Option contains some lease information and message types. The option field contains at least one and up to 255 options.
- Sub-option 1: IP address of the network call processor (NCP-IP).
- Sub-option 2: IP address of the alternate server (AS-IP).
- Sub-option 3: Voice VLAN configuration.
- Sub-option 4: Fail-over call routing.

II. Meanings of the sub-options for option 184

Table 2-23 Meanings of the sub-options for option 184

Sub-option	Feature	Function	Note
NCP-IP (sub-option 1)	The NCP-IP sub-option carries the IP address of the network call processor (NCP).	The IP address of the NCP server carried by sub-option 1 of option 184 is intended for identifying the server serving as the network call controller and the server used for application downloading.	When used in option 184, this sub-option must be the first sub-option, that is, sub-option 1

Sub-option	Feature	Function	Note
AS-IP (sub-option 2)	The AS-IP sub-option carries the IP address of the alternate server (AS).	The alternate NCP server identified by sub-option 2 of option 184 acts as the backup of the NCP server. The NCP server specified by this option is used only when the IP address carried by the NCP-IP sub-option is unreachable or invalid.	The AS-IP sub-option takes effect only when sub-option 1 (that is, the NCP-IP sub-option) is defined
Voice VLAN Configuration (sub-option 3)	The voice VLAN configuration sub-option carries the ID of the voice VLAN and the flag indicating whether the voice VLAN identification function is enabled.	The sub-option 3 of option 184 comprises two parts: • One part carries the flag indicating whether the voice VLAN identification function is enabled. • The other part carries the ID of the voice VLAN.	• A flag value of 0 indicates that the voice VLAN identification function is not enabled, in which case the information carried by the VLAN ID part will be neglected. • A flag value of 1 indicates that the voice VLAN identification function is enabled.
Fail-Over Call Routing (sub-option 4)	The fail-over call routing sub-option carries the IP address for fail-over call routing and the associated dial number. The IP address for fail-over call routing and the dial number in sub-option 4 of option 184 refer to the IP address and dial number of the session initiation protocol (SIP) peer.	When the NCP server is unreachable, a SIP user can use the configured IP address and dial number of the peer to establish a connection and communicate with the peer SIP user.	—

Note:

For the configurations specifying to add sub-option 2, sub-option 3, and sub-option 4 in the response packets to take effect, you must configure the DHCP server to add sub-option 1.

III. Mechanism of using option 184 on DHCP server

The DHCP server encapsulates the information for option 184 to carry in the response packets sent to the DHCP clients. Supposing that the DHCP clients are on the same segment as the DHCP server, the mechanism of option 184 supporting on DHCP server is as follows:

1) A DHCP client sends to the DHCP server a request packet carrying option 55, which indicates the client requests the configuration parameters of option 184.
2) The DHCP server checks the request list in option 55 carried by the request packet, and then adds the sub-options of option 184 in the Options field of the response packet to be sent to the DHCP client.

Note:

Only when the DHCP client specifies in option 55 of the request packet that it requires option 184, does the DHCP server add option 184 in the response packet sent to the client.

2.6.2 Prerequisites

The following are required before you configure the option 184 supporting function.

- The network parameters, address pools, and lease time are configured.
- The DHCP server and the DHCP clients can communicate properly with each other.
- Before configuring option 184, you must configure an IP address for the interface on which option 184 is to be enabled.

2.6.3 Configuring the Option 184 Supporting Function

You can configure the sub-options of option 184 in system view, interface view, and DHCP global address pool view. Note that an interface-based address pool is needed for the first two methods.

I. Configuring the option 184 supporting function in system view

Table 2-24 Configure the option 184 supporting function in system view

Operation	Command	Description
Enter system view	**system-view**	—
Configure the interface to operate in DHCP server mode and assign the IP addresses of a specified interface-based address pool to DHCP clients	**dhcp select interface** { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Required
Configure the NCP-IP sub-option	**dhcp server voice-config ncp-ip** *ip-address* { **all | interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Required
Configure the AS-IP sub-option	**dhcp server voice-config as-ip** *ip-address* { **all | interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Optional
Configure the voice VLAN configuration sub-option	**dhcp server voice-config voice-vlan** *vlan-id* { **enable | disable** } { **all | interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	
Configure the Fail-over call routing sub-option	**dhcp server voice-config fail-over** *ip-address dialer-string* { **all | interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	

Note:

- Perform the operations listed in Table 2-24 in system view if you specify to assign IP addresses of an interface-based address pool to DHCP clients.
- This method allows you to configure the option 184 supporting function for multiple interfaces.

II. Configuring the option 184 supporting function in interface view

Table 2-25 Configure the option 184 supporting function in interface view

Operation	Command	Description
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Configure an IP address for the interface	**ip address** *ip-address net-mask*	—
Configure the interface to operate in DHCP server mode and assign the IP addresses of an interface-based address pool to DHCP clients	**dhcp select interface**	Required
Configure the NCP-IP sub-option	**dhcp server voice-config ncp-ip** *ip-address*	Required
Configure the AS-IP sub-option	**dhcp server voice-config as-ip** *ip-address*	Optional
Configure the voice VLAN configuration sub-option	**dhcp server voice-config voice-vlan** *vlan-id* { **enable | disable** }	Optional
Configure the Fail-over call routing sub-option	**dhcp server voice-config fail-over** *ip-address dialer-string*	Optional

Note:

- Perform the operations listed in Table 2-25 in interface view if you specify to assign IP addresses of an interface-based address pool to DHCP clients.
- This method allows you to configure the option 184 supporting function for a specific interface.

III. Configuring the option 184 supporting function in global DHCP address pool view

Table 2-26 Configure the option 184 supporting function in global DHCP address pool view

Operation	Command	Description
Enter system view	**system-view**	—
Configure the interface to operate in DHCP server mode and assign the IP addresses of a global address pool to DHCP clients	**dhcp select global** { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Required
Enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	—
Configure an IP address range IP addresses in which are dynamically assigned	**network** *ip-address* [**mask** *netmask*]	—
Configure the NCP-IP sub-option	**voice-config ncp-ip** *ip-address*	Required
Configure the AS-IP sub-option	**voice-config as-ip** *ip-address*	Optional
Configure the voice VLAN configuration sub-option	**voice-config voice-vlan** *vlan-id* { **enable** | **disable** }	Optional
Configure the Fail-over call routing sub-option	**voice-config fail-over** *ip-address dialer-string*	Optional

Note:

Perform the operations listed in Table 2-26 in global address pool view if you specify to assign IP addresses of a global DHCP address pool to DHCP clients.

2.6.4 Configuration Example

I. Network requirements

A 3COM VCX device operating as a DHCP client requests the DHCP server for all sub-options of option 184. A H3C series switch operates as the DHCP server. The option 184 supporting function is configured for a global DHCP address pool. The sub-options of option 184 are as follows:

- NCP-IP: 3.3.3.3

- AS-IP: 2.2.2.2
- Voice VLAN configuration: voice VLAN: enabled; voice VLAN ID: 3
- Fail-over routing: IP address: 1.1.1.1; dialer string: 99*

II. Network diagram

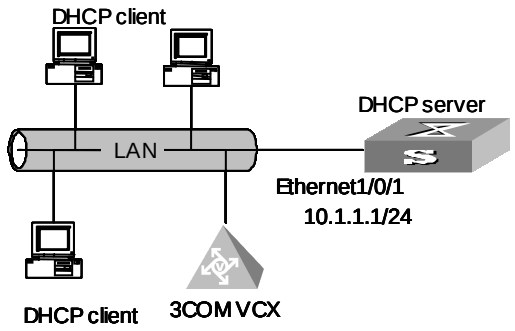


Figure 2-1 Network diagram for option 184 supporting configuration

III. Configuration procedure

1) Configure the DHCP client.

Configure the 3COM VCX device to operate as a DHCP client and to request for all sub-options of option 184. (Configuration process omitted)

2) Configure the DHCP server.

Enter system view.

```
<H3C> system-view
[H3C]
```

Add Ethernet1/0/1 to VLAN 2 and configure the IP address of VLAN 2 interface to be 10.1.1.1/24.

```
[H3C] vlan 2
[H3C-vlan2] port Ethernet 1/0/1
[H3C-vlan2] quit
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
[H3C-Vlan-interface2] quit
```

Configure VLAN 2 interface to operate in the DHCP server mode.

```
[H3C] dhcp select global interface Vlan-interface 2
```

Enter DHCP address pool view.

```
[H3C] dhcp server ip-pool 123
```

Configure sub-options of option 184 in global DHCP address pool view.

```
[H3C-dhcp-pool-123] network 10.1.1.1 mask 255.255.255.0
[H3C-dhcp-pool-123] voice-config ncp-ip 3.3.3.3
```

```
[H3C-dhcp-pool-123] voice-config as-ip 2.2.2.2
[H3C-dhcp-pool-123] voice-config voice-vlan 3 enable
[H3C-dhcp-pool-123] voice-config fail-over 1.1.1.1 99*
```

2.7 Displaying and Debugging a DHCP Server

You can verify your DHCP-related configuration by executing the **display** command in any view.

To clear the information about DHCP servers, execute the **reset** command in user view.

Table 2-27 Display and debug a DHCP server

Operation	Command	Description
Display the statistics on IP address conflicts	**display dhcp server conflict** { **all** | **ip** *ip-address* }	The **display** command can be executed in any view
Display lease expiration information	**display dhcp server expired** { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }	
Display the free IP addresses	**display dhcp server free-ip**	
Display information about address binding	**display dhcp server ip-in-use** { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }	
Display the statistics on a DHCP server	**display dhcp server statistics**	
Display information about DHCP address pool tree	**display dhcp server tree** { **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }	
Clear IP address conflict statistics	**reset dhcp server conflict** { **all** | **ip** *ip-address* }	The **reset** command can be executed in user view
Clear dynamic address binding information	**reset dhcp server ip-in-use** { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }	
Clear the statistics on a DHCP server	**reset dhcp server statistics**	

Note:

Executing the **save** command will not save the lease information on a DHCP server to the flash memory. Therefore, the configuration file contains no lease information after the DHCP server restarts or you clear the lease information by executing the **reset dhcp server ip-in-use** command. In this case, any lease-update requests will be denied, and the clients must apply for IP addresses again.

2.8 DHCP Server Configuration Example

Currently, DHCP networking can be implemented in two ways. One is to deploy the DHCP server and DHCP clients in the same network segment. This enables the clients to communicate with the server directly. The other is to deploy the DHCP server and DHCP clients in different network segments. In this case, IP address assigning is carried out through DHCP relay. Note that DHCP server configuration is the same in both scenarios.

I. Network requirements

The DHCP server assigns IP addresses dynamically to the DHCP clients on the same network segment. The network segment 10.1.1.0/24, to which the IP addresses of the address pool belong, is divided into two sub-network segment: 10.1.1.0/25 and 10.1.1.128/25. The switch operating as the DHCP server holds two VLANs, whose interface IP addresses are 10.1.1.1/25 and 10.1.1.129/25 respectively.

The DHCP settings of the 10.1.1.0/25 network segment are as follows:

- Lease time: 10 days plus 12 hours
- Domain name: aabbcc.com
- DNS server: 10.1.1.2
- WINS server: none
- Gateway: 10.1.1.126

The DHCP settings of the 10.1.1.128/25 network segment are as follows:

- Lease time: 5 days
- Domain name: aabbcc.com
- DNS server: 10.1.1.2
- WINS server: 10.1.1.4
- Gateway: 10.1.1.254

Note:

If you use the inheriting relation of parent and child address pools, make sure that the number of the assigned IP addresses does not exceed the number of the IP addresses in the child address pool; otherwise extra IP addresses will be obtained from the parent address pool, and the attributes (for example, gateway) also are based on the configuration of the parent address pool.

For example, in the network to which VLAN-interface1 is connected, if multiple clients apply for IP addresses, the child address pool 10.1.1.0/25 assigns IP addresses first. When the IP addresses in the child address pool have been assigned, if other clients need IP addresses, the IP addresses will be assigned from the parent address pool 10.1.1.0/24 and the attributes will be based on the configuration of the parent address pool.

For this example, the number of clients applying for IP addresses from VLAN-interface1 is recommended to be less than or equal to 122 and the number of clients applying for IP addresses from VLAN-interface2 is recommended to be less than or equal to 124.

II. Network diagram

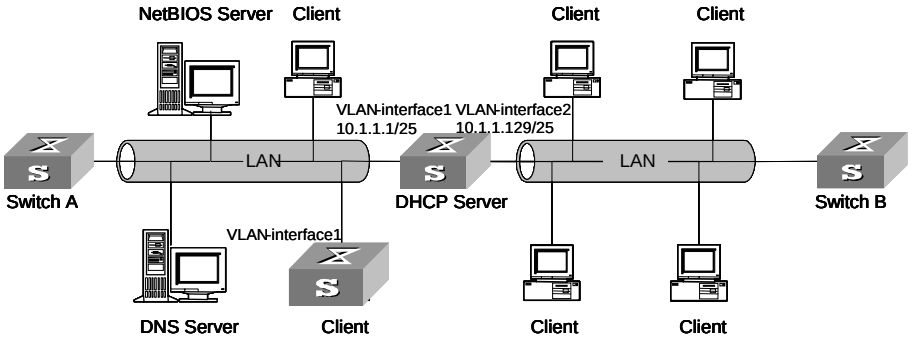


Figure 2-2 Network diagram for DHCP configuration

III. Configuration procedure

1) Configure a VLAN and add a port in this VLAN, and then configure the IP address of the VLAN interface (omitted).
2) Configure DHCP service.

Enable DHCP.

```
<H3C> system-view
[H3C] dhcp enable
```

Configure the IP addresses that are not dynamically assigned. (That is, the IP addresses of the DNS server, WINS server, and gateways.)

```
[H3C] dhcp server forbidden-ip 10.1.1.2
[H3C] dhcp server forbidden-ip 10.1.1.4
[H3C] dhcp server forbidden-ip 10.1.1.126
[H3C] dhcp server forbidden-ip 10.1.1.254
```

Configure DHCP address pool 0, including address range and DNS server address.

```
[H3C] dhcp server ip-pool 0
[H3C-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[H3C-dhcp-pool-0] domain-name aabbcc.com
[H3C-dhcp-pool-0] dns-list 10.1.1.2
[H3C-dhcp-pool-0] quit
```

Configure DHCP address pool 1, including address range, gateway, and lease time.

```
[H3C] dhcp server ip-pool 1
[H3C-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
[H3C-dhcp-pool-1] gateway-list 10.1.1.126
[H3C-dhcp-pool-1] expired day 10 hour 12
[H3C-dhcp-pool-1] quit
```

Configure DHCP address pool 2, including address range, gateway, WINS server address, and lease time.

```
[H3C] dhcp server ip-pool 2
[H3C-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
[H3C-dhcp-pool-2] expired day 5
[H3C-dhcp-pool-2] nbns-list 10.1.1.4
[H3C-dhcp-pool-2] gateway-list 10.1.1.254
```

2.9 Troubleshooting a DHCP Server

I. Symptom

The IP address dynamically assigned by a DHCP server to a client conflicts with the IP address of another host.

II. Analysis

With DHCP enabled, IP address conflicts are usually caused by IP addresses that are manually configured on hosts.

III. Solution

- Disconnect the DHCP client from the network and then check whether there is a host using the conflicting IP address by performing ping operation on another host

on the network, with the conflicting IP address as the destination and an enough timeout time.

- The IP address is manually configured on a host if you receive a response packet of the ping operation. You can then disable the IP address from being dynamically assigned by using the **dhcp server forbidden-ip** command on the DHCP server.
- Attach the DHCP client to the network, release the dynamically assigned IP address and obtain an IP address again. For example, enter DOS by executing the **cmd** command in Windows XP, and then release the IP address by executing the **ipconfig/release** command. Then obtain an IP address again by executing the **ipconfig/renew** command.

Chapter 3 DHCP Relay Configuration

3.1 Introduction to DHCP Relay

3.1.1 Usage of DHCP Relay

Since the packets are broadcasted in the process of obtaining IP addresses, DHCP is only applicable to the situation that DHCP clients and DHCP servers are in the same network segment, that is, you need to deploy at least one DHCP server for each network segment, which is far from economical.

DHCP Relay is designed to address this problem. It enables DHCP clients in a subnet to communicate with the DHCP server in another subnet so that the DHCP clients can obtain IP addresses. In this case, the DHCP clients in multiple networks can use the same DHCP server, which can decrease your cost and provide a centralized administration.

3.1.2 DHCP Relay Fundamentals

Figure 3-1 illustrates a typical DHCP relay application.

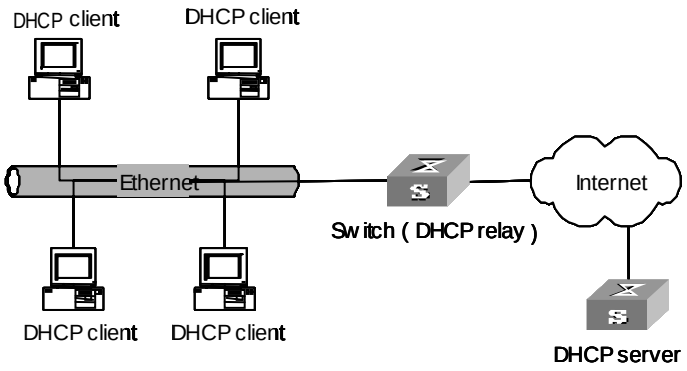


Figure 3-1 Typical DHCP relay application

DHCP relays can transparently transmit broadcast packets of DHCP clients or servers to the DHCP servers or clients in other network segments.

In the process of dynamic IP address assignment through the DHCP relay, the DHCP client and DHCP server interoperate with each other in a similar way as they do without the DHCP relay. The following sections only describe the forwarding process of the DHCP relay. For the interaction process of the packets, see section 1.2.2 “Obtaining IP Addresses Dynamically”.

1) The DHCP client broadcasts the DHCP-DISCOVER packet.

2) After receiving the packet, the network device providing the DHCP relay function unicasts the packet to the designated DHCP server based on the configuration.
3) The DHCP server assigns IP addresses and sends the configuration information to the clients through the DHCP relay so that the clients can be configured dynamically (the sending mode is decided by the flag filed in the DHCP-DISCOVER packet, refer to section 1.3 "DHCP Packet Format" for detail).

3.1.3 Option 82 Supporting

I. Introduction to option 82 supporting

Option 82 is a relay agent information option in DHCP packets. When a request packet from a DHCP client travels through a DHCP relay on its way to the DHCP server, the DHCP relay adds option 82 into the request packet. Option 82 includes many sub-options, but the DHCP server supports only sub-option 1 and sub-option 2 at present. Sub-option 1 defines agent circuit ID (that is, Circuit ID) and sub-option 2 defines remote agent ID (that is, Remote ID).

Option 82 enables a DHCP server to track the address information of DHCP clients and DHCP relays, through which and other proper software, you can achieve the DHCP assignment limitation and accounting functions.

II. Primary terminologies

- Option: A length-variable field in DHCP packets, carrying information such as part of the lease information and packet type. It includes at least one option and at most 255 options.
- Option 82: Also known as relay agent information option. This option is a part of the Option field in DHCP packet. According to RFC3046, option 82 lies before option 255 and after the other options. Option 82 includes at least one sub-option and at most 255 sub-options. Currently, the commonly used sub-options in option 82 are sub-option 1, sub-option 2, and sub-option 5.
- Sub-option 1: A sub-option of option 82. Sub-option 1 represents the agent circuit ID, namely Circuit ID. It holds the port number and VLAN-ID of the switch port connected to the DHCP client, and is usually configured on the DHCP relay. Generally, sub-option 1 and sub-option 2 must be used together to identify information about a DHCP source.
- Sub-option 2: A sub-option of option 82. Sub-option 2 represents the remote agent ID, namely Remote ID. This option is usually configured on the DHCP relay, and defines to carry the MAC address of the DHCP relay in the packet to be sent. Generally, sub-option 1 and sub-option 2 must be used together to identify information about a DHCP source.

III. Related specification

The specifications concerning option 82 supporting are as follows:

RFC2131 Dynamic Host Configuration Protocol

RFC3046 DHCP Relay Agent Information Option

IV. Mechanism of option 82 supporting on DHCP relay

The procedure for a DHCP client to obtain an IP address from a DHCP server through a DHCP relay is similar to that for the client to obtain an IP address from a DHCP server directly. The following are the mechanism of option 82 supporting on DHCP relay.

1) A DHCP client broadcasts a request packet when it initiates.
2) If a DHCP server exists in the local network, it assigns an IP address to the DHCP client directly; otherwise the DHCP relay on the local network receives and processes the request packet. The DHCP relay checks whether the packet contains option 82 and processes the packet accordingly.
3) If the packet contains option 82, the DHCP relay processes the packet depending on the configured strategy (that is, discards the packet, replaces the original option 82 in the packet with its own, or leaves the original option 82 unchanged in the packet), and forwards the packet (if not discarded) to the DHCP server.
4) If the packet does not contain option 82, the DHCP relay adds option 82 to the packet and forwards the packet to the DHCP server. The forwarded packet contains the port number of the switch to which the DHCP client is connected, the VLAN to which the port belongs, and the MAC address of the DHCP relay.
5) Upon receiving the DHCP request packet forwarded by the DHCP relay, the DHCP server stores the information contained in the option field and sends a packet that contains DHCP configuration information and option 82 to the DHCP relay.
6) Upon receiving the packet returned from the DHCP server, the DHCP relay strips option 82 from the packet and forwards the packet with the DHCP configuration information to the DHCP client.

Note:

Request packets sent by a DHCP client fall into two categories: DHCP-DISCOVER packets and DHCP-REQUEST packets. As DHCP servers coming from different manufacturers process DHCP request packets in different ways (that is, some DHCP servers process option 82 in DHCP-DISCOVER packets, whereas the rest process option 82 in DHCP-REQUEST packets), a DHCP relay adds option 82 to both types of packets to accommodate to DHCP servers of different manufacturers.

3.2 DHCP Relay Configuration

Note:

If a switch belongs to a fabric, you need to enable the UDP-helper function on it before configure it to be a DHCP relay.

3.2.1 DHCP Relay Configuration Tasks

Table 3-1 DHCP relay configuration tasks

Configuration task	Remarks	Section
Enable DHCP	Required	3.2.2 “Enabling DHCP”
Configure an interface to operate in DHCP relay mode	Required	3.2.3 “Configuring an Interface to Operate in DHCP Relay Mode”
Configure DHCP relay security	Optional	3.2.4 “Configuring DHCP Relay Security”
Configure option 82 supporting	Optional	3.2.5 “Configuring Option 82 Supporting”

3.2.2 Enabling DHCP

Make sure to enable DHCP before you perform other DHCP relay-related configurations, since other DHCP-related configurations cannot take effect with DHCP disabled.

Table 3-2 Enable DHCP

Operation	Command	Description
Enter system view	**system-view**	—
Enable DHCP	**dhcp enable**	Required By default, DHCP is enabled

3.2.3 Configuring an Interface to Operate in DHCP Relay Mode

When an interface operates in the relay mode, the interface forwards the DHCP packets received from DHCP clients to an external DHCP server, which assigns IP addresses to the DHCP clients.

To enhance reliability, you can set multiple DHCP servers on the same network. These DHCP servers form a DHCP server group. When the interface establishes mapping relationship with the DHCP server group, the interface forwards the DHCP packets to all servers in the server group.

Table 3-3 Configure an interface to operate in DHCP relay mode

Operation	Command	Description
Enter system view	**system-view**	—
Configure the DHCP server IP address(es) in a specified DHCP server group	**dhcp-server** *groupNo* **ip** *ip-address*&<1-8>	Required By default, no DHCP server IP address is configured in a DHCP server group.
Map an interface to a DHCP server group	**interface** *interface-type interface-number*	Required By default, a VLAN interface is not mapped to any DHCP server group.
	dhcp-server *groupNo*	

Note:

To improve security and avoid malicious attack to the unused SOCKETs, S3600 Ethernet switches provide the following functions:

- UDP 67 and UDP 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP 67 and UDP 68 ports are disabled when DHCP is disabled.

The corresponding implementation is as follows:

- When a VLAN interface is mapped to a DHCP server group with the **dhcp-server** command, the DHCP relay agent is enabled. At the same time, UDP 67 and UDP 68 ports used by DHCP are enabled.
- When the mapping between a VLAN interface and a DHCP server group is removed with the **undo dhcp-server** command, DHCP services are disabled. At the same time, UDP 67 and UDP 68 ports are disabled.

🕮 **Note:**

- You can configure up to eight external DHCP server IP addresses in a DHCP server group.
- You can map multiple VLAN interfaces to one DHCP server group. But one VLAN interface can be mapped to only one DHCP server group.
- If you execute the **dhcp-server** *groupNo* command repeatedly, the new configuration overwrites the previous one.
- You need to configure the group number specified in the **dhcp-server** *groupNo* command in VLAN interface view by using the command **dhcp-server** *groupNo* **ip** *ip-address*&<1-8> in advance.

3.2.4 Configuring DHCP Relay Security

I. Configuring address checking

When a DHCP client obtain an IP address from a DHCP server with the help of a DHCP relay, the DHCP relay creates an entry (dynamic entry) in the user address table to track the IP-MAC address binding information about the DHCP client. You can also configure user address entries manually (static entries) to bind an IP address and a MAC address statically.

The purpose of the address checking function on DHCP relay is to prevent unauthorized users from statically configuring IP addresses to access external networks. With this function enabled, a DHCP relay inhibits a user from accessing external networks if the IP address configured on the user end and the MAC address of the user end do not match any entries (including the entries dynamically tracked by the DHCP relay and the manually configured static entries) in the user address table on the DHCP relay.

Table 3-4 Configure address checking

Operation	Command	Description
Enter system view	**system-view**	—
Create a DHCP user address entry manually	**dhcp-security static** *ip-address mac-address*	Optional By default, no DHCP user address entry is configured. (Only S3600-EI series switches among S3600 series switches support this configuration.)
Enter interface view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Enable the address checking function	**address-check enable**	Required By default, the address checking function is disabled. (Only S3600-EI series switches among S3600 series switches support this configuration.)

II. Configuring DHCP relay handshake

When the DHCP client obtains an IP address from the DHCP server through the DHCP relay, the DHCP relay records the binding relationship of the IP address and the MAC address. After the DHCP relay handshake function is enabled, the DHCP relay sends the handshake packet (the DHCP-REQUEST packet) which carries includes the IP address recorded in the binding and its own bridge MAC address to the DHCP server periodically.

- If the DHCP server returns the DHCP-ACK packet, it indicates that the IP address can be assigned. The DHCP relay ages the corresponding entry in the user address table.
- If the DHCP server returns the DHCP-NAK packet, it indicates that the lease of the IP address is not expired. The DHCP relay does not age the corresponding entry.

After the DHCP relay handshake function is disabled, the DHCP relay does not send the handshake packet (the DHCP-REQUEST packet) periodically to the DHCP server.

- When the DHCP client releases this IP address, the client unicasts the DHCP-RELEASE packet to the DHCP server.
- The DHCP relay does not process this packet, so the user address entries of the DHCP relay cannot be updated in real time.

Table 3-5 Enable/disable DHCP relay handshake

Operation	Command	Description
Enter system view	**system-view**	—
Enable DHCP relay handshake	**dhcp relay hand enable**	By default, the DHCP relay handshake function is enabled. (Only S3600-EI series switches among S3600 series switches support this configuration.)
Disable DHCP relay handshake	**dhcp relay hand disable**	

III. Configuring the dynamic user address entry updating function

When a DHCP client obtains an IP address from a DHCP server with the help of a DHCP relay, the DHCP relay creates an entry (dynamic entry) in the user address table to track the binding information about the IP address and MAC address of the DHCP client. But as a DHCP relay does not process DHCP-RELEASE packets, which are sent to DHCP servers by DHCP clients through unicast when the DHCP clients release IP addresses, the user address entries maintained by the DHCP cannot be updated in time. The dynamic user address entry updating function is developed to resolve this problem.

The dynamic user address entry updating function works as follows: at regular intervals, the DHCP relay sends a DHCP-REQUEST packet that carries the IP address assigned to a DHCP client and its own bridge MAC address to the corresponding DHCP server. If the DHCP server answers with a DHCP-ACK packet, the IP address is available (it can be assigned again) and the DHCP relay ages the corresponding entry in the user address table. If the DHCP server answers with a DHCP-NAK packet, the IP address is still in use (the lease is not expired) and the DHCP relay remains the corresponding user address entry unchanged.

Table 3-6 Configure the dynamic user address entry updating function

Operation	Command	Description
Enter system view	**system-view**	—
Enable DHCP relay handshake	**dhcp relay hand enable**	Required
Set the interval at which the DHCP relay dynamically updates the user address entries	**dhcp-security tracker** { *interval* | **auto** }	Optional Only S3600-EI series switches among S3600 series switches support this configuration.

IV. Configuring private DHCP server detection function

If there is an unauthorized DHCP server in the network, when a client applies for an IP address, the unauthorized DHCP server interconnects with the DHCP client. As a result, the DHCP client obtains an incorrect IP address. Such unauthorized DHCP server is called a private DHCP server.

After the private DHCP server detection function is enabled on a DHCP relay, when a DHCP client sends the DHCP-REQUEST packet, the DHCP relay can obtain from the packet the information (such as the IP address and interface receiving the packet) of the DHCP server that assigns an IP address to the client. As a result, the administrator can find and deal with the private DHCP server.

Table 3-7 Configure private DHCP server detection function

Operation	Command	Description
Enter system view	**system-view**	—
Enable private DHCP server detection function	**dhcp-server detect**	Required By default, the private DHCP server detection function is disabled

3.2.5 Configuring Option 82 Supporting

I. Prerequisites

Before configuring option 82 supporting on a DHCP relay, you need to:

- Configure network parameters and relay function of the DHCP relay device.
- Perform assignment strategy-related configurations, such as network parameters of the DHCP server, address pool, and lease time.
- The routes between the DHCP relay and the DHCP server are reachable.

II. Enabling option 82 supporting on a DHCP relay

The following operations need to be performed on a DHCP relay–enabled network device.

Table 3-8 Enable option 82 supporting on a DHCP relay

Operation	Command	Description
Enter system view	**system-view**	—
Enable option 82 supporting on the DHCP relay	**dhcp relay information enable**	Required By default, this function is disabled
Configure the strategy for the DHCP relay to process request packets containing option 82	**dhcp relay information strategy** { **drop** | **keep** | **replace** }	Optional By default, the **replace** strategy is adopted

Note:

- By default, with the option 82 supporting function enabled on the DHCP relay, the DHCP relay will adopt the **replace** strategy to process the request packets containing option 82. However, if other strategies are configured before, then enabling the 82 supporting on the DHCP relay will not change the configured strategies.
- To enable option 82, you need to perform the corresponding configuration on the DHCP server and the DHCP relay.

3.3 Displaying and Debugging DHCP Relay

After the preceding configurations, you can execute the **display** command in any view to verify the configurations. You can also execute the **reset** command to clear the statistics information about the specified DHCP server group.

Table 3-9 Display DHCP relay information

Operation	Command	Description
Display the information about a specified DHCP server group	**display dhcp-server** *groupNo*	The **display** command can be executed in any view
Display the information about the DHCP server group to which a specified VLAN interface is mapped	**display dhcp-server interface Vlan-interface** *vlan-id*	
Display the address information of all the users in the valid user address table of the DHCP server group	**display dhcp-security** [*ip-address* | **dynamic** | **static | tracker**]	
Clear the statistics information of the specified DHCP server group	**reset dhcp-server** *groupNo*	The **reset** command must be executed in user view

3.4 DHCP Relay Configuration Example

I. Network requirements

The DHCP clients on the network segment 10.110.0.0/16 are connected to a port of VLAN 2. The IP address of the DHCP server is 202.38.1.2. DHCP packets between the DHCP clients and the DHCP server are forwarded by the DHCP relay, through which

the DHCP clients can obtain IP addresses and related configuration information from the DHCP server.

II. Network diagram

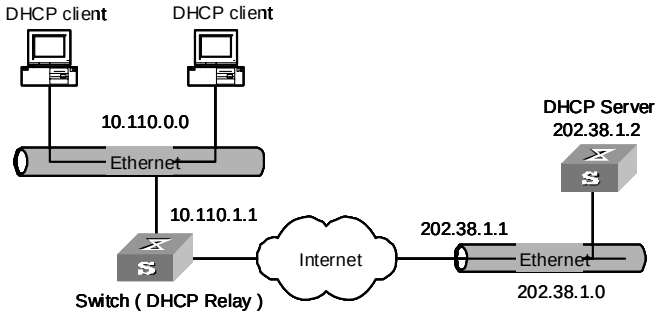


Figure 3-2 Network diagram for DHCP relay

III. Configuration procedure

Enter system view.

```
<H3C> system-view
```

Enable DHCP.

```
[H3C] dhcp enable
```

Create DHCP server group 1 and configure an IP address of 202.38.1.2 for it.

```
[H3C] dhcp-server 1 ip 202.38.1.2
```

Map VLAN-interface2 to DHCP server group 1.

```
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2] dhcp-server 1
```

Configure an IP address for VLAN-interface2. The IP address of the interface should be on the same network segment with the DHCP clients.

```
[H3C-Vlan-interface2] ip address 10.110.1.1 255.255.0.0
```

Note:

You need to perform corresponding configurations on the DHCP server to enable the DHCP clients to obtain IP addresses from the DHCP server. The DHCP server configurations vary with different DHCP server devices, so the configurations are omitted.

3.5 Troubleshooting DHCP Relay

I. Symptom

A client fails to obtain configuration information through a DHCP relay.

II. Analysis

This problem may be caused by improper DHCP relay configuration. When a DHCP relay operates improperly, you can locate the problem by enabling debugging and checking the information about debugging and interface state (You can display the information by executing the corresponding **display** command.)

III. Solution

- Check if DHCP is enabled on the DHCP server and the DHCP relay.
- Check if an address pool that is on the same network segment with the DHCP clients is configured on the DHCP server.
- Check if a reachable route is configured between the DHCP relay and the DHCP server.
- Check the DHCP relay-enabled network devices. Check if the correct DHCP server group is configured on the interface connecting the network segment where the DHCP client resides. Check if the IP address of the DHCP server group is correct.

Chapter 4 DHCP Snooping Configuration

Note:

After DHCP-Snooping is enabled on an S3600 Ethernet switch, clients connected with this switch cannot obtain IP addresses dynamically through BOOTP.

4.1 Introduction to DHCP Snooping

For the sake of security, the IP addresses used by online DHCP clients need to be tracked for the administrator to verify the corresponding relationship between the IP addresses the DHCP clients obtained from DHCP servers and the MAC addresses of the DHCP clients.

- Layer 3 switches can track DHCP client IP addresses through DHCP relay.
- Layer 2 switches can track DHCP client IP addresses through the DHCP snooping function, which listens DHCP broadcast packets.

When an unauthorized DHCP server exists in the network, a DHCP client may obtains an illegal IP address. To ensure that the DHCP clients obtain IP addresses from valid DHCP servers, you can specify a port to be a trusted port or an untrusted port by the DHCP snooping function.

- Trusted ports can be used to connect DHCP servers or ports of other switches. Untrusted ports can be used to connect DHCP clients or networks.
- Untrusted ports drop the DHCP-ACK and DHCP-OFFER packets received from DHCP servers. Trusted ports forward any received DHCP packets to ensure that DHCP clients can obtain IP addresses from valid DHCP servers.

Figure 4-1 illustrates a typical network diagram for DHCP snooping application, where Switch A is an S3600 series Ethernet switch.

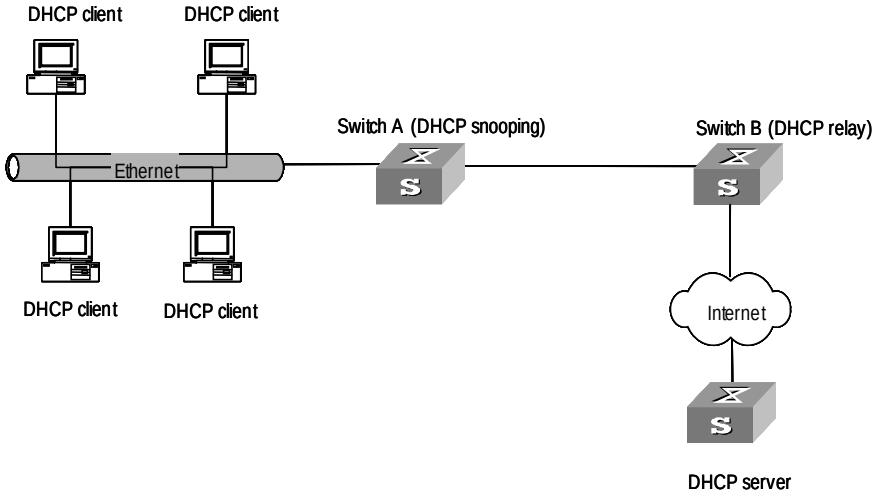


Figure 4-1 Typical network diagram for DHCP snooping application

Figure 4-2 illustrates the interaction between a DHCP client and a DHCP server.

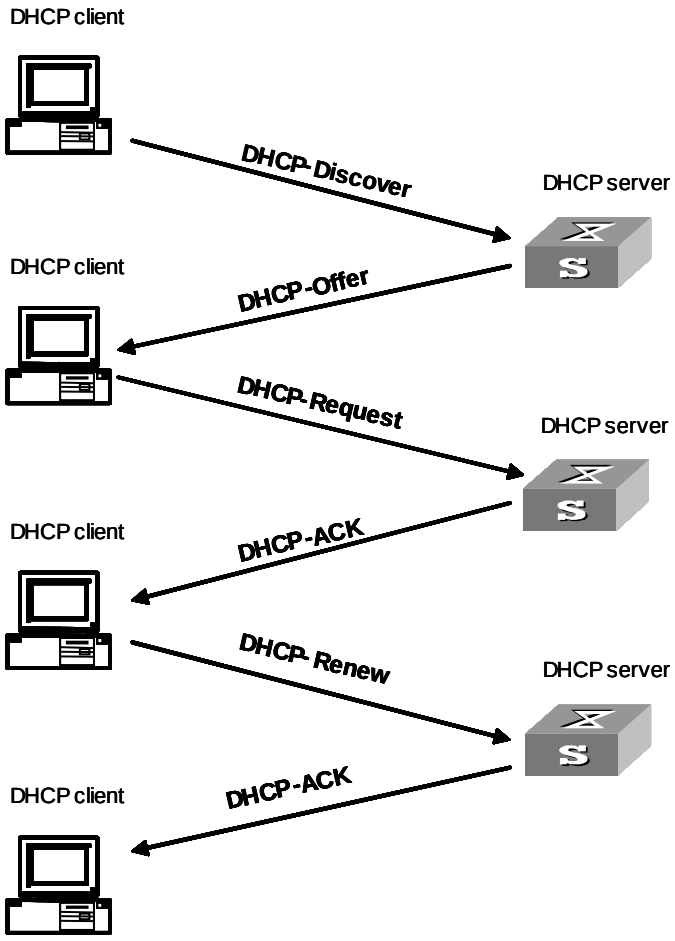


Figure 4-2 Interaction between a DHCP client and a DHCP server

DHCP snooping listens the following two types of packets to retrieve the IP addresses the DHCP clients obtain from DHCP servers and the MAC addresses of the DHCP clients:

- DHCP-ACK packet
- DHCP-REQUEST packet

4.2 DHCP Snooping Configuration

Table 4-1 Configure the DHCP snooping function

Operation	Command	Description
Enter system view	**system-view**	—
Enable the DHCP snooping function	**dhcp-snooping**	Required By default, the DHCP snooping function is disabled.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the port connected to a DHCP server to a trusted port	**dhcp-snooping trust**	Optional By default, all ports of a switch are untrusted ports.

Note:

When you need to enable DHCP snooping on the switches in a fabric state, configure the fabric ports on all devices to be trusted ports to ensure that the users connected to each device can obtain IP addresses.

4.3 Displaying DHCP Snooping

After the above configurations, you can verify the configurations by executing the **display** command in any view.

Table 4-2 Display DHCP snooping

Operation	Command	Description
Display the user IP-MAC address mapping entries recorded by the DHCP snooping function	**display dhcp-snooping** [**unit** *unit-id*]	You can execute the **display** command in any view
Display the (enabled/disabled) state of the DHCP snooping function and the trusted ports	**display dhcp-snooping trust**	

4.4 Configuration Example

I. Network requirements

As shown in Figure 4-1, the Ethernet1/0/1 port of Switch A (an S3600 series switch) is connected to Switch B (acting as a DHCP relay). A network segment containing some DHCP clients is connected to the Ethernet1/0/2 port of Switch A.

- Enable the DHCP snooping function on Switch A.
- Set the Ethernet1/0/1 port of Switch A to a trusted port.

II. Configuration procedure

Enter system view.

```
<H3C> system-view
```

Enable the DHCP snooping function.

```
[H3C] dhcp-snooping
```

Enter Ethernet1/0/1 port view.

```
[H3C] interface Ethernet1/0/1
```

Set the port to a trusted port.

```
[H3C-Ethernet1/0/1] dhcp-snooping trust
```

Chapter 5 DHCP Accounting Configuration

5.1 Introduction to DHCP Accounting

DHCP accounting allows a DHCP server to notify the RADIUS server of the start/end of accounting when it assigns/releases a lease. The cooperation of DHCP server and RADIUS server implements the network accounting function and ensures network security at the same time.

5.1.1 DHCP Accounting Fundamentals

After you complete AAA and RADIUS configuration on a switch with the DHCP server function enabled, the DHCP server acts as a RADIUS client. For the authentication process of the DHCP server acting as a RADIUS client, refer to the “Introduction to RADIUS” section of the "Security” part in this manual. The following describes only the accounting interaction between DHCP server and RADIUS server.

- After sending a DHCP-ACK packet with the IP configuration parameters to the DHCP client, the DHCP server sends an Accounting START packet to a specified RADIUS server. The RADIUS server processes the packet, makes a record, and sends a response to the DHCP server.
- Once releasing a lease for some reason, the DHCP server sends an Accounting STOP packet to the RADIUS server. The RADIUS server processes the packet, stops the recording for the DHCP client, and sends a response to the DHCP server. A lease can be released for the reasons such as lease expiration, a release request received from the DHCP client, a manual release operation, an address pool removal operation.
- If the RADIUS server of the specified domain is unreachable, the DHCP server sends up to three Accounting START packets (including the first sending attempt) at regular intervals. If the three packets bring no response from the RADIUS server, the DHCP server does not send Accounting START packets any more.

5.2 DHCP Accounting Configuration

5.2.1 Prerequisites

Before configuring DHCP accounting, make sure that:

- The DHCP server is configured and operates properly. Address pools and lease time are configured.
- DHCP clients are configured and DHCP service is enabled.
- The network operates properly.

5.2.2 Configuring DHCP Accounting

Table 5-1 Configure DHCP accounting

Operation	Command	Description
Enter system view	**system-view**	—
Enter address pool view	**dhcp server ip-pool** *pool-name*	Required
Enable DHCP accounting	**accounting domain** *domain-name*	Required The domain identified by the *domain-name* argument can be created by using the **domain** command.

5.2.3 DHCP Accounting Configuration Example

I. Network requirements

- The DHCP server connects to a DHCP client and a RADIUS server respectively through its Ethernet1/0/2 and Ethernet1/0/1 ports.
- Ethernet1/0/2 belongs to VLAN 2; Ethernet1/0/1 belongs to VLAN 3.
- The IP address of VLAN 2 interface is 10.1.1.1/24, and that of VLAN 3 interface is 10.1.2.1/24.
- The IP address of the RADIUS server is 10.1.2.2/24.
- DHCP accounting is enabled on the DHCP server.
- The IP addresses of the global DHCP address pool belongs to the network segment 10.1.1.0/24. The DHCP server operates as a RADIUS client and adopts AAA for authentication.

II. Network diagram

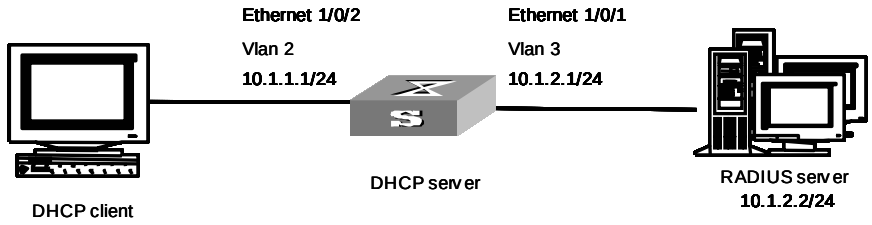


Figure 5-1 Network diagram for DHCP accounting configuration

III. Configuration procedure

Enter system view.

```
<H3C> system-view
```

Create VLAN 2.

```
[H3C] vlan 2
[H3C-vlan2] quit
```

Create VLAN 3.

```
[H3C] vlan 3
[H3C-vlan3] quit
```

Enter Ethernet1/0/2 port view and add the port to VLAN 2.

```
[H3C] interface Ethernet 1/0/2
[H3C-Ethernet1/0/2] port access vlan 2
[H3C-Ethernet1/0/2] quit
```

Enter Ethernet1/0/1 port view and add the port to VLAN 3.

```
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] port access vlan 3
[H3C-Ethernet1/0/1] quit
```

Enter VLAN 2 interface view and assign the IP address 10.1.1.1/24 to the VLAN interface.

```
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2] ip address 10.1.1.1 24
[H3C-Vlan-interface2] quit
```

Enter VLAN 3 interface view and assign the IP address 10.1.2.1/24 to the VLAN interface.

```
[H3C] interface Vlan-interface 3
[H3C-Vlan-interface3] ip address 10.1.2.1 24
[H3C-Vlan-interface3] quit
```

Create a domain and a RADIUS scheme. Associate the domain with the RADIUS scheme.

```
[H3C] radius scheme 123
[H3C-radius-123] primary authentication 10.1.2.2
[H3C-radius-123] primary accounting 10.1.2.2
[H3C] domain 123
[H3C-isp-123] scheme radius-scheme 123
[H3C-isp-123] quit
```

Create an address pool on the DHCP server.

```
[H3C] dhcp server ip-pool test
[H3C-dhcp-pool-test] network 10.1.1.0 mask 255.255.255.0
```

Enable DHCP accounting.

```
[H3C-dhcp-pool-test] accounting domain 123
```

Table of Contents

Chapter 1 ACL Configuration 1-1
1.1 ACL Overview 1-1
1.1.1 Ways to Apply ACL on a Switch 1-1
1.1.2 ACL Matching Order 1-2
1.1.3 Time Range-based ACL 1-3
1.1.4 Types of ACLs Supported by the Ethernet Switch 1-3
1.2 Time Range Configuration 1-3
1.2.1 Configuration Procedure 1-3
1.2.2 Configuration Example 1-4
1.3 Basic ACL Configuration 1-4
1.3.1 Configuration Preparation 1-5
1.3.2 Configuration Procedure 1-5
1.3.3 Configuration Example 1-6
1.4 Advanced ACL Configuration 1-6
1.4.1 Configuration Preparation 1-6
1.4.2 Configuration Procedure 1-6
1.4.3 Configuration Example 1-12
1.5 Layer 2 ACL Configuration 1-12
1.5.1 Configuration Preparation 1-13
1.5.2 Configuration Procedure 1-13
1.5.3 Configuration Example 1-15
1.6 User-Defined ACL Configuration 1-15
1.6.1 Configuration Preparation 1-16
1.6.2 Configuration Procedure 1-16
1.6.3 Configuration Example 1-17
1.7 Applying ACLs on Ports 1-17
1.7.1 Configuration Preparation 1-17
1.7.2 Configuration Procedure 1-17
1.7.3 Configuration Example 1-18
1.8 Displaying ACL Configuration 1-18
1.9 ACL Configuration Example 1-19
1.9.1 Basic ACL Configuration Example 1-19
1.9.2 Advanced ACL Configuration Example 1-20
1.9.3 Layer 2 ACL Configuration Example 1-21
1.9.4 User-Defined ACL Configuration Example 1-22

Chapter 1 ACL Configuration

1.1 ACL Overview

An access control list (ACL) is mainly used for traffic classification. To filter data packets, a network device needs to be configured with a series of ACLs to identify the packets to be filtered. A network device can permit/deny specific packets in a predefined way only after the traffic is classified.

ACLs classify packets using a series of conditions known as rules. The conditions can be based on source addresses, destination addresses and port numbers carried in the packets.

The rules of an ACL can be referenced by other functions that need traffic classification, such as QoS.

According to their application purposes, ACLs fall into the following four types.

- Basic ACL. Rules are created based on Layer 3 source IP addresses only.
- Advanced ACL. Rules are created based on the Layer 3 and Layer 4 information such as the source and destination IP addresses, the type of the protocols carried by IP, protocol-specific features, and so on.
- Layer 2 ACL. Rules are created based on the Layer 2 information such as source and destination MAC addresses, VLAN priorities, Layer 2 protocols, and so on.
- User-defined ACL. An ACL of this type matches packets by comparing specific strings retrieved from the packets with specified strings.

1.1.1 Ways to Apply ACL on a Switch

I. Applied to the hardware directly

In the switch, an ACL can be directly applied to the hardware for packet filtering and traffic classification. In this case, the rules in an ACL are matched in the order determined by the hardware instead of that defined in the ACL.

ACLs are directly applied to hardware when they are used for:

- Implementing QoS
- Filtering the packets to be forwarded

II. Referenced by upper-level modules

ACL can also be used to filter and classify the packets to be processed by software. In this case, the rules in an ACL can be matched in one of the following two ways:

- **config**, where rules in an ACL are matched in the order defined by the user.

- **auto**, where the rules in an ACL are matched in the order determined by the system, namely the “depth-first” order.

When applying ACLs in this way, you can specify the order in which the rules in the ACL are matched. The matching order cannot be modified once it is determined unless you delete all the rules in the ACL.

An ACL is referenced by an upper-layer module when it is

- Referenced by route policies
- Used to control login users

1.1.2 ACL Matching Order

An ACL can contain multiple rules, each of which matches specific type of packets. So the order in which the rules of an ACL are matched needs to be determined.

The order in which the rules of an ACL are matched can be:

- The order the rules are created.
- The order determined by the system. In this case, the rues are matched according to the “depth-first” rule.

With the depth-first rule adopted, the rules of an ACL are matched according to:

1) Protocol range. The range for IP is 1 to 255 and those of other protocols are their protocol numbers. The smaller the protocol range, the higher the priority.
2) Range of source IP address. The smaller the source IP address range (that is, the longer the mask), the higher the priority.
3) Range of destination IP address. The smaller the destination IP address range (that is, the longer the mask), the higher the priority.
4) Range of Layer 4 port number, that is, of TCP/UDP port number. The smaller the range, the higher the priority.

If rule A and rule B are the same in all the four ACEs (access control elements) above, and also in their numbers of other ACEs to be considered in deciding their priority order, the weighting principles will be used in deciding their priority order, as listed below.

- Each ACE is given a fixed weighting value. This weighting value and the value of the ACE itself will jointly decide the final matching order.
- The weighting values of ACEs rank in the following descending order: DSCP, ToS, ICMP, established, precedence, fragment.
- A fixed weighting value is deducted from the weighting value of each ACE of the rule. The smaller the weighting value left, the higher the priority.
- If the number and type of ACEs are the same for multiple rules, then the sum of ACE values of a rule determines its priority. The smaller the sum, the higher the priority.

1.1.3 Time Range-based ACL

A time range-based ACL takes effect only in specified time ranges.

You can specify a time range for each rule in an ACL. An ACL rule cannot take effect if you do not configure the time range for it. It takes effect only when the time range is configured and the system time is within the time range. If you remove the time range of an ACL rule, the ACL rule becomes invalid after the ACL rule timer refreshes.

1.1.4 Types of ACLs Supported by the Ethernet Switch

The following types of ACLs are supported by the Ethernet switch:

- Basic ACL
- Advanced ACL
- Layer 2 ACL
- User-defined ACL

1.2 Time Range Configuration

A time section can be periodic or absolute. A periodic time section is defined by specifying days of a week, while an absolute time section is defined by specifying the start time and the end time.

Note:

An absolute time range on an H3C S3600 switch can be within the range 1970/1/1 00:00 to 2100/12/31 24:00.

1.2.1 Configuration Procedure

Table 1-1 Configure a time range

Operation	Command	Description
Enter system view	**system-view**	—
Create a time range	**time-range** *time-name* { *start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] | **to** *end-time end-date* }	Required

Note that:

If only a periodic time section is defined in a time range, the time range is active only when the system time within the defined periodic time section. If multiple periodic time sections are defined in a time range, the time range is active only when the system time is within one of the periodic time sections.

If only an absolute time section is defined in a time range, the time range is active only when the system time within the defined absolute time section. If multiple absolute time sections are defined in a time range, the time range is active only when the system time is within one of the absolute time sections.

If both a periodic time section and an absolute time section are defined in a time range, the time range is active only when the periodic time range and the absolute time range are both matched. Assume that a time range contains an absolute time section ranging from 00:00 January 1, 2004 to 23:59 December 31, 2004, and a periodic time section ranging from 12:00 to 14:00 on every Wednesday. This time range is active only when the system time within the range from 12:00 to 14:00 on every Wednesday in 2004.

If the start time is not specified, the time section starts on the earliest date available in the system and ends on the specified end date. If the end date is not specified, the time section starts from the specified start date to 2100/12/31 23:59.

1.2.2 Configuration Example

Define a periodic time range that will be active from 8:00 to 18:00 on Monday through Friday.

```
<H3C> system-view
[H3C] time-range test 8:00 to 18:00 working-day
[H3C] display time-range test
Current time is 13:27:32 4/16/2005 Saturday

Time-range : test ( Inactive )
 08:00 to 18:00 working-day
```

Define an absolute time range from 15:00 1/28/2000 to 15:00 1/28/2004.

```
<H3C> system-view
[H3C] time-range test from 15:00 1/28/2000 to 15:00 1/28/2004
[H3C] display time-range test
Current time is 13:30:32 4/16/2005 Saturday

Time-range : test ( Inactive )
 From 15:00 Jan/28/2000 to 15:00 Jan/28/2004
```

1.3 Basic ACL Configuration

A basic ACL filters packets based on their Layer 3 source IP addresses.

A basic ACL can be numbered from 2000 to 2999.

1.3.1 Configuration Preparation

To configure a time range-based basic ACL rule, you need to create the corresponding time range first. For information about time range configuration, refer to section 1.2 “Time Range Configuration”.

The source IP addresses based on which the ACL filters packets are determined.

1.3.2 Configuration Procedure

Table 1-2 Define a basic ACL rule

Operation	Command	Description
Enter system view	**system-view**	—
Create an ACL or enter basic ACL view	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	By the default, the matching order is **config**.
Define an ACL rule	**rule** [*rule-id*] { **permit** | **deny** } [**fragment** | **source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name*]*	Required
Assign a description string to the ACL	**description** *text*	Optional

When you define an ACL rule using the **rule** command with the *rule-id* argument provided,

- If the ACL is created with the **config** keyword specified and the rule identified by the *rule-id* argument exists, the settings specified in the **rule** command overwrite the counterparts of the existing rule (other settings of the rule remain unchanged). If the ACL is created with the **auto** keyword specified, the rules of the ACL cannot be edited. In this case, the system prompts errors when you execute the **rule** command.
- If the ACL rule identified by the *rule-id* argument does not exist, you will create a new rule.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.

If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically.

1.3.3 Configuration Example

Configure ACL 2000 to deny packets whose source IP addresses are 1.1.1.1.

```
<H3C> system-view
[H3C] acl number 2000
[H3C-acl-basic-2000] rule deny source 1.1.1.1 0
[H3C-acl-basic-2000] display acl 2000
Basic ACL  2000, 1 rule
Acl's step is 1
rule 0 deny source 1.1.1.1 0
```

1.4 Advanced ACL Configuration

An advanced ACL can filter packets by their source and destination IP addresses, the protocols carried by IP. The rules in an advanced ACL rule can based on protocol-specific features such as TCP/UDP source and destination ports, ICMP protocol type, code, and so on.

An advanced ACL can be numbered from 3000 to 3999. Note that ACL 3998 and ACL 3999 cannot be configured because they are reserved for the cluster management.

Advanced ACLs support analysis and processing of three packet priority levels: type of service (ToS) priority, IP priority and differentiated services codepoint priority (DSCP).

Using advanced ACLs, you can define classification rules that are more accurate, more abundant, and more flexible than those defined for basic ACLs.

1.4.1 Configuration Preparation

To configure an time range-based advanced ACL rule, you need to create the corresponding time ranges first. For information about of time range configuration, refer to section 1.2 “Time Range Configuration”.

The settings to be specified in the rule, such as source and destination IP addresses, the protocols carried by IP, and protocol-specific features, are determined.

1.4.2 Configuration Procedure

Table 1-3 Define an advanced ACL rule

Operation	Command	Description
Enter system view	**system-view**	—
Create an advanced VLAN or enter advanced ACL view	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	By the default, the match order is **config**.
Define an ACL rule	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	Required

Operation	Command	Description
Assign a description string to the ACL rule	**rule** *rule-id* **comment** *text*	Optional
Assign a description string to the ACL	**description** *text*	Optional

The *rule-string* argument of the **rule** command listed in Table 1-3 can be a combination of the argument/keywords described in Table 1-4. Note that the *rule-string* argument must begin with the *protocol* argument.

Table 1-4 Description on the argument/keywords used in the *rule-string* argument

Arguments/Keywords	Type	Function	Description
protocol	Protocol type	Type of the protocols carried by IP	When expressed in numerals, this argument ranges from 1 to 255. When expressed with a name, the value can be GRE, ICMP, IGMP, IP, IPinIP, OSPF, TCP, and UDP.
source { *sour-addr sour-wildcard* | **any** }	Source address	Specifies the source address information for the ACL rule	The *sour-addr sour-wildcard* arguments specify the source address of the packets, expressed in dotted decimal notation. You can specify the IP address of a host as the source address by providing 0 for the *sour-wildcard* argument. **any** represents any source address.
destination { *dest-addr dest-wildcard* | **any** }	Destination address	Specifies the destination address information for the ACL rule	The *dest-addr dest-wildcard* arguments specify the destination address of the packets, expressed in dotted decimal notation. You can specify the IP address of a host as the destination address by providing 0 for the *dest-wildcard* argument. **any** represents any destination address.

Arguments/Keywords	Type	Function	Description
precedence *precedence*	Packet priority	IP precedence	The *precedence* argument ranges from 0 to 7.
tos *tos*	Packet priority	ToS	The *tos* argument ranges from 0 to 15.
dscp *dscp*	Packet priority	DSCP	The *dscp* argument ranges from 0 to 63.
fragment	Fragment information	Specifies that the rule is effective for the packets that are not the first fragments.	—
time-range *time-name*	Time range information	Specifies the time range in which the rule is active.	—

If you specify the **dscp** keyword, you can directly input a value ranging from 0 to 63 or input one of the keywords listed in Table 1-5 as the DSCP.

Table 1-5 DSCP values and the corresponding keywords

Keyword	DSCP value in decimal	DSCP value in binary
ef	46	101110
af11	10	001010
af12	12	001100
af13	14	001110
af21	18	010010
af22	20	010100
af23	22	010110
af31	26	011010
af32	28	011100
af33	30	011110
af41	34	100010
af42	36	100100
af43	38	100110
cs1	8	001000
cs2	16	010000

Keyword	DSCP value in decimal	DSCP value in binary
cs3	24	011000
cs4	32	100000
cs5	40	101000
cs6	48	110000
Cs7	56	111000
be (default)	0	000000

If you specify the **precedence** keyword, you can directly input a value ranging from 0 to 7 or input one of the keywords listed in Table 1-6 as the IP precedence.

Table 1-6 IP precedence values and the corresponding keywords

Keyword	IP Precedence in decimal	IP Precedence in binary
routine	0	000
priority	1	001
immediate	2	010
flash	3	011
flash-override	4	100
critical	5	101
internet	6	110
network	7	111

If you specify the **tos** keyword, you can directly input a value ranging from 0 to 15 or input one of the keywords listed in Table 1-7 as the ToS value.

Table 1-7 ToS value and the corresponding keywords

Keyword	ToS in decimal	ToS in binary
normal	0	0000
min-monetary-cost	1	0001
max-reliability	2	0010
max-throughput	4	0100
min-delay	8	1000

If the protocol type is TCP or UDP, you can also define the information listed in Table 1-8.

Table 1-8 TCP/UDP-specific ACL rule information

Parameter	Type	Function	Description
source-port *operator port1* [*port2*]	Source port	Defines the source port information of UDP/TCP packets	The value of *operator* can be lt (less than), gt (greater than), eq (equal to), neq (not equal to) or range (within the range of). Only the "range" operator requires two port numbers as the operands. Other operators require only one port number as the operand. *port1* and *port2*: TCP/UDP port numbers, expressed as port names or port numbers. When expressed as numbers, the value range is 0 to 65535.
destination-port *operator port1* [*port2*]	Destination port	Defines the destination port information of UDP/TCP packets	
established	TCP connection flag	Specifies that the rule is applicable only to the first SYN segment for establishing a TCP connection	TCP-specific argument

When using port name to specify TCP/UDP ports, you can define the following information.

Table 1-9 TCP/UDP port values

Protocol type	Value
TCP	**CHARgen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), **www** (80)
UDP	**biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (139), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), **xdmcp** (177)

Note:

When advanced ACLs are applied to ports of the H3C S3600 series Ethernet switches, only the rules configured with the *operator* argument specified as eq are valid.

If the protocol type is ICMP, you can also define the information listed in Table 1-10.

Table 1-10 ICMP-specific ACL rule information

Parameter	Type	Function	Description
icmp-type *icmp-type* *icmp-code*	Type and message code information of ICMP packets	Specifies the type and message code information of ICMP packets in the rule	*icmp-type*: ICMP message type, ranging from 0 to 255 *icmp-code*: ICMP message code, ranging from 0 to 255

If the protocol type is ICMP, you can also just input the ICMP message name after the **icmp-type** keyword. Table 1-11 lists some common ICMP messages.

Table 1-11 ICMP messages

Name	ICMP type	ICMP code
echo	Type=8	Code=0
echo-reply	Type=0	Code=0
fragmentneed-DFset	Type=3	Code=4
host-redirect	Type=5	Code=1
host-tos-redirect	Type=5	Code=3
host-unreachable	Type=3	Code=1
information-reply	Type=16	Code=0
information-request	Type=15	Code=0
net-redirect	Type=5	Code=0
net-tos-redirect	Type=5	Code=2
net-unreachable	Type=3	Code=0
parameter-problem	Type=12	Code=0
port-unreachable	Type=3	Code=3
protocol-unreachable	Type=3	Code=2
reassembly-timeout	Type=11	Code=1
source-quench	Type=4	Code=0

Name	ICMP type	ICMP code
source-route-failed	Type=3	Code=5
timestamp-reply	Type=14	Code=0
timestamp-request	Type=13	Code=0
ttl-exceeded	Type=11	Code=0

When you define an ACL rule using the **rule** command with the *rule-id* argument provided,

- If the ACL is created with the **config** keyword specified and the rule identified by the *rule-id* argument exists, the settings specified in the **rule** command overwrite the counterparts of the existing rule (other settings of the rule remain unchanged). If the ACL is created the **auto** keyword specified, the rules of the ACL cannot be edited. In this case, the system will prompt errors when you execute the **rule** command.
- If the ACL rule identified by the *rule-id* argument does not exist, you will create a new rule.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.

If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically.

1.4.3 Configuration Example

Configure ACL 3000 to permit the TCP packets sourced from the network 129.9.0.0 and destined for the network 202.38.160.0 and with the destination port number being 80.

```
<H3C> system-view
[H3C] acl number 3000
[H3C-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination
202.38.160.0 0.0.0.255 destination-port eq 80
[H3C-acl-adv-3000] display acl 3000
Advanced ACL  3000, 1 rule
Acl's step is 1
 rule 0 permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0
0.0.0.255 destination-port eq www
```

1.5 Layer 2 ACL Configuration

Layer 2 ACLs filter packets according to their Layer 2 information, such as the source and destination MAC addresses, VLAN priority, and Layer 2 protocol types.

A Layer 2 ACL can be numbered from 4000 to 4999.

1.5.1 Configuration Preparation

To configure a time range-based Layer 2 ACL rule, you need to create the corresponding time ranges first. For information about time range configuration, refer to section 1.2 “Time Range Configuration”.

The settings to be specified in the rule, such as source and destination MAC addresses, VLAN priorities, and Layer 2 protocol types, are determined.

1.5.2 Configuration Procedure

Table 1-12 Define a Layer 2 ACL rule

Operation	Command	Description
Enter system view	**system-view**	—
Create a Layer 2 ACL or enter layer 2 ACL view	**acl number** *acl-number*	Required
Define an ACL rule	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	Required
Assign a description string to the ACL rule	**rule** *rule-id* **comment** *text*	Optional
Assign a description string to the ACL	**description** *text*	Optional

The *rule-string* argument of the **rule** command can be a combination of the arguments/keywords described in Table 1-13.

Table 1-13 Layer 2 ACL rule information

Parameter	Type	Function	Description
format-type	Link layer encapsulation type	Specifies the link layer encapsulation type for the ACL rule	This argument can be 802.3/802.2, 802.3, ether_ii, or snap.
lsap lsap-code lsap-wildcard	lsap field	Specifies the lsap field for the ACL rule	lsap-code: Encapsulation format of data frames, a 16-bit hexadecimal number. lsap-wildcard: Mask of the lsap value, a 16-bit hexadecimal number used to specify the mask bits.

Parameter	Type	Function	Description
source { source-addr source-mask | vlan-id }*	Source MAC address information	Specifies the source MAC address range for the ACL rule	source-addr: Source MAC address, in the format of H-H-H. source-mask: Mask of the source MAC address, in the format of H-H-H. vlan-id: Source VLAN ID, in the range of 1 to 4094.
dest dest-addr dest-mask	Destination MAC address information	Specifies the destination MAC address range for the ACL rule	dest-addr: Destination MAC address, in the format of H-H-H. dest-mask: Mask of the destination MAC address, in the format of H-H-H.
cos cos	Priority	Specifies the 802.1p priority for the rule	cos: VLAN priority, in the range of 0 to 7.
time-range time-name	Time range information	Specifies the time range in which the ACL rule is active	time-name: Specifies the name of the time range in which the rule is active, a string comprising 1 to 32 characters.
type protocol-type protocol-mask	Protocol type of Ethernet frames	Specifies the protocol type of Ethernet frames for the ACL rule	protocol-type: Protocol type. protocol-mask: Protocol type mask.

Note:

- An H3C S3600 Ethernet switch does not support the *format-type* argument for a layer 2 ACL.
- A rule with the **lsap** keyword specified can be applied to a port but does not take effect.

If you specify the **cos** keyword, you can directly input a value ranging from 0 to 7 or input one of the keywords listed in Table 1-6 as the CoS value.

Table 1-14 CoS value and the corresponding keywords

Keyword	CoS in decimal	CoS in binary
best-effort	0	000
background	1	001

Keyword	CoS in decimal	CoS in binary
spare	2	010
excellent-effort	3	011
controlled-load	4	100
video	5	101
voice	6	110
network-management	7	111

When you define an ACL rule using the **rule** command with the *rule-id* argument provided,

- If the ACL rule identified by the *rule-id* argument already exists, the settings specified in the **rule** command overwrite the corresponding settings of the existing rule. And the existing settings remain unchanged if the corresponding settings are not specified in the command.
- If the ACL rule identified by the *rule-id* argument does not exist, you will create a new rule.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.

If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically.

1.5.3 Configuration Example

Configure ACL 4000 to deny packets sourced from the MAC address 000d-88f5-97ed, destined for the MAC address 0011-4301-991e, and with their 802.1p priority being 3.

```
<H3C> system-view
[H3C] acl number 4000
[H3C-acl-ethernetframe-4000] rule deny cos 3 source 000d-88f5-97ed
ffff-ffff-ffff dest 0011-4301-991e ffff-ffff-ffff
[H3C-acl-ethernetframe-4000] display acl 4000
Ethernet frame ACL  4000, 1 rule
Acl's step is 1
 rule 0 deny cos excellent-effort source 000d-88f5-97ed ffff-ffff-ffff dest
0011-4301-991e ffff-ffff-ffff
```

1.6 User-Defined ACL Configuration

A user-defined ACL filters packets by comparing specific bytes in packet headers with specified string.

A user-defined ACL can be numbered from 5000 to 5999.

1.6.1 Configuration Preparation

To configure a time range-based user-defined ACL rule, you need to define the corresponding time ranges first. For information about time range configuration, refer to section 1.2 "Time Range Configuration".

1.6.2 Configuration Procedure

Table 1-15 Define a user-defined ACL rule

Operation	Command	Description
Enter system view	**system-view**	—
Create a user-defined ACL or enter user-defined ACL view	**acl number** *acl-number*	Required
Define an ACL rule	**rule** [*rule-id*] { **permit** | **deny** } [*rule-string rule-mask offset*] &<1-8> [**time-range** *name*]	Required
Assign a description string to the ACL	**description** *text*	Optional
Assign a description string to the ACL rule	**rule** *rule-id* **comment** *text*	Optional

Note:

The bytes in packet headers and to be compared with the specified string are determined by the offset from the beginning of the packet headers. You can specify the offset through the *offset* argument when executing the **rule** command. Note the following when you specify the offset.

- Each packet that is processed by a switch internally carries a VLAN tag. A VLAN tag is four bytes in size.
- A switch with the VLAN VPN function enabled inserts a VLAN tag to each packet it processes no matter whether or not the packet already carries a VLAN tag before being processed. Each packet carries two VLAN tags after being processed by a switch of this type.

When you define an ACL rule using the **rule** command with the *rule-id* argument provided,

- If the ACL rule identified by the *rule-id* argument already exists, the settings specified in the **rule** command overwrite the corresponding settings of the existing

rule. And the existing settings remain unchanged if the corresponding settings are not specified in the command.

- If the ACL rule identified by the *rule-id* argument does not exist, you will create a new rule.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.

If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically.

1.6.3 Configuration Example

Configure ACL 5001 to deny all the TCP packets. The ACL is active from 18:00 to 23:00 on each Saturday(The VLAN VPN function not enabled).

```
<H3C> system-view
[H3C] time-range t1 18:00 to 23:00 sat
[H3C] acl number 5001
[H3C-acl-user-5001] rule 25 deny 06 ff 27 time-range t1
[H3C-acl-user-5001] display acl 5001
User defined ACL  5001, 1 rules
Acl's step is 1
rule 25 deny 06 ff 27 time-range t1 (Inactive)
```

1.7 Applying ACLs on Ports

By applying ACLs on ports, you can filter outbound or inbound packets on the corresponding ports.

1.7.1 Configuration Preparation

You need to define an ACL before applying it on a port. For information about defining an ACL, refer to section 1.3 “Basic ACL Configuration”, section 1.4 “Advanced ACL Configuration”, section 1.5 “Layer 2 ACL Configuration”, and section 1.6 “User-Defined ACL Configuration”.

1.7.2 Configuration Procedure

Table 1-16 Apply an ACL on a port

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Apply an ACL on the port	**packet-filter** { **inbound** | **outbound** } *acl-rule*	Required

You can apply ACLs on a port in different ways, as listed in Table 1-17.

Table 1-17 Ways to apply ACLs on a port

Combination mode	The *acl-rule* argument
Apply all the rules of an ACL that is of IP type	**ip-group** *acl-number*
Apply a rule of an ACL that is of IP type	**ip-group** *acl-number* **rule** *rule-id*
Apply all the rules of an ACL that is of link type	**link-group** *acl-number*
Apply a rule of an ACL that is of link type	**link-group** *acl-number* **rule** *rule-id*
Apply all the rules of a user-defined ACL	**user-group** *acl-number*
Apply a rule of a user-defined ACL	**user-group** *acl-number* **rule** *rule-id*
Apply a rule of an ACL that is of IP type and a rule of an ACL that is of link type	**ip-group** *acl-number* **rule** *rule-id* **link-group** *acl-number* **rule** *rule-id*

1.7.3 Configuration Example

Apply ACL 2100 on GigabitEthernet1/1/1 to filter inbound packets.

```
<H3C> system-view
[H3C] interface gigabitethernet 1/1/1
[H3C-GigabitEthernet1/1/1] packet-filter inbound ip-group 2100
```

1.8 Displaying ACL Configuration

After the above configuration, you can execute the **display** commands in any view to view the ACL running information, so as to verify the configuration.

Table 1-18 Display ACL configuration

Operation	Command	Description
Display a configured ACL or all the ACLs	**display acl** { **all** | *acl-number* }	These commands can be executed in any view.
Display a time range or all the time ranges	**display time-range** { **all** | *time-name* }	
Display the information about packet filtering	**display packet-filter** { **interface** *interface-type interface-number* | **unitid** *unit-id* }	

1.9 ACL Configuration Example

1.9.1 Basic ACL Configuration Example

I. Network requirements

Apply an ACL on GigabitEthernet1/1/1 to filter packets sourced from 10.1.1.1 from 8:00 to 18:00 everyday.

II. Network diagram

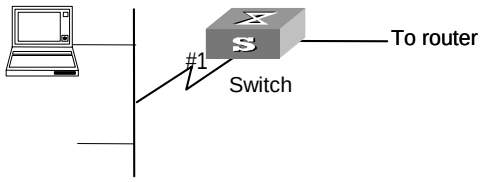


Figure 1-1 Network diagram for basic ACL configuration

III. Configuration procedure

Note:

Only the commands related to the ACL configuration are listed below.

1) Define the time range

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<H3C> system-view
[H3C] time-range test 8:00 to 18:00 daily
```

2) Define an ACL for packets with the source IP address of 10.1.1.1.

Create ACL 2000 or enter ACL 2000 view.

```
[H3C] acl number 2000
```

Define an access rule to deny packets with their source IP addresses being 10.1.1.1, applying the time range to the ACL.

```
[H3C-acl-basic-2000] rule 1 deny source 10.1.1.1 0 time-range test
[H3C-acl-basic-2000] quit
```

3) Apply the ACL on the port

Apply ACL 2000 on the port.

```
[H3C] interface gigabitethernet1/1/1
[H3C-GigabitEthernet1/1/1] packet-filter inbound ip-group 2000
```

1.9.2 Advanced ACL Configuration Example

I. Network requirements

The networks of different departments of an enterprise are interconnected through a switch. The IP address of the wage query server is 192.168.1.2. The network of the R&D department is connected to GigabitEthernet1/1/1 of the switch. Apply an ACL to deny requests sourced from the R&D department and destined for the wage server during the working hours (8:00 to 18:00).

II. Network diagram

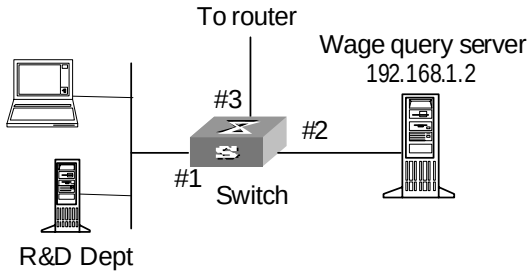


Figure 1-2 Network diagram for advanced ACL configuration

III. Configuration procedure

Note:

Only the commands related to the ACL configuration are listed below.

---

1) Define the time range

Define a periodic time range that is active from 8:00 to 18:00 on each working day.

```
<H3C> system-view
[H3C] time-range test 8:00 to 18:00 working-day
```

2) Define an ACL for filtering requests destined for the wage server.

Create ACL 3000 or enter ACL 3000 view.

```
[H3C] acl number 3000
```

Define an ACL rule for requests destined for the wage server.

```
[H3C-acl-adv-3000] rule 1 deny ip destination 192.168.1.2 255.255.255.0
time-range test
[H3C-acl-adv-3000] quit
```

3) Apply the ACL on the port.

Apply ACL 3000 on the port.

```
[H3C] interface gigabitethernet1/1/1
[H3C-GigabitEthernet1/1/1] packet-filter inbound ip-group 3000
```

1.9.3 Layer 2 ACL Configuration Example

I. Network requirements

Apply an ACL on GigabitEthernet1/1/1 port to filter packets with their source MAC addresses being 000f-e20f-0101 and destination MAC addresses being 000f-e20f-0303 from 8:00 to 18:00 everyday.

II. Network diagram

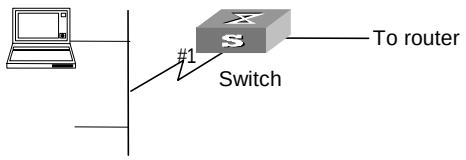


Figure 1-3 Network diagram for Layer 2 ACL configuration

III. Configuration procedure

Note:

Only the commands related to the ACL configuration are listed below.

---

1) Define the time range

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<H3C> system-view
[H3C] time-range test 8:00 to 18:00 daily
```

2) Define an ACL rule for packets with the source MAC address of 000f-e20f-0101 and destination MAC address of 000f-e20f-0303.

Create ACL 4000 or enter ACL 4000 view.

```
[H3C] acl number 4000
```

Define an ACL rule to deny packets with the source MAC address of 000f-e20f-0101 and destination MAC address of 000f-e20f-0303, specifying the time range named test for the ACL rule.

```
[H3C-acl-ethernetframe-4000] rule 1 deny source 000f-e20f-0101 ffff-ffff-ffff
dest 000f-e20f-0303 ffff-ffff-ffff time-range test
[H3C-acl-ethernetframe-4000] quit
```

3) Apply the ACL on GigabitEthernet1/1/1.

Apply the ACL on GigabitEthernet1/1/1.

```
[H3C] interface GigabitEthernet1/1/1
[H3C-GigabitEthernet1/1/1] packet-filter inbound link-group 4000
```

1.9.4 User-Defined ACL Configuration Example

I. Network requirements

Apply an ACL on Ethernet1/0/1 to deny all the TCP packets within the time range from 8:00 to 18:00 everyday.

II. Network diagram

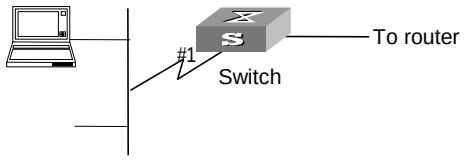


Figure 1-4 Network diagram for user-defined ACL configuration

III. Configuration procedure

Note:

Only the commands related to the ACL configuration are listed below.

---

1) Define the time range.

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
[H3C] time-range aaa 8:00 to 18:00 daily
```

2) Create an ACL rule to filter TCP packets.

Create ACL 5000 or enter ACL 5000 view.

```
[H3C] acl number 5000
```

Define a rule for TCP packets(The VLAN VPN function not enabled).

```
[H3C-acl-user-5000] rule 1 deny 06 ff 27 time-range aaa
```

3) Apply the ACL on Ethernet1/0/1.

Apply the ACL 5000 on Ethernet1/0/1.

```
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] packet-filter inbound user-group 5000
```

Table of Contents

Chapter 1 QoS Configuration 1-1
1.1 Overview 1-1
1.1.1 Traffic 1-1
1.1.2 Traffic Classification 1-1
1.1.3 Precedence 1-2
1.1.4 Priority of Protocol Packets 1-5
1.1.5 Priority Remark 1-5
1.1.6 Packet Filter 1-5
1.1.7 Port Rate Limit 1-5
1.1.8 TP 1-5
1.1.9 Queue Scheduling Configuration Synchronization on Aggregated Ports 1-7
1.1.10 Redirect 1-8
1.1.11 Queue Scheduling 1-8
1.1.12 Traffic-based Traffic Statistics 1-11
1.2 QoS Supported by S3600 Series 1-11
1.3 Configuring the Mapping between 802.1p Priority and Queues 1-12
1.4 Setting to Use the Port Priority or Packet Priority 1-13
1.5 Configuring Priority Remark 1-14
1.5.1 Configuration Prerequisites 1-15
1.5.2 Configuration Procedure 1-15
1.5.3 Configuration Example 1-16
1.6 Setting the Precedence of Protocol Packet 1-16
1.6.1 Configuration Prerequisites 1-16
1.6.2 Configuration Procedure 1-16
1.6.3 Configuration Example 1-17
1.7 Configuring Port Rate Limit 1-17
1.7.1 Configuration Prerequisites 1-17
1.7.2 Configuration Procedure 1-18
1.7.3 Configuration Example 1-18
1.8 Configuring TP 1-18
1.8.1 Configuration Prerequisites 1-18
1.8.2 Configuration Procedure of TP 1-19
1.8.3 Configuration Example 1-20
1.9 Configuring Redirect 1-20
1.9.1 Configuration Prerequisites 1-20
1.9.2 Configuration Procedure 1-20
1.9.3 Configuration Example 1-21
1.10 Configuring Queue-Scheduling 1-21

1.10.1 Configuration Prerequisites 1-22
1.10.2 Configuration Procedure 1-22
1.10.3 Configuration Example 1-23
1.11 Configuring Congestion Avoidance 1-24
1.11.1 Configuration Prerequisites 1-24
1.11.2 Configuration Procedure 1-24
1.11.3 Configuration Example 1-25
1.12 Configuring Traffic Statistics 1-25
1.12.1 Configuration Prerequisites 1-25
1.12.2 Configuration Procedure of Traffic Statistics 1-25
1.12.3 Clearing Traffic Statistics Information 1-26
1.12.4 Configuration Example 1-26
1.13 QoS Configuration Example 1-27
1.13.1 Configuration Example of TP and Port Rate Limit 1-27
1.13.2 Configuration Example of Priority Remark 1-28

Chapter 2 QoS Profile Configuration 2-1
2.1 Introduction to QoS Profile 2-1
2.1.1 Application Mode of QoS Profile 2-1
2.2 Introduction to QoS Profile Configurations 2-1
2.3 Configuring QoS Profile 2-2
2.3.1 Configuration Prerequisites 2-2
2.3.2 Configuration Procedure 2-2
2.3.3 Configuration Example 2-3
2.4 Applying the QoS Profile to the Port Manually 2-5
2.5 Displaying QoS Profile 2-6

Chapter 1 QoS Configuration

1.1 Overview

QoS (Quality of Service) is a concept generally existing in occasions with service supply and demand. It evaluates the ability to meet the need of the customers in service. Generally, the evaluation is not to grade precisely. Its purpose is to analyze the conditions where the service is the best and the conditions where the service still needs improvement and then to make improvements in the specified aspects.

In an internet, QoS evaluates the ability of the network to deliver packets. The evaluation on QoS can be based on different aspects because the network provides various services. Generally speaking, QoS is the evaluation on the service ability to support the core requirements such as delay, jitter, and packet loss ratio in the packet delivery.

1.1.1 Traffic

Traffic means service traffic; that is, all the packets passing the switch.

1.1.2 Traffic Classification

Traffic classification means identifying packets that conform to certain characteristics according to certain rules.

A classification rule is a filter rule configured to meet your management requirements. It can be very simple. For example, you can use a classification rule to identify traffic with different priorities according to the ToS field in the IP packet header. It can be very complicated too. For example, you can use a classification rule to identify the packets according to the combination of link layer (Layer 2), network layer (Layer 3), and transport layer (Layer 4) information including MAC addresses, IP protocols, source addresses, destination addresses, port numbers of applications, and so on.

Classification is generally based on the information in the packet header and rarely based on the packet contents.

1.1.3 Precedence

1) IP precedence, ToS precedence, and DSCP precedence

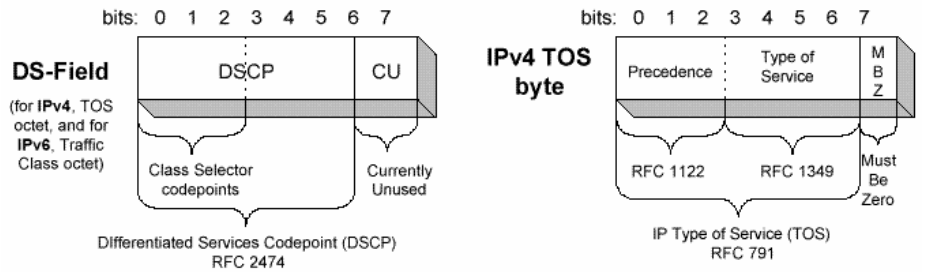


Figure 1-1 DS field and TOS byte

The TOS field in an IP header contains eight bits:

- The first three bits indicate IP precedence in the range of 0 to 7.
- Bit 3 to bit 6 indicate ToS precedence in the range of 0 to 15.
- RFC2474 re-defines the ToS field in the IP packet header, which is called the DS field. The first six (bit 0 to bit 5) bits of the DS field indicate DSCP precedence in the range of 0 to 63. The first three bits in DSCP precedence are class selector codepoints, bit 4 and bit 5 indicate drop precedence, and bit 6 is zero indicating that the device sets the service class with the DS model. The last two bits (bit 6 and bit 7) are reserved bits.

The precedence values of the IP packet indicate eight different service classes.

Table 1-1 Description on IP Precedence

IP Precedence (decimal)	IP Precedence (binary)	Description
0	000	routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

The Diff-Serv network defines four traffic classes:

- Expedited Forwarding (EF) class: In this class, packets can be forwarded regardless of link share of other traffic. The class is suitable for preferential

services with low delay, low packet loss ratio, low jitter, and assured bandwidth (such as virtual leased line);

- Assured forwarding (AF) class: This class is further divided into four subclasses (AF1/2/3/4) and a subclass is further divided into three drop priorities, so the AF service level can be segmented. The QoS rank of the AF class is lower than that of the EF class;
- Class selector (CS) class: This class comes from the IP TOS field and includes eight classes;
- Best Effort (BE) class: This class is a special class without any assurance in the CS class. The AF class can be degraded to the BE class if it exceeds the limit. Current IP network traffic belongs to this class by default.

Table 1-2 Description on DSCP values

DSCP value (decimal)	DSCP value (binary)	Description
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	default (be)

2) 802.1p priority

802.1p priority lies in Layer 2 packet headers and is applicable to occasions where the Layer 3 packet header does not need analysis but QoS must be assured at Layer 2.

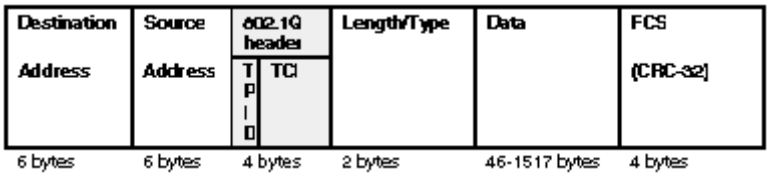


Figure 1-2 An Ethernet frame with an 802.1Q tag header

As shown in the figure above, each host supporting 802.1Q protocol adds a 4-byte 802.1Q tag header after the source address of the former Ethernet frame header when sending packets.

The 4-byte 802.1Q tag header contains a 2-byte Tag Protocol Identifier (TPID) whose value is 8100 and a 2-byte Tag Control Information (TCI). TPID is a new class defined by IEEE to indicate a packet with an 802.1Q tag. Figure 1-3 describes the detailed contents of an 802.1Q tag header.

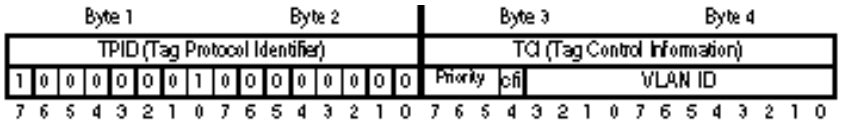


Figure 1-3 802.1Q tag headers

In the figure above, the 3-bit priority field in TCI is 802.1p priority in the range of 0 to 7. These three bits specify the precedence of the frame. Eight classes of precedence are used to determine which packet is sent preferentially when congestion occurs.

Table 1-3 Description on 802.1p priority

CoS (decimal)	CoS (binary)	Description
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

The precedence is called 802.1p priority because the related applications of this precedence are defined in detail in the 802.1p specifications.

1.1.4 Priority of Protocol Packets

Protocol packets carry their own priority. You can perform QoS actions on protocol packets by setting their priorities.

1.1.5 Priority Remark

The priority remark function is to use ACL rules in traffic identification and remark the priority for the packets matching the ACL rules.

1.1.6 Packet Filter

Packet filter means filtering the service traffic. For example, in the operation of dropping packets, the service traffic matching the traffic classification rule is dropped and the other traffic is permitted. The Ethernet switch adopts a complicated traffic classification rule to filter the packets based on much information and to drop these useless, unreliable, and doubtful packets. Therefore, the network security is enhanced.

The two critical steps in the packet filter operation are:

Step1: Classify the inbound packets to the port by the set classification rule.

Step 2: Perform the filter——drop operation on the classified packets.

The packet filter function can be implemented by applying ACL rules on the port. Refer to the description in the *ACL* module for detailed configurations.

1.1.7 Port Rate Limit

Port rate limit is port-based rate limit. It limits the total rate of outbound packets on a port.

1.1.8 TP

The network will be made more congested by plenty of continuous burst packets if the traffic of each user is not limited. The traffic of each user must be limited in order to make better use of the limited network resources and provide better service for more users. For example, a traffic can be limited to get only its committed resources during a time period to avoid network congestion caused by excessive bursts.

TP (traffic policing) is a kind of traffic control policy to limit the traffic and its resource usage by supervising the traffic specification. The regulation policy is implemented according to the evaluation result on the premise of knowing whether the traffic exceeds the specification when TP or TS is performed. The token bucket is generally adopted in the evaluation of traffic specification.

I. Traffic evaluation and the token bucket

The token bucket can be considered as a container with a certain capacity to hold tokens. The system puts tokens into the bucket at the set rate. When the token bucket is full, the extra tokens will overflow and the number of tokens in the bucket stops increasing.

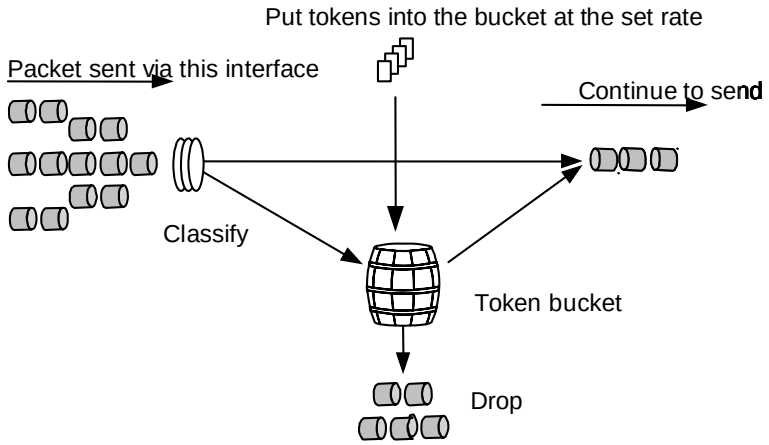


Figure 1-4 Evaluate the traffic with the token bucket

1) Evaluating the traffic with the token bucket

The evaluation for the traffic specification is based on whether the number of tokens in the bucket can meet the need of packet forwarding. If the number of tokens in the bucket is enough to forward the packets (generally, one token is associated with a 1-bit forwarding authority), the traffic is conforming to the specification; otherwise, the traffic is nonconforming or excess.

When the token bucket evaluates the traffic, its parameter configurations include:

- Average rate: The rate at which tokens are put into the bucket, namely, the permitted average rate of the traffic. It is generally set to committed information rate (CIR).
- Burst size: The capacity of the token bucket, namely, the maximum traffic size that is permitted in each burst. It is generally set to committed burst size (CBS). The set burst size must be greater than the maximum packet length.

One evaluation is performed on each arriving packet. In each evaluation, if the number of tokens in the bucket is enough, the traffic is conforming to the specification and you must take away some tokens whose number is corresponding to the packet forwarding authority; if the number of tokens in the bucket is not enough, it means that too many tokens have been used and the traffic is excess.

2) Complicated evaluation

You can set two token buckets in order to evaluate more complicated conditions and implement more flexible regulation policies. For example, TP uses four parameters:

- CIR
- CBS
- Peak information rate (PIR)
- Excess burst size (EBS)

Two token buckets are used in this evaluation. Their rates of putting tokens into the buckets are CIR and PIR respectively, and their sizes are CBS and EBS respectively (the two buckets are called C bucket and E bucket respectively for short), representing different permitted burst levels. In each evaluation, you can implement different regulation policies in different conditions, including “enough tokens in C bucket”, “insufficient tokens in C bucket but enough tokens in E bucket” and “insufficient tokens in both C bucket and E bucket”.

II. TP

The typical application of TP is to supervise the specification of certain traffic into the network and limit it within a reasonable range, or to "discipline" the extra traffic. In this way, the network resources and the interests of the operators are protected. For example, you can limit HTTP packets to be within 50% of the network bandwidth. If the traffic of a certain connection is excess, TP can choose to drop the packets or to reset the priority of the packets.

TP is widely used in policing the traffic into the network of internet service providers (ISPs). TP can classify the policed traffic and perform pre-defined policing actions based on different evaluation results. These actions include:

- Forward: Forward the packet whose evaluation result is “conforming” or mark DSCP precedence for Diff-Serv packets and then forward them.
- Drop: Drop the packet whose evaluation result is “nonconforming”.
- Modify the precedence and forward: Modify the priority of the packets whose evaluation result is “partly-conforming” and forward them.
- Enter the next-rank policing: TP can be piled up rank by rank and each rank polices more detailed objects.

1.1.9 Queue Scheduling Configuration Synchronization on Aggregated Ports

The feature of queue scheduling configuration synchronization on aggregated ports makes the queue scheduling configuration synchronous on each port of an aggregation group.

- Supporting the feature of queue scheduling configuration synchronization on the ports in an aggregation group

When you modify or delete the queue scheduling mode in Ethernet port view, the queue scheduling modes of all the ports in the aggregation group are modified or deleted if this port belongs to an aggregation group; only the queue scheduling mode of this port is modified or deleted if this port does not belong to any aggregation group.

- Dynamic aggregation supported by queue scheduling modes on ports

If the queue scheduling configuration information of some LACP-enabled ports in up state is the same, these ports can be aggregated into the same aggregation group.

- Static aggregation or manual aggregation supported by queue scheduling modes on ports

You can add a queue-scheduling-enabled port into a specific static or manual aggregation group. This operation can be performed not only on the local device but also across devices in an intelligent resilient framework (IRF).

- You can use the **copy** command to copy the queue scheduling configuration of a port.

🕮 **Note:**

For the introduction to the **copy** command, refer to the Basic Port Configuration Module in this manual.

1.1.10 Redirect

You can re-specify the forwarding port of packets as required by your own QoS policy.

1.1.11 Queue Scheduling

When the network is congested, the problem that many packets compete for resources must be solved, usually through queue scheduling.

In the following section, strict priority (SP) queues, weighted fair queue (WFQ), and weighted round robin (WRR) queues are introduced.

1) SP queueing

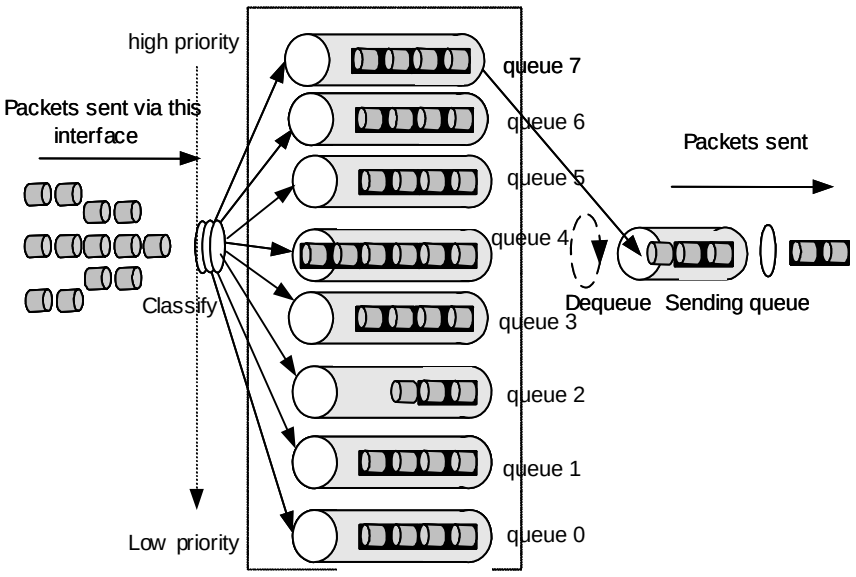


Figure 1-5 Diagram for SP queueing

SP queue-scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay. Assume that there are eight output queues on the port and the preferential queue classifies the eight output queues on the port into eight classes, which are queue7, queue6, queue5, queue4, queue3, queue2, queue1, and queue0. Their priorities decrease in order.

In queue scheduling, SP sends packets in the queue with higher priority strictly following the priority order from high to low. When the queue with higher priority is empty, packets in the queue with lower priority are sent. You can put critical service packets into the queues with higher priority and put non-critical service (such as e-mail) packets into the queues with lower priority. In this case, critical service packets are sent preferentially and non-critical service packets are sent when critical service groups are not sent.

The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be “starved” because they are not served.

2) WFQ queueing

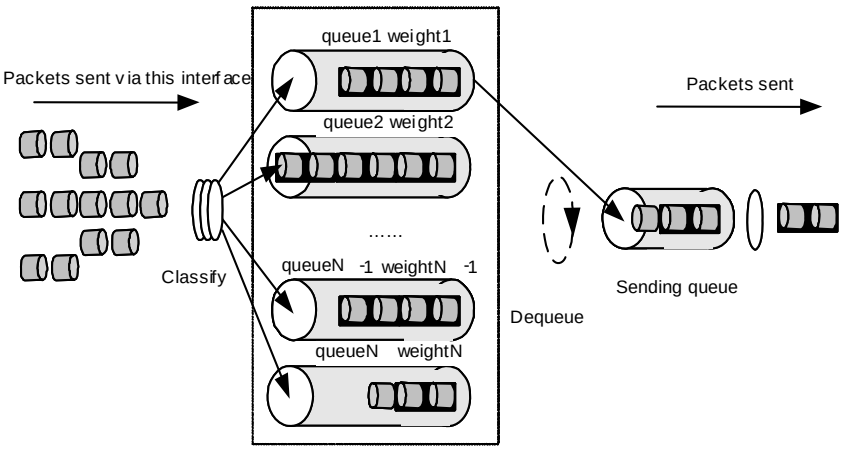


Figure 1-6 Diagram for WFQ

Before WFQ is introduced, you must understand fair queuing (FQ) first. FQ is designed for the purpose of sharing network resources fairly and optimizing the delays and delay jitters of all the flows. It takes the interests of all parties into account, such as:

- Different queues are scheduled fairly, so the delay of each flow is balanced globally.
- Both short and long packets are scheduled fairly. When there are multiple long packets and short packets to be sent among different queues, the short packets must be scheduled preferentially, so that the delay jitters of packets of each flow is reduced globally.

Compared with FQ, WFQ takes the priority into account when calculating the scheduling sequence of packets. Statistically speaking, WFQ assigns more scheduling chances to high priority packets than those to low priority packets. WFQ can classify the traffic automatically according to the session information of traffic including the protocol types, source and destination TCP or UDP port numbers, source and destination IP addresses, and priority bits in the TOS field. WFQ also provide as many queues as possible to accommodate each traffic evenly. Thus, the delay of each traffic is balanced globally. When the packets dequeue, WFQ assigns the bandwidth to each traffic on the egress according to the traffic precedence or DSCP precedence. The lower the traffic precedence is, the less bandwidth the traffic gets. The higher the traffic precedence is, the more bandwidth the traffic gets. Finally, each queue is polled and the corresponding number of packets are taken out to be sent according to the proportion of bandwidth.

You can use the WFQ algorithm to assign bandwidth to queue 0 to queue 7, and then decide which queue a traffic flows into according to the mapping between the COS value of the traffic and the queue, and also deicide how much bandwidth is to be assigned to each traffic.

3) WRR queueing

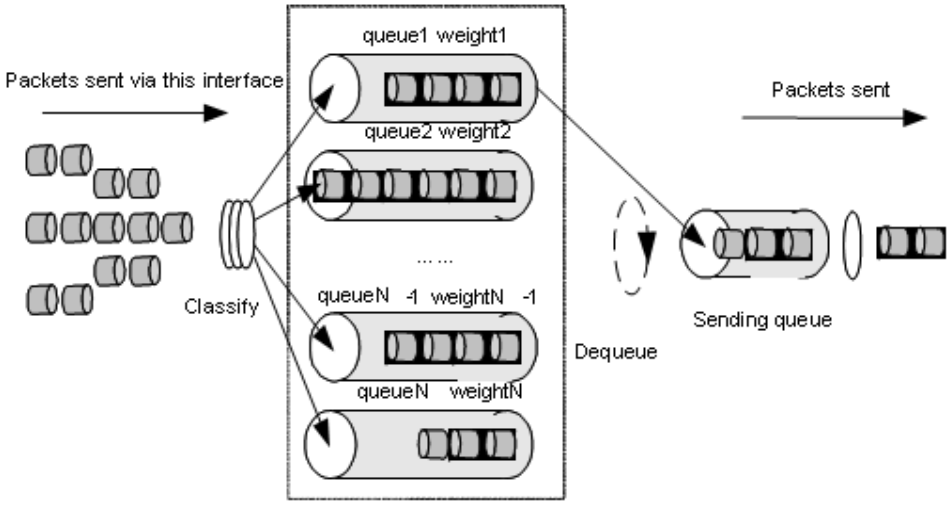


Figure 1-7 Diagram for WRR

WRR queue-scheduling algorithm schedules all the queues in turn and every queue can be assured of a certain service time. Assume there are eight priority queues on a port. WRR configures a weight value for each queue, which is w7, w6, w5, w4, w3, w2, w1, and w0. The weight value indicates the proportion of obtaining resources. On a 100 M port, configure the weight value of WRR queue-scheduling algorithm to 50, 50, 30, 30, 10, 10, 10, and 10 (corresponding to w7, w6, w5, w4, w3, w2, w1, and w0 in order). In this way, the queue with the lowest priority can get 5 Mbps bandwidth at least, and the disadvantage of SP queue-scheduling that the packets in queues with lower priority may not get service for a long time is avoided. Another advantage of WRR queue is that: though the queues are scheduled in order, the service time for each queue is not fixed; that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use.

1.1.12 Traffic-based Traffic Statistics

The function of traffic-based traffic statistics is to use ACL rules in traffic identifying and perform traffic statistics on the packets matching the ACL rules. You can get the statistics of the packets you are interested in through this function.

1.2 QoS Supported by S3600 Series

Table 1-4 QoS functions supported by S3600 series and related commands

QoS	Specification	Related command
Priority mapping	Support only the mapping between 802.1p priority and local queues	**qos cos-local-precedence-map**

QoS	Specification	Related command
Port priority	Supported	**priority** *priority-level* **priority trust**
TP	—	**traffic-limit**
Priority remark	—	**traffic-priority**
Redirect	—	**traffic-redirect**
Queue scheduling	Support SP, WFQ, and WRR Support queue scheduling configuration synchronization on aggregated ports	**queue-scheduler**
Traffic statistics	Supported	**traffic-statistic**
Set the priority of protocol packets	Supported	**protocol-priority**

1.3 Configuring the Mapping between 802.1p Priority and Queues

The mapping between the local precedence and the outbound queue is one-to-one. You can modify the mapping between the 802.1p priority and the outbound queue by modifying the mapping between the 802.1p priority and the local precedence.

I. Configuration prerequisites

You have understood the mapping between the 802.1p priority and the local precedence and the default mapping table.

II. Configuration procedure

Table 1-5 Configure the mapping table

Operation	Command	Description
Enter system view	**system-view**	—
Configure the COS-to-local-precedence mapping table	**qos** **cos-local-precedence-map** *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*	Optional

Operation	Command	Description
Display the mapping table	**display qos cos-local-precedence-map**	Optional You can execute the **display** command in any view

III. Configuration example

- Configure the following 802.1p priority-to-local precedence mappings: 0 to 2, 1 to 3, 2 to 4, 3 to 1, 4 to 7, 5 to 0, 6 to 5, and 7 to 6.
- Display the configuration results.

Configuration procedure:

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] qos cos-local-precedence-map 2 3 4 1 7 0 5 6
[H3C] dis qos cos-local-precedence-map
 cos-local-precedence-map:
            cos(802.1p) :      0     1     2     3     4     5     6     7
------------------------------------------------------------------------------
local precedence(queue) :      2     3     4     1     7     0     5     6
```

1.4 Setting to Use the Port Priority or Packet Priority

By default, the switch replaces the 802.1p priority of the received packet with the priority of the inbound interface, and then assigns local precedence to the packet according to the priority. In this case, you can set the port priority.

In addition, you can specify the switch to use the packet priority.

I. Configuration prerequisites

- The priority trust mode is specified
- The port whose priority is to be configured is specified
- The priority value of the specified port is specified

II. Configuration procedure

Table 1-6 Set to use the port priority

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Set the port priority	**priority** *priority-level*	Optional By default, the port priority is 0

Table 1-7 Set to use the packet priority

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the switch to use the packet priority	**priority trust**	Through this configuration, the switch uses the packet priority instead of the port priority

III. Configuration example

- Set to use the port priority and specify the priority of Ethernet1/0/1 to 7.

Configuration procedure:

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] undo priority
[H3C-Ethernet1/0/1] priority 7
```

- Set the switch to use the 802.1p priority carried in the packet on Ethernet1/0/1.

Configuration procedure:

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] priority trust
```

1.5 Configuring Priority Remark

Refer to section 1.1.5 "Priority Remark" for the introduction to priority remark.

Priority remark can be implemented in the following ways:

- Through TP. When configuring TP, you can define the action of remarking the DSCP precedence of the packets out of the traffic limit. Refer to section 1.8.2 "Configuration Procedure of TP".
- Through the **traffic-priority** command. You can remark the IP precedence, 802.1p precedence, DSCP precedence, and local precedence of the packets.

1.5.1 Configuration Prerequisites

- ACL rules used for traffic identifying are defined. Refer to the *ACL* module in the manual for defining ACL rules
- The type and value of the precedence that the packets matching ACL rules are remarked are determined
- The ports which need this configuration are defined

1.5.2 Configuration Procedure

Table 1-8 Configure priority remark

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Use ACL rules in traffic identifying and specify a new precedence for the packet matching the ACL rules	**traffic-priority** { **inbound** | **outbound** } *acl-rule* { { **dscp** *dscp-value* | **ip-precedence** { *pre-value* | **from-cos** } } | **cos** { *pre-value* | **from-ipprec** } | **local-precedence** *pre-value* }*	Required
Display the parameter configurations of priority remark	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-priority**	Optional You can execute the **display** command in any view
Display all the QoS settings of the port	**display qos-interface** { *interface-type interface-number* | *unit-id* } **all**	

acl-rule: Applied ACL rules which can be the combination of various ACL rules. The way of combination is described in the following table:

Table 1-9 Ways of applying combined ACLs

ACL combination	Form of the ***acl-rule*** **argument**
Apply all the rules in an IP ACL separately	**ip-group** *acl-number*
Apply a rule in an IP ACL separately	**ip-group** *acl-number* **rule** *rule-id*
Apply all the rules in a Link ACL separately	**link-group** *acl-number*
Apply a rule in a Link ACL separately	**link-group** *acl-number* **rule** *rule-id*
Apply all the rules in a user-defined ACL separately	**user-group** *acl-number*

ACL combination	Form of the *acl-rule* argument
Apply a rule in a user-defined ACL separately	**user-group** *acl-number* **rule** *rule-id*
Apply a rule in an IP ACL and a rule in a Link ACL at the same time	**ip-group** *acl-number* **rule** *rule-id* **link-group** *acl-number* **rule** *rule-id*

1.5.3 Configuration Example

- Ethernet1/0/1 of the switch is connected to the 10.1.1.1/24 network segment
- Remark the DSCP precedence of the traffic from the 10.1.1.1/24 network segment to 56

Configuration procedure:

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] acl number 2000
[H3C-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[H3C-acl-basic-2000] quit
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] traffic-priority inbound ip-group 2000 dscp 56
```

1.6 Setting the Precedence of Protocol Packet

The protocol packet carries its own precedence. You can modify the precedence of the protocol packet by setting its precedence. And then you can match the precedence with the corresponding QoS action to perform the corresponding QoS operation on the protocol packet.

1.6.1 Configuration Prerequisites

- The type of protocol whose precedence needs modification is specified
- The precedence value after modification is specified

1.6.2 Configuration Procedure

Table 1-10 Set the precedence of the protocol packet

Operation	Command	Description
Enter system view	**system-view**	—

Operation	Command	Description
Set the precedence of the protocol packet	**protocol-priority protocol-type** *protocol-type* { **ip-precedence** *ip-precedence* | **dscp** *dscp-value* }	Required You can modify the IP precedence or DSCP precedence of the protocol packet Only the precedence of TELNET, OSPF, SNMP, and ICMP protocol packets is supported currently
Display the precedence of the protocol packet	**display protocol-priority**	Optional You can execute the **display** command in any view

Note:

The precedence of OSPF protocol packets cannot be changed on S3600-SI series switches.

1.6.3 Configuration Example

- Set the IP precedence of ICMP protocol packets to 3.
- Display the configuration results.

Configuration procedure:

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] protocol-priority protocol-type icmp ip-precedence 3
[H3C] display protocol-priority
Protocol: icmp
  IP-Precedence: flash(3)
```

1.7 Configuring Port Rate Limit

1.7.1 Configuration Prerequisites

- The ports on which rate limit is to be performed is specified
- The target rate is specified
- The direction of rate limit is specified

1.7.2 Configuration Procedure

Table 1-11 Configure port rate limit

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure port-based rate limit	**line-rate** { **inbound** | **outbound** } *target-rate*	Required • *target-rate*: Total rate to limit packet sending and receiving on the port, in Kbps. The granularity of rate limit is 64 Kbps. If the number you input is in the range of N*64 to (N+1)*64 (N is a natural number), the switch will set the value to (N+1)*64 Kbps automatically • The rate range of 100 M Ethernet ports is from 64 to 99,968 • The rate range of Gigabit Ethernet ports is in from 64 to 1,000,000

1.7.3 Configuration Example

- Set rate limit in the outbound direction of Ethernet1/0/1 on the switch
- The limit rate is 1 Mbps (1,024 Kbps)

Configuration procedure:

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] line-rate outbound 1024
```

1.8 Configuring TP

Refer to section 1.1.8 "TP" for the introduction to TP.

1.8.1 Configuration Prerequisites

- ACL rules used for traffic identifying are defined. Refer to the *ACL* module in the manual for defining ACL rules
- The limit rate for TP, the actions for the packets within the specified traffic and the actions for the packets beyond the specified traffic have been specified.

- The ports that need this configuration are specified

1.8.2 Configuration Procedure of TP

Table 1-12 Configure TP

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure traffic-based TP	**traffic-limit inbound** *acl-rule target-rate* [**exceed** *action*]	Required **exceed** *action*: Sets the actions on the packets exceeding the specified traffic when the packet traffic exceeds the specified traffic. The actions include: • **drop**: Drops the packets. • **remark-dscp** *dscp-value*: Resets the DSCP precedence of the packets and forwards them.
Display the parameter configurations of traffic policing	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-limit**	Optional You can execute the **display** command in any view
Display all the QoS settings of the port	**display qos-interface** { *interface-type interface-number* | *unit-id* } **all**	

acl-rule: Applied ACL rules which can be the combination of various ACL rules. The way of combination is described in Table 1-9.

🕮 **Note:**

- The granularity of TP is 64 Kbps. If the number you input is in the range of N*64 to (N+1)*64 (N is a natural number), the switch will set the value to (N+1)*64 Kbps automatically
- TP configuration is effective only for the ACL rules whose actions are **permit**.

1.8.3 Configuration Example

- Ethernet1/0/1 of the switch is connected to the 10.1.1.1/24 network segment
- Perform TP on the packets from the 10.1.1.1/24 network segment and the rate of TP is set to100 Kbps
- The packets beyond the specified traffic are forwarded after their DSCP precedence is remarked as 56

Configuration procedure:

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] acl number 2000
[H3C-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[H3C-acl-basic-2000] quit
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] traffic-limit inbound ip-group 2000 100 exceed
remark-dscp 56
```

1.9 Configuring Redirect

Refer to section 1.1.10 "Redirect" for the introduction to redirect.

1.9.1 Configuration Prerequisites

- ACL rules used for traffic identifying are defined. Refer to the *ACL* module in the manual for defining ACL rules.
- The port that the packets matching the configurations rules are redirected to is specified.
- The ports that need this configuration are specified.

1.9.2 Configuration Procedure

Table 1-13 Configure redirect

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure redirect	**traffic-redirect** { **inbound** | **outbound** } *acl-rule* { **cpu** | **interface** *interface-type interface-number* }	Required

Operation	Command	Description
Display the parameter configurations of redirect	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-redirect**	Optional You can execute the **display** command in any view
Display all the QoS settings of the port	**display qos-interface** { *interface-type interface-number* | *unit-id* } **all**	

acl-rule: Applied ACL rules which can be the combination of various ACL rules. The way of combination is described in Table 1-9.

Note:

- The redirect configuration is effective only for the ACL rules whose actions are **permit**.
- When packets are redirected to CPU, they cannot be forwarded normally.
- If you set to redirect the traffic to a Combo port in down state, the system automatically redirects the traffic to the port corresponding to the Combo port in up state.

1.9.3 Configuration Example

- Ethernet1/0/1 of the switch is connected to the 10.1.1.1/24 network segment
- Redirect all the traffic from the 10.1.1.1/24 network segment to Ethernet1/0/7

Configuration procedure:

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] acl number 2000
[H3C-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[H3C-acl-basic-2000] quit
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] traffic-redirect inbound ip-group 2000 interface
Ethernet1/0/7
```

1.10 Configuring Queue-Scheduling

Refer to section 1.1.11 "Queue Scheduling" for the introduction to queue scheduling.

1.10.1 Configuration Prerequisites

The queue-scheduling algorithm is specified: which queues adopt the WRR queue-scheduling algorithm, which queues adopt the WFQ queue-scheduling algorithm, and which queues adopt the SP queue-scheduling algorithm.

1.10.2 Configuration Procedure

Table 1-14 Configure queue scheduling in system view

Operation	Command	Description
Enter system view	**system-view**	—
Configure the queue scheduling mode	**queue-scheduler** { **strict-priority** | **wfq** *queue0-width queue1-width queue2-width queue3-width queue4-width queue5-width queue6-width queue7-width* | **wrr** *queue0-weight queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight* }	Required In WRR or WFQ mode, if the weight value or minimum bandwidth of one or more queues is set to 0, SP algorithm is used for this or these queues By default, all the outbound queues on the port adopt the WRR queue scheduling algorithm and their default weight values are 1:2:3:4:5:9:13:15.
Display the queue-scheduling mode and related parameters on the switch	**display queue-scheduler**	Optional You can execute the **display** command in any view.

Table 1-15 Configure queue scheduling in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Configure the queue scheduling mode	**queue-scheduler** { **wfq** *queue0-width queue1-width queue2-width queue3-width queue4-width queue5-width queue6-width queue7-width* | **wrr** *queue0-weight queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight* }	Required In WRR or WFQ mode, if the weight value or minimum bandwidth of one or more queues is set to 0, SP algorithm is used for this or these queues By default, all the outbound queues on the port adopt the WRR queue scheduling algorithm and their default weight values are 1:2:3:4:5:9:13:15.

Note:

- The queue scheduling algorithm defined by executing the **queue-scheduler** command in system view takes effect on all ports of the switch. The queue scheduling algorithm defined by executing the **queue-scheduler** command in Ethernet port view takes effect on the current port only. If the weight values (or bandwidth values) of the queues in the WRR (or WFQ) queue scheduling algorithm defined globally cannot satisfy the requirement of a port, you can modify the weight values (or bandwidth values) of the queues in Ethernet port view of this port. A new queue scheduling algorithm on this port will overwrite the globally defined queue weight value (or bandwidth value). You cannot use the **display queue-scheduler** command to display the queue weight (or bandwidth value) defined in Ethernet port view.
- If you have configured link aggregation groups, the queue scheduling algorithm defined on a port in an aggregation group will be synchronized to other ports in the aggregation group automatically.

1.10.3 Configuration Example

- The switch adopts the WRR queue scheduling algorithm, and the weight values of outbound queues are 2, 2, 3, 3, 4, 4, 5, and 5, respectively;
- Disable the applied queue scheduling mode. By default, all outbound queues on the port adopts the WRR queue scheduling algorithm and their default weight values are 1:2:3:4:5:9:13:15;
- Query the configuration information.

Configuration procedure:

```
<H3C> system-view
```

```
System View: return to User View with Ctrl+Z.
[H3C] queue-scheduler wrr 2 2 3 3 4 4 5 5
[H3C]display queue-scheduler
 Queue scheduling mode: weighted round robin
 weight of queue 0: 2
 weight of queue 1: 2
 weight of queue 2: 3
 weight of queue 3: 3
 weight of queue 4: 4
 weight of queue 5: 4
 weight of queue 6: 5
 weight of queue 7: 5
[H3C] undo queue-scheduler
[H3C] display queue-scheduler
weight of queue 0: 1
 weight of queue 1: 2
 weight of queue 2: 3
 weight of queue 3: 4
 weight of queue 4: 5
 weight of queue 5: 9
 weight of queue 6: 13
 weight of queue 7: 15
```

1.11 Configuring Congestion Avoidance

When congestion happens, the switch drops packets as soon as possible to release queue resources and try not to put packets into high-delay queues in order to eliminate congestion. The switch adopts the WRED algorithm for congestion avoidance.

1.11.1 Configuration Prerequisites

- The indexes of queues to be dropped at random, the queue length that starts the drop action, and the drop probability are specified
- The ports that need this configuration are specified

1.11.2 Configuration Procedure

Table 1-16 Configure WRED parameters

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Configure WRED parameters	**wred** *queue-index qstart probability*	Required The WRED function is disabled by default

1.11.3 Configuration Example

- Configure WRED parameters for queue 2 on Ethernet 1/0/1. Packets are dropped at random when the queue length is more than 64 packets, and the drop probability is 20%.

Configuration procedure:

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] wred 2 64 20
```

1.12 Configuring Traffic Statistics

Refer to section 1.1.12 "Traffic-based Traffic Statistics" for the introduction to traffic statistics.

1.12.1 Configuration Prerequisites

- ACL rules used for traffic identifying are defined. Refer to the *ACL* module in the manual for defining ACL rules
- The ports that needs this configuration are specified

1.12.2 Configuration Procedure of Traffic Statistics

Table 1-17 Configure traffic statistics

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Use the ACL rules in traffic identifying and perform traffic statistics on the packets matching the ACL rules.	**traffic-statistic inbound** *acl-rule*	Required

Operation	Command	Description
Display the traffic statistics.	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-statistic**	Optional You can execute the **display** command in any view
Display all the QoS settings of the port	**display qos-interface** { *interface-type interface-number* | *unit-id* } **all**	

acl-rule: Applied ACL rules which can be the combination of various ACL rules. The way of combination is described in Table 1-9.

1.12.3 Clearing Traffic Statistics Information

Table 1-18 Clear traffic statistics information

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Clear the statistics of the traffic matching the specified ACL rules	**reset traffic-statistic inbound** *acl-rule*	Required The function of clearing is effective only when the traffic statistics function is configured

acl-rule: Applied ACL rules which can be the combination of various ACL rules. The way of combination is described in Table 1-9.

1.12.4 Configuration Example

- Ethernet1/0/1 of the switch is connected to the 10.1.1.1/24 network segment
- Perform traffic statistics on packets from the 10.1.1.1/24 network segment

Configuration procedure:

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] acl number 2000
[H3C-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[H3C-acl-basic-2000] quit
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] traffic-statistic inbound ip-group 2000
```

1.13 QoS Configuration Example

1.13.1 Configuration Example of TP and Port Rate Limit

I. Network requirement

The enterprise network interconnects all the departments through the ports of the Ethernet switch. The salary query server of the financial department is accessed through Ethernet1/0/1 whose IP address is 129.110.1.2. The network requirements are to limit the average rate of outbound traffic within 640 Kbps and set the precedence of packets exceeding the specification to 4.

II. Network diagram

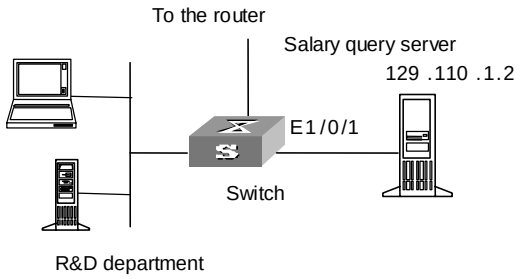


Figure 1-8 QoS configuration example

III. Configuration procedure

Note:

Only the commands related to QoS/ACL configurations are listed in the following configurations.

---

1) Define the outbound traffic of the salary query server

Enter ACL 3000 view.

```
<H3C> system-view
[H3C] acl number 3000
```

Define ACL 3000 rules.

```
[H3C-acl-adv-3000] rule 1 permit ip source 129.110.1.2 0.0.0.0 destination any
[H3C-acl-adv-3000] quit
```

2) Limit the outbound traffic of the salary query server

Limit the average rate of outbound traffic to be within 640 Kbps and set the precedence of packets exceeding the specification to 4.

```
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] traffic-limit inbound ip-group 3000 640 exceed
remark-dscp 4
```

1.13.2 Configuration Example of Priority Remark

I. Network requirements

Mark ef on the packets that PC1 (whose IP address is 1.0.0.1) sends from 8:00 to 18:00 every day to provide the basis of precedence for the upper-layer devices.

II. Network diagram

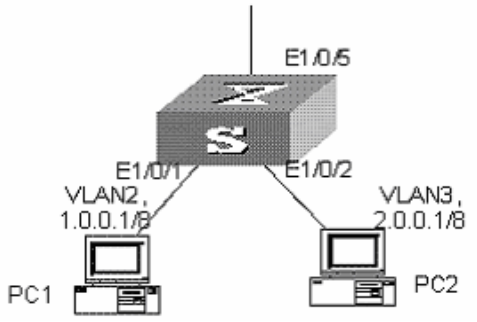


Figure 1-9 QoS configuration example

III. Configuration procedure

1) Define the time rang from 8:00 to 18:00

Define the time rang

```
<H3C> system-view
[H3C] time-range test 8:00 to 18:00 daily
```

2) Define the traffic rules of PC packets

Enter number-identification-based basic ACL view identified.

```
[H3C] acl number 2000
[H3C-acl-basic-2000] rule 0 permit source 1.0.0.1 0 time-range test
[H3C-acl-basic-2000] quit
```

3) Remark ef precedence on the packets that PC1 sends

```
[H3C-Ethernet1/0/1] traffic-priority inbound ip-group 2000 dscp ef
```

Chapter 2 QoS Profile Configuration

2.1 Introduction to QoS Profile

The switch can dynamically provide pre-defined QoS functions for one or one group of authenticated user(s) through the combination of QoS profile function and 802.1x authentication function.

After you have passed the 802.1x authentication, the switch dynamically issues the corresponding profiles to your login port according to the matching relationship between the user name and the profile configured on the AAA server.

Currently, the QoS profile function of the switch can provide packet filter, TP, precedence remark functions and so on.

2.1.1 Application Mode of QoS Profile

After the QoS profile function is configured, the switch will dynamically issue the QoS profiles corresponding to you to your access port if you pass the authentication. The processing procedures of the switch in different application modes are described as follows:

- User-based mode: If the source information (source MAC, source IP, or source MAC + source IP) is defined in the traffic rule adopted by the traffic action of the QoS profile, the QoS profile cannot be issued successfully. If the source information is not defined, the switch will create a new traffic rule by adding your source MAC information into the former rule, and then issue all the traffic actions in the QoS profile to the your access port.
- Port-based mode: The switch will issue all the actions in the QoS profile to your access port.

2.2 Introduction to QoS Profile Configurations

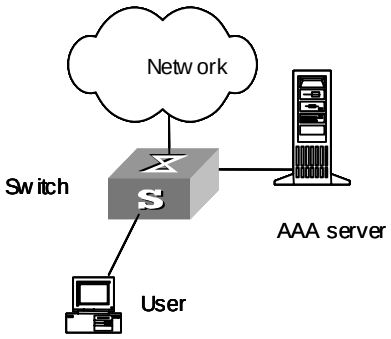


Figure 2-1 Diagram for QoS profile configurations

The following table describes the QoS profile configurations:

Table 2-1 Configure QoS profile

Device	Configuration	Configuration link
AAA server	Configure user authentication information	—
	Configure the matching relationship between the QoS profile and the user name	One QoS profile can match with more than one user.
Switch	Enable the 802.1x authentication function	Refer to *802.1x* module in this manual for the related configuration procedure.
	Configure QoS profile	See section 2.3 "Configuring QoS Profile".
	Apply the QoS profile to a port manually	See section 2.4 "Applying the QoS Profile to the Port Manually".

2.3 Configuring QoS Profile

Refer to section 2.1 "Introduction to QoS Profile" for the introduction to QoS profile.

2.3.1 Configuration Prerequisites

- ACL rules used for traffic identifying are defined. Refer to the *ACL* module in this manual for defining ACL rules
- The global 802.1x authentication function is enabled and 802.1x authentication function is enabled on the user access port
- The type and number of actions in the QoS profile is specified
- The application mode of the QoS profile on the port is specified

2.3.2 Configuration Procedure

Table 2-2 Configure QoS profile

Operation	Command	Description
Enter system view	**system-view**	—
Enter QoS profile view	**qos-profile** *profile-name*	—
Add TP actions	**traffic-limit inbound** *acl-rule target-rate* [**exceed** *action*]	Optional
Add packet filter actions	**packet-filter** { **inbound** | **outbound** } *acl-rule*	Optional

Operation	Command	Description
Add priority remark actions	**traffic-priority** { **inbound** | **outbound** } *acl-rule* { { **dscp** *dscp-value* | **ip-precedence** { *pre-value* | **from-cos** } } | **cos** { *pre-value* | **from-ipprec** } | **local-precedence** *pre-value* }*	Optional
Quit current view	**quit**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the application mode of QoS profile on the current port as port-based	**qos-profile port-based**	By default, the application mode of QoS profile is user-based. • If MAC-address-based authentication is configured in 802.1x, the application mode of QoS profile must be user-based. • If port-based authentication is configured in 802.1x, the application mode of QoS profile must be port-based.
Display the configurations of QoS profiles	**display qos-profile** { **all** | **name** *profile-name* | **interface** *interface-type interface-number* | **user** *user-name* }	Optional You can execute the **display** command in any view

acl-rule: Applied ACL rules which can be the combination of various ACL rules. The way of combination is described in Table 1-9.

Note:

If a QoS profile has been applied on a port, you cannot delete this QoS profile.

2.3.3 Configuration Example

I. Network requirements

The switch implements the QoS profile function for the access users.

The user name is someone and its authentication password is hello. It is connected to Ethernet1/0/1 of the switch and belongs to the test163.net domain. Its corresponding

QoS profile is “example” and the actions of the QoS profile is to limit the bandwidth of the traffic matching ACL rules to 128 k and remark the DSCP precedence to 46.

II. Network diagram

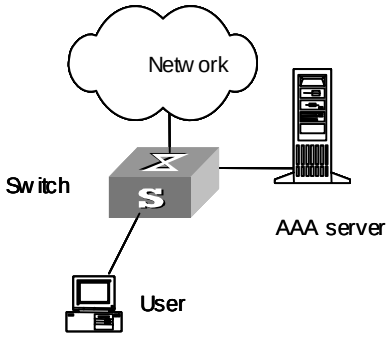


Figure 2-2 QoS configuration example

III. Configuration procedure

(1) Configuration on the AAA server

Configure the user authentication information and the matching relationship between the user name and the QoS profile, which will not be detailed here.

(2) Configuration on the switch

Enable 802.1x.

```
<H3C> system-view
[H3C] dot1x
[H3C] dot1x interface Ethernet 1/0/1
```

Configure the IP address information for the RADIUS server.

```
[H3C] radius scheme radius1
[H3C-radius-radius1] primary authentication 10.11.1.1
[H3C-radius-radius1] primary accounting 10.11.1.2
[H3C-radius-radius1] secondary authentication 10.11.1.2
[H3C-radius-radius1] secondary accounting 10.11.1.1
```

Set the encryption passwords for the switch to exchange packets with the authentication RADIUS servers and accounting RADIUS servers.

```
[H3C-radius-radius1] key authentication name
[H3C-radius-radius1] key accounting money
```

Order the switch to delete the user domain name from the user name and then send the user name to the RADIUS sever.

```
[H3C-radius-radius1] user-name-format without-domain
[H3C-radius-radius1] quit
```

Create the user domain test163.net and specify radius1 as your RADIUS server group.

```
[H3C] domain test163.net
[H3C-isp-test163.net] radius-scheme radius1
[H3C-isp-test163.net] quit
```

Define the ACL rules

```
[H3C] acl number 3000
[H3C-acl-adv-3000] rule 1 permit ip destination any
[H3C-acl-adv-3000] quit
```

Define the QoS profile function

```
[H3C] qos-profile example
[H3C-qos-profile-example] traffic-limit inbound ip-group 3000 128 exceed drop
[H3C-qos-profile-example] traffic-priority inbound ip-group 3000 dscp 46
```

2.4 Applying the QoS Profile to the Port Manually

After this configuration, all the traffic actions in the QoS profile will be applied to the current port.

I. Applying the QoS profile to the port in system view

You can apply the profile configurations to one port or more continuous ports manually in system view.

Table 2-3 Apply the QoS profile to the port manually in system view

Operation	Command	Description
Enter system view	**system-view**	—
Apply the QoS profile to the port manually	**apply qos-profile** *profile-name* **interface** *interface-list*	Required

II. Applying the QoS profile to the current port in Ethernet port view

Table 2-4 Apply the QoS profile to the port manually

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Apply the QoS profile to the current port manually	**apply qos-profile** *profile-name*	Required

2.5 Displaying QoS Profile

After finishing the configurations mentioned above, you can execute the display command in any view to check the running state of the QoS profile. You can verify the configuration by checking the information on display.

Table 2-5 Display the QoS profile

Operation	Command	Description
Display the configurations of the QoS profile	**display qos-profile** { **all** | **name** *profile-name* | **interface** *interface-type interface-number* | **user** *user-name* }	You can execute the **display** command in any view

Table of Contents

Chapter 1 Web Cache Redirection Configuration 1-1
1.1 Overview 1-1
1.2 Web Cache Redirection Configuration 1-2
1.2.1 Configuration Prerequisites 1-2
1.2.2 Configuration Procedure 1-2
1.2.3 Configuration Example 1-3

Chapter 1 Web Cache Redirection Configuration

Note:

The S3600-SI series switches do not support Web cache redirection.

1.1 Overview

Hypertext transfer protocol (HTTP) is one of the most widely used approaches to access the Internet. Ethernet switch provides Web cache redirection function, which helps relieve the pressure on the links connecting to WANs and improve the speed to access the Internet. The following figure shows an implementation of Web cache redirection.

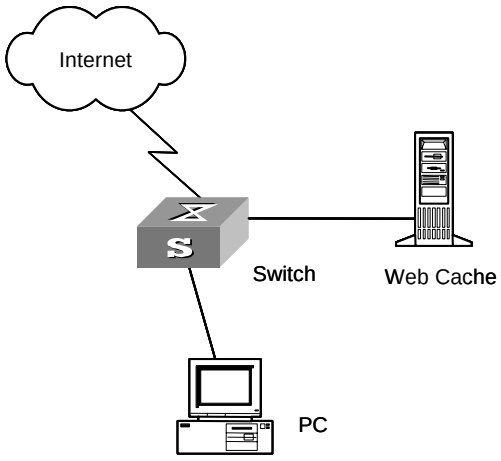


Figure 1-1 Web cache redirection

As shown in the figure, PC is one of the users in the LAN connected to the switch, and Web cache is the server that stores the Internet information often browsed by the users in the LAN. When Web cache redirection is enabled on the switch, the access to the Internet via HTTP is redirected to Web cache. If the desired contents are in the Web cache, the Web cache directly forwards them to users, thus eliminating the access to the Internet. If the cache does not have the information, the users will log onto the Internet to obtain information.

1.2 Web Cache Redirection Configuration

1.2.1 Configuration Prerequisites

- The route between the switch and Web cache is reachable, and the Web cache function is enabled on the Web cache.
- The IP address and MAC address of the Web cache and the VLANs whose HTTP traffic is be redirected to the Web cache are determined.
- The port through which the switch is connected to the Web cache and TCP port number used by HTTP are determined.

1.2.2 Configuration Procedure

Table 1-1 Configure Web cache redirection in system view

Operation	Command	Description
Enter system view	**system-view**	—
Configure Web cache parameters	**webcache address** *ip-address* **mac** *mac-address* **vlan** *vlan-id* **port** *interface-type interface-number* [**tcpport** *tcpport-num*]	Required
Specify a VLAN whose HTTP traffic is to be redirected to the Web cache	**webcache redirect-vlan** *vlan-id*	Required You can specify multiple VLANs for Web cache redirection so that the HTTP traffic of the users in these VLANs can be redirected to the Web cache. By default, HTTP traffic is not redirected to the Web cache.
Display Web cache redirection configuration and the state of the Web cache	**display webcache**	Optional This command can be executed in any view.

Table 1-2 Configure Web cache redirection in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Configure Web cache parameters	**webcache address** *ip-address* **mac** *mac-address* **vlan** *vlan-id* [**tcpport** *tcpport-num*]	Required
Quit to system view	**quit**	—
Specify a VLAN whose HTTP traffic is to be redirected to the Web cache	**webcache redirect-vlan** *vlan-id*	Required You can specify multiple VLANs for Web cache redirection so that the HTTP traffic of the users in these VLANs can be redirected to the Web cache. By default, the HTTP traffic is not redirected to the Web cache.
Display Web cache redirection configuration and the state of the Web cache	**display webcache**	Optional This command can be executed in any view.

Note:

- Web cache redirection configurations made in Ethernet port view and system view come into the same effect.
- If the configured Web cache is inaccessible, Web cache redirection cannot be enabled.
- A switch supports only one Web cache configuration. If you configure a new Web cache, the new configuration will replace the old one.
- If the VLAN where Web cache is located does not have the corresponding VLAN interface on the switch, this configuration will be failed.
- If the VLAN interface is not up, Web cache redirection will be failed.
- You can use the **undo webcache all** command to remove all Web cache redirection configurations.

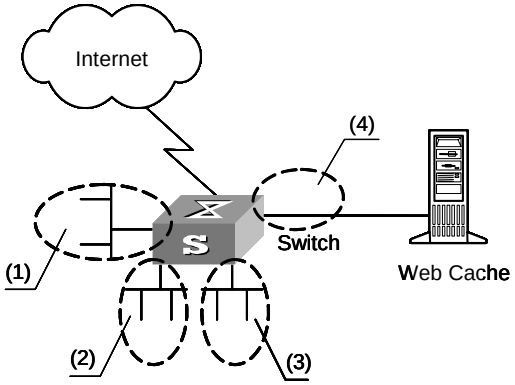
1.2.3 Configuration Example

I. Networking requirements

In a company, the marketing department is located at VLAN10 connected to Ethernet 1/0/1 of the switch, R&D department is located at VLAN20 connected to Ethernet1/0/2, and President's office at VLAN30 connected to Ethernet1/0/3. VLAN10 is in the network segment 10.15.17.1/24, VLAN20 in 10.15.18.1/24, and VLAN30 in

10.15.19.1/24. The IP address of the Web cache is 10.15.20.2, MAC address is 000f-e20f-0101, and the Web cache VLAN is VLAN40. Ethernet3/0/4 of the switch connects to the Web cache. It is required to enable Web cache redirection to redirect the HTTP traffic of R&D department, marketing department, and President's office.

II. Networking diagram



1): VLAN 10, Marketing Dept. 2): VLAN 20, R&D Dept.
3): VLAN 30, President's Office 4): VLAN 40, VLAN where Web cache is located

Figure 1-2 Networking diagram for Web cache redirection configuration

III. Configuration procedure

Configure the VLAN for marketing department on the switch.

```
<H3C> system-view
[H3C] vlan 10
[H3C-vlan10] port Ethernet 1/0/1
[H3C-vlan10] quit
[H3C] interface Vlan-interface 10
[H3C-Vlan-interface10] ip address 10.15.17.1 255.255.255.0
```

Configure the VLAN for R&D department on the switch.

```
[H3C] vlan 20
[H3C-vlan20] port Ethernet 1/0/2
[H3C-vlan20] quit
[H3C] interface Vlan-interface 20
[H3C-Vlan-interface20] ip address 10.15.18.1 255.255.255.0
```

Configure the VLAN for President's office on the switch.

```
[H3C] vlan 30
[H3C-vlan30] port Ethernet 1/0/3
[H3C-vlan30] quit
[H3C] interface Vlan-interface 30
[H3C-Vlan-interface30] ip address 10.15.19.1 255.255.255.0
```

Configure the VLAN where Web cache is located on the switch.

```
[H3C] vlan 40
[H3C-vlan40] port Ethernet 1/0/4
[H3C-vlan40] quit
[H3C] interface Vlan-interface 40
[H3C-Vlan-interface40] ip address 10.15.20.1 255.255.255.0
```

Enable Web cache redirection function on the switch.

```
[H3C] webcache address 10.15.20.2 mac 000f-e20f-0101 vlan 40 port
Ethernet1/0/4
[H3C] webcache redirect-vlan 10
[H3C] webcache redirect-vlan 20
[H3C] webcache redirect-vlan 30
```

Table of Contents

Chapter 1 Mirroring Configuration 1-1
1.1 Mirroring Overview 1-1
1.1.1 Traffic Mirroring 1-1
1.1.2 Port Mirroring 1-1
1.1.3 Remote Port Mirroring — RSPAN 1-1
1.2 Mirroring Functions Supported by S3600 1-4
1.3 Mirroring Configuration for S3600-EI 1-4
1.3.1 Configuring Traffic Mirroring 1-4
1.3.2 Configuring Port Mirroring 1-6
1.3.3 Configuring RSPAN 1-10
1.3.4 Displaying Mirroring Parameter Settings 1-16
1.4 Mirroring Configuration for S3600-SI 1-16
1.4.1 Configuring Traffic Mirroring 1-16
1.4.2 Configuring Port Mirroring 1-16
1.4.3 Displaying Mirroring Parameter Settings 1-17

Chapter 1 Mirroring Configuration

1.1 Mirroring Overview

Mirroring refers to the process of copying packets that meet the specified rules to a destination port. Generally, a destination port is connected to a data detect device, which users can use to analyze the mirrored packets for monitoring and troubleshooting the network.

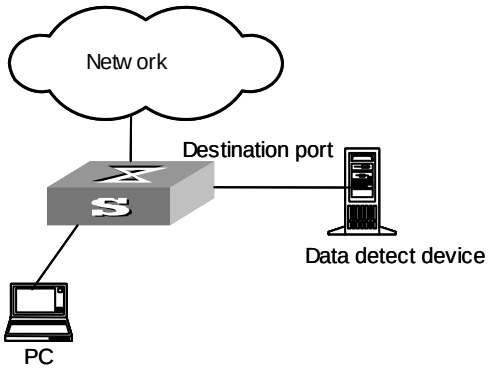


Figure 1-1 Mirroring

1.1.1 Traffic Mirroring

Traffic mirroring refers to the process of copying traffic flows that match specific ACLs to the specified destination port for packet analysis and monitoring. Before configuring traffic mirroring, you need to define ACLs required for flow identification.

1.1.2 Port Mirroring

Port mirroring refers to the process of copying the packets received or sent by the specified port to the destination port.

1.1.3 Remote Port Mirroring — RSPAN

Remote switched port analyzer (RSPAN) refers to remote port mirroring. It eliminates the limitation that the source port and the destination port must be located on the same switch. This feature makes it possible for the source port and the destination port to be located across several devices in the network, and facilitates the network administrator to manage remote switches.

The application of RSPAN is illustrated in the following figure:

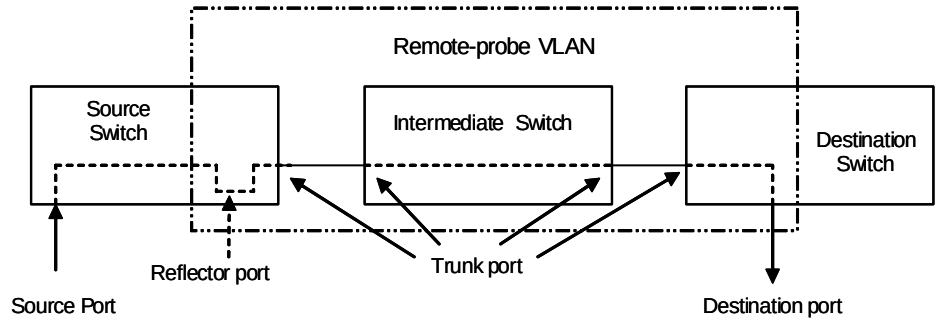


Figure 1-2 RSPAN application

There are three types of switches with the RSPAN enabled.

- Source switch: The monitored port resident switch. Through Layer 2 forwarding, it sends traffics to be mirrored to an intermediate switch or destination switch over the remote-probe VLAN.
- Intermediate switch: Switches between the source switch and destination switch on the network. An intermediate switch forwards mirrored traffic flows to the next intermediate switch or the destination switch. Circumstances can occur where no intermediate switch is present, if a direct connection exists between the source and destination switches.
- Destination switch: The remote mirroring destination port resident switch. It forwards mirrored traffic flows it received from the remote-probe VLAN to the monitoring device through the destination port.

Table 1-1 describes how the ports on various switches are involved in the mirroring operation.

Table 1-1 Ports involved in the mirroring operation

Switch	Ports involved	Function
Source switch	Source port	Port monitored. It copies user data packets to the specified reflector port through local port mirroring. There can be more than one source port.
	Reflector port	Receives user data packets that are mirrored on a local port.
	Trunk port	Sends mirrored packets to the intermediate switch or the destination switch.
Intermediate switch	Trunk port	Sends mirrored packets to the destination switch. Two Trunk ports are necessary for the intermediate switch to connect the devices at the source switch side and the destination switch side.

Switch	Ports involved	Function
Destination switch	Trunk port	Receives remote mirrored packets.
	Destination port	Monitors remote mirrored packets

To implement remote port mirroring, you need to define a special VLAN, called remote-probe VLAN, on a switch. All mirrored packets will be transferred from the source switch to the destination ports of the destination switch through this VLAN. Thus, the destination switch can monitor the port packets sent from the ports of the source switch. Remote-probe VLAN requires that:

- All ports connecting the devices in remote-probe VLAN are configured as the trunk ports.
- The default VLAN and management VLAN cannot be configured as remote-probe VLAN.
- Layer 2 interoperability must be ensured by configuration between the source and destination switches over the remote-probe VLAN.

Caution:

To ensure the normal packet mirroring, it is not recommended to perform any of the following operations on the remote-probe VLAN:

- Configuring a source port to the remote-probe VLAN that is used by the local mirroring group;
- Configuring a Layer 3 interface for the remote-probe VLAN;
- Configuring to run other protocol packets, or bear other service packets;
- Using remote-probe VLAN as a special type of VLAN, such as voice VLAN or protocol VLAN;
- Configuring other VLAN-related functions.

1.2 Mirroring Functions Supported by S3600

Table 1-2 Mirroring functions supported by S3600-EI and related commands

Function	Specifications	Related command	Link
Mirroring	Supports traffic mirroring	**monitor-port** **mirrored-to**	Section 1.3.1
	Supports port mirroring	**mirroring-group** **mirroring-group mirroring-port** **mirroring-group monitor-port** **monitor-port** **mirroring-port**	Section 1.3.2
	Supports remote port mirroring	**mirroring-group** **mirroring-group mirroring-port** **mirroring-group monitor-port** **mirroring-group reflector-port** **mirroring-group remote-probe vlan** **remote-probe vlan enable**	Section 1.3.3

Table 1-3 Mirroring functions supported by S3600-SI and related commands

Function	Specifications	Related command	Link
Mirroring	Supports traffic mirroring	**monitor-port** **mirrored-to**	Section 1.3.1
	Supports port mirroring	**monitor-port** **mirroring-port**	Section 1.4.2

1.3 Mirroring Configuration for S3600-EI

For mirroring features, see section 1.1 "Mirroring Overview".

1.3.1 Configuring Traffic Mirroring

I. Configuration prerequisites

- ACLs for identifying traffics have been defined. For defining ACLs, see the description in the ACL module of this manual.

- The destination port is determined.
- The port to be configured with traffic mirroring function and the direction of the traffic flow to be mirrored are determined.

II. Configuration procedure

Table 1-4 Configure traffic mirroring

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view of the determined destination port	**interface** *interface-type interface-number*	—
Define the current port as the destination port	**monitor-port**	Required LACP and STP must be disabled on the destination port.
Exit current view	**quit**	—
Enter Ethernet port view of traffic mirroring configuration	**interface** *interface-type interface-number*	—
Invoke ACLs for identifying traffic flows and perform traffic mirroring for the packets matching the ACLs.	**mirrored-to** { **inbound** | **outbound** } *acl-rule* { **monitor-interface** | **cpu** }	Required
Display the parameter settings of traffic mirroring	**display qos-interface** { *interface-type interface-number* | *unit-id* } **mirrored-to**	Optional These commands can be executed in any view.
Display all QoS settings of a port	**display qos-interface** { *interface-type interface-number* | *unit-id* } **all**	

acl-rule: applied ACL rules, which can be the combination of different types of ACL sub-rules. The following table describes the combined-ACL applications.

Table 1-5 Combined-ACL applications

Combination mode	Form of acl-rule
Apply all sub-rules in an IP type ACL (either a basic or an advanced ACL) separately	**ip-group** *acl-number*
Apply one sub-rule in an IP type ACL separately	**ip-group** *acl-number* **rule** *rule-id*

Combination mode	Form of acl-rule
Apply all sub-rules in a Layer 2 ACL separately	**link-group** *acl-number*
Apply one sub-rule in a Layer 2 ACL separately	**link-group** *acl-number* **rule** *rule-id*
Apply one sub-rule in a user-defined ACL separately	**user-group** *acl-number*
Apply all sub-rules in a user-defined ACL separately	**user-group** *acl-number* **rule** *rule-id*
Apply one sub-rule in an IP type ACL and one sub-rule in a Layer 2 ACL simultaneously	**ip-group** *acl-number* **rule** *rule-id* **link-group** *acl-number* **rule** *rule-id*

III. Configuration example

Network requirements:

- GigabitEthernet 1/1/1 on the switch is connected to the 10.1.1.1/24 network segment.
- The packets from the 10.1.1.1/24 network segment are to be mirrored to the destination port GigabitEthernet 1/1/4.

Configuration procedure:

```
<H3C> system-view
[H3C] acl number 2000
[H3C-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[H3C-acl-basic-2000] rule deny source any
[H3C-acl-basic-2000] quit
[H3C] interface gigabitEthernet 1/1/4
[H3C-GigabitEthernet1/1/4] monitor-port
[H3C-GigabitEthernet1/1/4] quit
[H3C] interface GigabitEthernet 1/1/1
[H3C-GigabitEthernet1/1/1] mirrored-to inbound ip-group 2000
monitor-interface
```

1.3.2 Configuring Port Mirroring

I. Configuration prerequisites

- The source port is determined and whether the packets to be mirrored are inbound, outbound or both inbound and outbound is specified. **Inbound** means only to mirror the packets received by the port; **outbound** means only to mirror the packets sent by the port; **both** means to mirror the packets received and sent by the port.
- The destination port is determined.

- The mirroring group number is determined.

II. Configuring port mirroring in Ethernet port view

Table 1-6 Configure port mirroring in Ethernet port view (1)

Operation	Command	Description
Enter system view	**system-view**	—
Create a port mirroring group	**mirroring-group** *group-id* **local**	Required
Enter Ethernet port view of the determined destination port	**interface** *interface-type interface-number*	—
Define the current port as the destination port	**monitor-port**	Required LACP and STP must be disabled on the destination port.
Exit current view	**quit**	—
Enter Ethernet port view of the determined source port	**interface** *interface-type interface-number*	—
Define the current port as the source port and specify the direction of the packets to be mirrored	**mirroring-port** { **inbound** | **outbound** | **both** }	Required
Display the mirroring parameter settings	**display mirroring-group** { **all** | **local** }	Optional This command can be executed in any view.

Note:

If you specify the destination port and source port in Ethernet port view without creating a port mirroring group, mirroring group 1 will be created automatically.

Table 1-7 Configure port mirroring in Ethernet port view (2)

Operation	Command	Description
Enter system view	**system-view**	—
Create a port mirroring group	**mirroring-group** *group-id* **local**	Required

Operation	Command	Description
Enter Ethernet port view of the determined destination port	**interface** *interface-type interface-number*	—
Define the current port as the destination port	**mirroring-group** *group-id* **monitor-port**	Required LACP and STP must be disabled on the destination port
Exit current view	**quit**	—
Enter Ethernet port view of the determined source port	**interface** *interface-type interface-number*	—
Define the current port as the source port and specify the direction of the packets to be mirrored	**mirroring-group** *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }	Required
Display the mirroring parameter settings	**display mirroring-group** { **all** | **local** }	Required This command can be executed in any view.

III. Configuring port mirroring in system view

Table 1-8 Configure port mirroring in system view

Operation	Command	Description
Enter system view	**system-view**	—
Create a port mirroring group	**mirroring-group** *group-id* **local**	Required
Define the determined destination port	**mirroring-group** *group-id* **monitor-port** *monitor-port*	Required LACP and STP must be disabled on the destination port.
Define the determined source port and specify the direction of the packets to be mirrored	**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }	Required
Display the mirroring parameter settings	**display mirroring-group** { **all** | **local** }	Optional This command can be executed in any view.

Note:

- Configurations listed in Table 1-6 do not involve specifying a mirroring group. Therefore these mirroring settings made in Ethernet port view applies to mirroring group 1 only.
- Configurations listed in Table 1-7 can be used to add mirroring settings for any defined mirroring group in Ethernet port view.
- Configurations listed in Table 1-8 are performed in system view. Therefore the mirroring group ID and port number must be specified.

IV. Configuration Example

Network requirements:

- The source port is GigabitEthernet 1/1/1. All packets received and sent by this port are to be mirrored.
- The destination port is GigabitEthernet 1/1/4.

Configuration procedure 1:

```
<H3C> system-view
[H3C] mirroring-group 1 local
[H3C] interface gigabitEthernet 1/1/4
[H3C-GigabitEthernet1/1/4] monitor-port
[H3C-GigabitEthernet1/1/4] quit
[H3C] interface gigabitEthernet 1/1/1
[H3C-GigabitEthernet1/1/1] mirroring-port both
```

Configuration procedure 2:

```
<H3C> system-view
[H3C] mirroring-group 1 local
[H3C] interface GigabitEthernet 1/1/4
[H3C-GigabitEthernet1/1/4] mirroring-group 1 monitor-port
[H3C-GigabitEthernet1/1/4] quit
[H3C] interface GigabitEthernet 1/1/1
[H3C-GigabitEthernet1/1/1] mirroring-group 1 mirroring-port both
```

Configuration procedure 3:

```
<H3C> system-view
[H3C] mirroring-group 1 local
[H3C] mirroring-group 1 monitor-port GigabitEthernet 1/1/4
[H3C] mirroring-group 1 mirroring-port GigabitEthernet 1/1/1 both
```

1.3.3 Configuring RSPAN

I. Configuration prerequisites

- The source switch, intermediate switch, and the destination switch are determined.
- The source port, the reflector port, the destination port, and the remote-probe VLAN are determined.
- Layer 2 interoperability is ensured by configuration between the source and destination switches over the remote-probe VLAN
- The direction of the packets to be monitored is determined.
- The remote-probe VLAN is enabled.

II. Configuring RSPAN on the source switch

Table 1-9 Configure RSPAN on the source switch

Operation	Command	Description
Enter system view	**system-view**	—
Create a VLAN and enter the VLAN view	**vlan** *vlan-id*	*vlan-id* is the ID of the remote-probe VLAN to be defined.
Define the current VLAN as the remote-probe VLAN	**remote-probe vlan enable**	Required
Exit the current view	**quit**	—
Enter the port view of the port that connects to the intermediate switch or destination switch	**interface** *interface-type interface-number*	—
Configure the current port as Trunk port	**port link-type trunk**	Required By default, the port type is Access.
Configure Trunk port to permit packets from the remote-probe VLAN	**port trunk permit vlan** *remote-probe-vlan-id*	Required This setting is required for the source switch port that connects to the intermediate switch or destination switch.
Exit current view	**quit**	—
Configure a remote source mirroring group	**mirroring-group** *group-id* **remote-source**	Required
Configure a source port for remote mirroring	**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }	Required

Operation	Command	Description
Configure a remote reflector port	**mirroring-group** *group-id* **reflector-port** *reflector-port*	Required The remote reflector port must be of the Access type. LACP and STP must be disabled on this port. After a port is configured as a reflector port, the switch does not allow you to perform any of the following configurations: • Changing the port type or its default VLAN ID • Add the port to another VLAN
Configure the remote-probe VLAN for the remote source mirroring group	**mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id*	Required
Display the configuration of the remote source mirroring group	**display mirroring-group remote-source**	Optional This command can be executed in any view.

Note:

- The reflector port cannot forward traffics as a normal port. In this scenario, it is recommended that you use an idle and down port as the reflector port, and do not perform other configuration on this port.
- If the **mac-address max-mac-count 0** command is executed on a port in a VLAN, it is recommended not to configure this VLAN as the remote-probe VLAN. Otherwise, remote mirroring may not work properly.
- Do not configure a port connecting the intermediate switch or destination switch as the mirroring source port. Otherwise, traffic disorder may occur in the network.

III. Configuring RSPAN on the intermediate switch

Table 1-10 Configure RSPAN on the intermediate switch

Operation	Command	Description
Enter system view	**system-view**	—
Create a VLAN and enter VLAN view	**vlan** *vlan-id*	v*lan-id* is the ID of the remote-probe VLAN to be defined.

Operation	Command	Description
Define the current VLAN as a remote-probe VLAN	**remote-probe vlan enable**	Required
Exit the current view	**quit**	—
Enter Ethernet port view of the port connecting to the source switch, destination switch or other intermediate switch	**interface** *interface-type interface-number*	—
Configure the current port as Trunk port	**port link-type trunk**	Required By default, the port type is Access.
Configure Trunk port to permit packets from the remote-probe VLAN	**port trunk permit vlan** *remote-probe-vlan-id*	Required This configuration is necessary for ports on the intermediate switch that are connected to the source switch, the destination switch or other intermediate switch.

IV. Configuring RSPAN on the destination switch

Table 1-11 Configure RSPAN on the destination switch

Operation	Command	Description
Enter system view	**system-view**	—
Create a VLAN and enter VLAN view	**vlan** *vlan-id*	v*lan-id* is the ID of the remote-probe VLAN to be defined.
Define the current VLAN as a remote-probe VLAN	**remote-probe vlan enable**	Required
Exit the current view	**quit**	—
Enter Ethernet port view of the port connecting to the source switch or an intermediate switch	**interface** *interface-type interface-number*	—
Configure the current port as Trunk port	**port link-type trunk**	Required By default, the port type is Access.

Operation	Command	Description
Configure Trunk port to permit packets from the remote-probe VLAN	**port trunk permit vlan** *remote*-probe-*vlan-id*	Required This configuration is necessary for ports through which the destination switch is connected to the source switch or an intermediate switch.
Exit the current view	**quit**	—
Configure a remote destination mirroring group	**mirroring-group** *group-id* **remote-destination**	Required
Configure the destination port for remote mirroring	**mirroring-group** *group-id* **monitor-port** *monitor-port*	Required The destination port for remote mirroring must be of the Access type. LACP and STP must be disabled on this port. After you configure a port as the destination port for remote mirroring, the switch does not allow you to change the port type or its default VLAN ID.
Configure the remote-probe VLAN for the remote destination mirroring group	**mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id*	Required
Display the configuration of the remote destination mirroring group	**display mirroring-group remote-destination**	Optional This command can be executed in any view.

Note:

If the **mac-address max-mac-count 0** command is executed on a port in a VLAN, it is recommended not to configure this VLAN as the remote-probe VLAN. Otherwise, remote mirroring may not work properly.

V. Configuration example

Network requirements:

- Switch A is connected to the data detect device through GigabitEthernet 1/1/2.
- GigabitEthernet 1/1/1, the Trunk port of Switch A, is connected to GigabitEthernet 1/1/1, the Trunk port of Switch B.
- GigabitEthernet 1/1/2, the Trunk port of Switch B, is connected to GigabitEthernet 1/1/1, the Trunk port of Switch C.
- GigabitEthernet 1/1/2, the port of Switch C, is connected to PC1.

The purpose is to use the data detect device to monitor and analyze the packets sent by PC1.

To meet the above purpose by using the RSPAN function, perform the following configuration:

- Define VLAN10 as the remote-probe VLAN.
- Define Switch A as the destination switch; configure GigabitEthernet 1/1/2, the port that is connected to the data detect device, as the destination port for remote mirroring. Set GigabitEthernet1/1/2 to an Access port, with STP and LACP functions disabled.
- Define Switch B as the intermediate switch.
- Define Switch C as the source switch, GigabitEthernet 1/1/2 as the source port for remote mirroring, and GigabitEthernet 1/1/3 as the reflector port. Set GigabitEthernet 1/1/3 to an Access port, with STP and LACP disabled.

Network diagram:

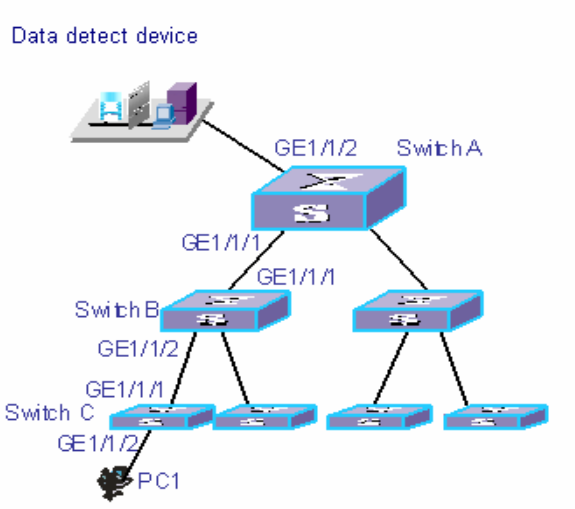


Figure 1-3 Network diagram for RSPAN

Configuration procedure:

Configure Switch C.

```
<H3C> system-view
[H3C] vlan 10
[H3C-vlan10] remote-probe vlan enable
[H3C-vlan10] quit
[H3C] interface GigabitEthernet 1/1/1
[H3C-GigabitEthernet1/1/1] port link-type trunk
[H3C-GigabitEthernet1/1/1] port trunk permit vlan 10
[H3C-GigabitEthernet1/1/1] quit
[H3C] mirroring-group 1 remote-source
[H3C] mirroring-group 1 mirroring-port GigabitEthernet 1/1/2 inbound
```

```
[H3C] mirroring-group 1 reflector-port GigabitEthernet 1/1/3
[H3C] mirroring-group 1 remote-probe vlan 10
[H3C] display mirroring-group remote-source
mirroring-group 1:
    type: remote-source
    status: active
    mirroring port:
        GigabitEthernet1/1/2  outbound
    reflector port: GigabitEthernet1/1/3
    remote-probe vlan: 10
```

Configure Switch B.

```
<H3C> system-view
[H3C] vlan 10
[H3C-vlan10] remote-probe vlan enable
[H3C-vlan10] quit
[H3C] interface GigabitEthernet 1/1/1
[H3C-GigabitEthernet1/1/1] port link-type trunk
[H3C-GigabitEthernet1/1/1] port trunk permit vlan 10
[H3C-GigabitEthernet1/1/1] quit
[H3C] interface GigabitEthernet 1/1/2
[H3C-GigabitEthernet1/1/2] port link-type trunk
[H3C-GigabitEthernet1/1/2] port trunk permit vlan 10
```

Configure Switch A.

```
<H3C> system-view
[H3C] vlan 10
[H3C-vlan10] remote-probe vlan enable
[H3C-vlan10] quit
[H3C] interface GigabitEthernet 1/1/1
[H3C-GigabitEthernet1/1/1] port link-type trunk
[H3C-GigabitEthernet1/1/1] port trunk permit vlan 10
[H3C-GigabitEthernet1/1/1] quit
[H3C] mirroring-group 1 remote-destination
[H3C] mirroring-group 1 monitor-port GigabitEthernet 1/1/2
[H3C] mirroring-group 1 remote-probe vlan 10
[H3C] display mirroring-group remote-destination
mirroring-group 1:
    type: remote-destination
    status: active
    monitor port: GigabitEthernet1/1/2
    remote-probe vlan: 10
```

1.3.4 Displaying Mirroring Parameter Settings

After the above configuration, you can use the **display** command in any view to view the mirroring running information, so as to verify the configurations you made.

Table 1-12 Display mirroring parameter settings

Operation	Command	Description
Display parameter settings of a mirroring group	**display mirroring-group** { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }	The command can be executed in any view.
Display parameter settings of traffic mirroring	**display qos-interface** { *interface-type interface-number* | *unit-id* } **mirrored-to**	

1.4 Mirroring Configuration for S3600-SI

For mirroring features, refer to section 1.1 "Mirroring Overview".

1.4.1 Configuring Traffic Mirroring

The traffic mirroring configurations for S3600-SI are the same as those for S3600-EI. Refer to section 1.3.1 “Configuring Traffic Mirroring” for details.

1.4.2 Configuring Port Mirroring

I. Configuration prerequisites

- The source port is determined and whether the packets to be mirrored are inbound, outbound or both inbound and outbound is specified. Inbound means only to mirror the packets received by the port; outbound means only to mirror the packets sent by the port; both means to mirror the packets received and sent by the port.
- The destination port is determined.

II. Configuration procedure

Table 1-13 Configure port mirroring

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view of the determined destination port	**interface** *interface-type interface-number*	—
Define the current port as the destination port	**monitor-port**	Required LACP and STP must be disabled on the destination port.

Operation	Command	Description
Exit the current view	**quit**	—
Enter Ethernet port view of the determined source port	**interface** *interface-type interface-number*	—
Define the current port as the source port and specify the direction of the packets to be mirrored	**mirroring-port** { **inbound** | **outbound** | **both** }	Required
Display parameter settings of the mirroring	**display mirror**	Optional This command can be executed in any view.

III. Configuration Example

- The source port is GigabitEthernet 1/1/1. Mirror all packets received and sent by this port.
- The destination port is GigabitEthernet 1/1/4.

Configuration procedure:

```
<H3C> system-view
[H3C] interface gigabitEthernet 1/1/4
[H3C-GigabitEthernet1/1/4] monitor-port
[H3C-GigabitEthernet1/1/4] quit
[H3C] interface gigabitEthernet 1/1/1
[H3C-GigabitEthernet1/1/1] mirroring-port both
```

1.4.3 Displaying Mirroring Parameter Settings

After the above configuration, you can use the **display** command in any view to view the mirroring running information, so as to verify the configurations you made..

Table 1-14 Display mirroring parameter settings

Operation	Command	Description
Display parameter settings of a mirroring group	**display mirror**	This command can be executed in any view.
Display parameter settings of traffic mirroring	**display qos-interface** { *interface-type interface-number* | *unit-id* } **mirrored-to**	

Table of Contents

Chapter 1 IRF Fabric Configuration 1-1
1.1 Overview 1-1
1.1.1 Introduction to IRF 1-1
1.1.2 Introduction to RMON on IRF 1-2
1.2 Peer Fabric Port Detection 1-2
1.2.1 Introduction to the Peer Fabric Port Detection Function 1-2
1.2.2 Work Flow of the Peer Fabric Port Detection Function 1-2
1.2.3 Prompt Information and Solution 1-3
1.3 IRF Fabric Configuration 1-5
1.3.1 Introduction to IRF Fabric Configuration 1-5
1.3.2 Specifying the VLAN Used to Form an IRF Fabric 1-6
1.3.3 Setting a Unit ID for a Switch 1-6
1.3.4 Specifying the Fabric Port of a Switch 1-8
1.3.5 Assigning a Unit Name to a Switch 1-9
1.3.6 Assigning an IRF Fabric Name to a Switch 1-9
1.3.7 Setting the IRF Fabric Authentication Mode 1-10
1.4 Displaying and Debugging IRF Fabric 1-10
1.5 IRF Fabric Configuration Example 1-11
1.5.1 Network Requirements 1-11
1.5.2 Network Diagram 1-11
1.5.3 Configuration Procedure 1-11

Chapter 1 IRF Fabric Configuration

1.1 Overview

1.1.1 Introduction to IRF

Several IRF (intelligent resilient framework) supported switches of the same model can be interconnected to form a fabric, in which each switch is a unit. The ports used to interconnect all the units are called fabric ports, and the other ports that are used to connect the fabric to users are called user ports. In this way, you can increase ports and switching capability by adding devices to the fabric. In addition, reliability of the system will be improved because the devices within the fabric can backup each other. This feature brings you many advantages:

- Realizes unified management of multiple devices. Only one connection and one IP address are required to manage the entire fabric. Therefore, management cost is reduced.
- Enables you to purchase devices on demand and expand network capacity smoothly. Protects your investment to the full extent during network upgrade.
- Ensures high reliability by N+1 redundancy, avoids single point failure, and lessens service interruption.

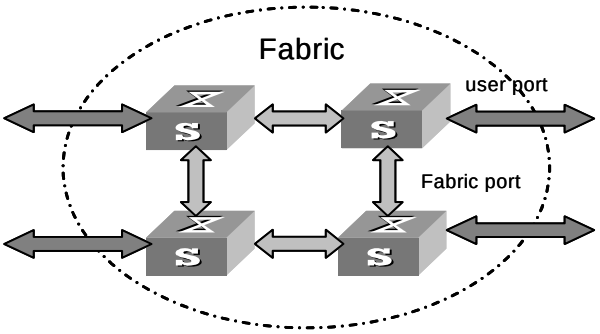


Figure 1-1 Fabric

You can manage and maintain fabric topology with the Fabric Topology Management (FTM) function. FTM on each unit exchanges information with other units, including unit ID, fabric name, and the authentication mode between units, by using a special kind of protocol packets. It manages and maintains fabric topology according to the acquired information. For example, when a new device is connected to a fabric, FTM will determine whether it should establish a new fabric with the device according to the obtained information.

Note:

- The S3600-SI series switches only support basic IRF fabric feature, that is, DDM (distributed device management) function.
- The S3600-EI series switches support enhanced IRF fabric feature, including DDM, DRR (distributed resilient routing) and DLA (distributed link aggregation).

1.1.2 Introduction to RMON on IRF

The RMON configurations of the devices in a fabric are the same. The RMON configuration performed on a device of a fabric will be automatically synchronized to all devices in the fabric if the configuration does not conflict with that of other devices in the fabric.

If you configure the same entry in the same RMON group for devices of a fabric to be different values, the value of the RMON group entry will be the one configured by the device with the smallest Unit ID when the devices are synchronized. Such a mechanism eliminates configuration conflicts between the devices in a fabric.

After the configurations are consistent, you can collect RMON history and statistics of any unit from any switch in the fabric.

1.2 Peer Fabric Port Detection

1.2.1 Introduction to the Peer Fabric Port Detection Function

As the basis of the IRF function, the fabric topology management (FTM) module manages and maintains the entire topology of a fabric. The FTM module also implements the peer fabric port detection function.

A device can join a fabric only when the following conditions are met.

- The number of the existing devices in the fabric does not reach the maximum number of devices allowed by the fabric.
- The fabric names of the device and the existing devices in the fabric are the same.
- The software version of the device is the same as that of the existing devices in the fabric.
- The device passes the security authentication if security authentication is enabled in the fabric.

1.2.2 Work Flow of the Peer Fabric Port Detection Function

After a switch is powered on, the FTM module releases device information of the switch through the fabric ports. The device information includes Unit ID, CPU MAC, device type ID, fabric port information, and all fabric configuration information. The device

information is released in the form of discovery packet (DISC). A new device can join a fabric only when its DISC packets pass the authentication performed by the existing devices in the fabric.

- If a fabric port of a switch is connected to a non-fabric port, the switch will not receive DISC packets from the peer. In this case, the switch cannot join the fabric.
- If the switch can receive DISC packets sent by the peer, the FTM module determines whether peer sending ports correspond to local receiving ports according to information in the packet. That is, if a DISC packet received by the left port of the switch is sent by the right port of the peer device, the packet is regarded legal. Otherwise, the packet is regarded illegal and is discarded.
- If the maximum number of devices allowed by the fabric is reached, the devices in the fabric do not send DISC packets and discard the received DISC packets. This prevents new devices from joining the fabric.
- After receiving a DISC packet from a directly connected device, a device in a fabric checks whether the device information (that is, the Fabric name and software version) contained in the packet and that of its own are the same. If not, the received DISC packet is illegal and will be discarded.
- If authentication is enabled in the fabric, the current device in the fabric authenticates received packets sent by new directly connected devices. Packets that fail to pass the authentication will be discarded.

1.2.3 Prompt Information and Solution

I. Normal

If the port displays “normal”, it indicates the fabric operates properly.

II. Temporary

If the port displays “temporary”, it indicates the port status is changing.

III. Redundance port

If the port displays “redundance port”, it indicates the port is the redundant port in a fabric ring topology.

Note:

The “normal”, “temporary” and “redundance port” information does not mean a device or a fabric operates improperly. No measure is needed for any of these three types of information.

IV. Connection error

Analysis: The port matching errors (as listed in Table 1-1) may occur if a switch prompts the “connection error” message.

Solution: Take the measures listed in Table 1-1 accordingly.

Table 1-1 Connection error type and solution

Error type	Solution
Two fabric ports of the same device (that is, the right port and the left port) are connected.	Pull out one end of the cable and connect it to a fabric port of another switch.
The left and right fabric ports of two devices are not connected in a crossed way.	Connect the left and right ports of two devices in a crossed way.
A fabric port of the local switch is connected to a non-fabric port, or is connected to a fabric port that does not have fabric port function enabled.	Check the types of the two interconnected ports on two sides. Make sure a fabric port is only connected to ports of the same type and the fabric ports on both sides are enabled with the fabric port function.

V. Reached max units

Analysis: The “reached max units” message indicates that the maximum number of units allowed by the current fabric is reached. You will fail to add new devices to the fabric in this case.

Solution: Remove the new device or existing devices in the fabric.

Note:

Up to eight devices can be in an IRF fabric at a time.

VI. Different system name

Analysis: The “different system name” message indicates the fabric name of the device directly connected to the switch and the existing fabric name of the fabric are not the same. Only the devices with the same fabric name can form a Fabric.

Solution: Configure the fabric name of the new device to be that of the fabric.

VII. Different product version

Analysis: The “different product version” message indicates the software version of the directly connected device and that of the current device are not the same. A device can join a fabric only when its software version is identical to that of the fabric.

Solution: Make sure the software version of the new device is the same as that of the fabric.

VIII. Auth failure

Analysis: The “auth failure” message indicates error occurs when the switch authenticates a directly connected device. The error may occur if the IRF fabric authentication modes configured for both devices are not the same, or the password configured does not match.

Solution: Make sure the IRF fabric authentication modes and the passwords configured for both devices are the same.

1.3 IRF Fabric Configuration

1.3.1 Introduction to IRF Fabric Configuration

FTM provides user interfaces. You can configure VLAN, unit IDs, fabric name, and the authentication mode between units by using a related command.

Table 1-2 Configure an IRF Fabric

Task	Description	Related section
Specify the VALN used to form the IRF fabric	Required	Section 1.3.2 “Specifying the VLAN Used to Form an IRF Fabric”
Set and save the unit ID for a switch	Optional	Section 1.3.3 “Setting a Unit ID for a Switch”
Specify the fabric ports for a switch	Required	Section 1.3.4 “Specifying the Fabric Port of a Switch”
Set the unit name for a switch	Optional	Section 1.3.5 “Assigning a Unit Name to a Switch”
Set a name for the IRF fabric	Required	Section 1.3.6 “Assigning an IRF Fabric Name to a Switch”
Set the authentication mode for the IRF fabric	Optional	Section 1.3.7 “Setting the IRF Fabric Authentication Mode”

1.3.2 Specifying the VLAN Used to Form an IRF Fabric

Table 1-3 Specify the VLAN used to form an IRF fabric

Operation	Command	Description
Enter system view	**system-view**	—
Specify the VLAN used to form the IRF fabric	**ftm fabric-vlan** *vlan-id*	Required By default, the VLAN used to form the IRF fabric is VLAN 4093

Caution:

You cannot specify an existing VLAN to form an IRF fabric; otherwise, your configuration fails.

1.3.3 Setting a Unit ID for a Switch

On the switches that support automatic numbering, FTM will automatically number the switches to constitute an IRF fabric, so that each switch has a unique unit ID in the fabric. You can use the command in the following table to set unit IDs for switches. Make sure to set different unit IDs for different switches in an IRF fabric. Otherwise, FTM will automatically number the switches with the same unit ID.

Table 1-4 Set a unit ID for a switch

Operation	Command	Description
Enter system view	**System-view**	—
Set a unit ID for the switch	**change self-unit to** { *unit-id* | **auto-numbering** }	Optional By default, the unit ID of a switch that belongs to no IRF fabric is 1. The unit ID of a switch belonging to an IRF fabric is assigned by FTM. Unit ID ranges from 1 to 8.

Note:

If you do not enable the fabric port, you cannot change the unit ID of the local switch.

After an IRF fabric is established, you can use the following command to change the unit IDs of the switches in the IRF fabric.

Table 1-5 Set a unit ID to a new value

Operation	Command	Description
Enter system view	**system-view**	—
Set a unit ID to a new value	**change unit-id** *unit-id1* **to** { *unit-id2* | **auto-numbering** }	Optional

Note:

- Unit IDs in an IRF fabric are not always arranged in order of 1 to 8.
- Unit IDs of an IRF fabric can be inconsecutive.

After you change the unit ID of switches, the following operations are performed.

- If the modified unit ID does not exist in the IRF fabric, the system sets its priority to 5 and saves it in the unit Flash memory.
- If the modified unit ID is an existing one, the system prompt you to confirm if you really want to change the unit ID. If you choose to change, the existing unit ID is replaced and the priority is set to 5. Then you can use the **fabric save-unit-id** command to save the modified unit ID into the unit Flash memory and clear the information about the existing one.
- If **auto-numbering** is selected, the system sets the unit priority to 10. You can use the **fabric save-unit-id** command to save the modified unit ID into the unit Flash memory and clear the information about the existing one.

Note:

Priority is the reference for FTM module to perform automatic numbering. The value of priority can be 5 or 10. A smaller value represents a higher priority. Priority 5 means the switch adopts manual numbering, and priority 10 means the switch adopts automatic numbering.

After the configuration of numbering, you can use the following command in the table to save the local unit ID in the unit Flash memory. When you restart the switch, it can load the unit ID configuration automatically.

Table 1-6 Save the unit ID of each unit in the IRF fabric

Operation	Command	Description
Save the unit ID of each unit in the IRF fabric	**fabric save-unit-id**	Optional

1.3.4 Specifying the Fabric Port of a Switch

The fabric port of an S3600 series Ethernet switch has the following features:

- An S3600 series Ethernet switch has four GigabitEthernet ports that can be used as fabric ports. The four ports fall into two groups according to the port number. GigabitEthernet1/1/1 and GigabitEthernet1/1/2 form the first group, and GigabitEthernet1/1/3 and GigabitEhternet1/1/4 form the second group.
- Only one group of ports can be the fabric ports at a time. GigabitEthernet1/1/1 and GigabitEthernet1/1/3 are the UP standby fabric port of their respective group. GigabitEthernet1/1/2 and GigabitEthernet1/1/4 are the DOWN standby fabric port of their respective group.
- The system has no restriction on the fabric port group. That is, if the local end uses the fabric port in the first group, it can connect to the fabric port in either the first or the second group of the peer end. As long as meeting the conditions introduced in section 1.2.1 , the switches can establish an IRF fabric connection successfully.

You can use the **fabric port** command to enable a fabric port. At the same time, the group where this fabric port resides becomes the fabric port group, and the other port in the group will be automatically enabled with fabric port feature. For example, after the **fabric port GigabitEthernet1/1/1 enable** command is executed, port GigabitEthernet1/1/1 becomes the UP fabric port. At the same time, the first group becomes the fabric port group, and the other port GigabitEthernet1/1/2 in the first group becomes DOWN fabric port automatically.

You can specify a port as a fabric port by executing the command in Table 1-7.

Table 1-7 Specify a fabric port

Operation	Command	Description
Enter system view	**system-view**	—
Specify the fabric port of a switch	**fabric-port** *interface-type interface-number* **enable**	Optional

Note:

- Establishing an IRF system requires a high consistency of the configuration of each device. Hence, before you enable the fabric port, do not perform any configuration for the port, and do not enable some functions that affect the IRF (such as TACACAS and VLAN-VPN) for other ports or globally. Otherwise, you cannot enable the fabric port. For detailed restrictions refer to the error information output by devices.
- When you have enabled fabric port function for a fabric port group, if you need to change the fabric port group, you must disable the fabric function of the current fabric port group before you execute the enable command on another group. Otherwise, the system will prompt that the current fabric port group is in use, you cannot change the fabric port group.
- As shutting down a fabric port directly may cause the fabric being removed and error messages, do not perform such operations.
- To remove a fabric, you can simply remove the cables used to form the fabric or disable fabric using the **undo fabric-port enable** command.
- You can shut down/bring up a port after you disable the fabric feature on the port.

1.3.5 Assigning a Unit Name to a Switch

You can assign a unit name to a switch by performing the operations listed in Table 1-8.

Table 1-8 Assign a unit name to a switch

Operation	Command	Description
Enter system view	**System-view**	—
Assign a unit name to a switch	**set unit** *unit-id* **name** *unit-name*	Required

1.3.6 Assigning an IRF Fabric Name to a Switch

Only the switches with the same IRF fabric name can form an IRF fabric.

Table 1-9 Assign a fabric name to a switch

Operation	Command	Description
Enter system view	**System-view**	—
Assign a fabric name to the switch	**sysname** *sysname*	Optional By default, the IRF fabric name is H3C.

1.3.7 Setting the IRF Fabric Authentication Mode

Only the switches with the same IRF fabric authentication mode can form an IRF fabric.

Table 1-10 Set the IRF fabric authentication mode for a switch

Operation	Command	Description
Enter system view	**System-view**	—
Set the IRF fabric authentication mode for the switch	**irf-fabric authentication-mode** { **simple** *password* | **md5** *key* }	Optional By default, no authentication mode is set on a switch.

Note:

When an IRF fabric operates normally, you can regard the whole fabric as a single device and perform configuration on it. Multiple switches constitute an IRF fabric. Therefore, data transmission and simultaneous program execution among the switches may cause the IRF fabric in a busy situation. When you configure the IRF fabric, you may receive a prompt “Fabric system is busy, please try later…” which indicates the fabric system does not perform your configuration properly. In this case, you need to verify your previous configuration or perform your configuration again.

1.4 Displaying and Debugging IRF Fabric

Following completion of the above configuration, you can execute the **display** command in any view to view device management and verify the settings. And you can execute the **reset** command to clear the FTM statistics.

Table 1-11 Display and debug FTM

Operation	Command	Description
Display the information about an IRF fabric	**display irf-fabric** [**port** | **status**]	These commands can be executed in any view.
Display the topology information of an IRF fabric	**display ftm** { **information** | **topology-database** }	
Display RMON statistics of a specified unit in an IRF fabric	**display rmon statistics unit** *unit-id*	
Display RMON history data of a specified unit in an IRF fabric	**display rmon history unit** *unit-id*	

Operation	Command	Description
Clear the FTM statistics	**reset ftm statistics**	Execute this command in user view

1.5 IRF Fabric Configuration Example

1.5.1 Network Requirements

Configure unit ID, unit name, IRF fabric name, and authentication mode for four switches to enable them to form an IRF fabric.

The configuration details are as follows:

- Unit IDs: 1, 2, 3, 4
- Unit names: unit 1, unit 2, unit 3, unit 4
- Fabric name: hello
- Authentication mode: simple password
- Password: welcome

1.5.2 Network Diagram

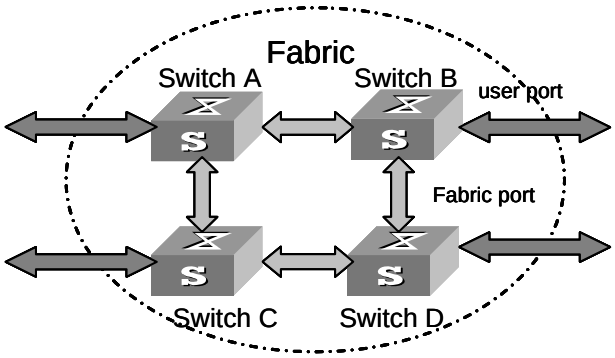


Figure 1-2 Network diagram for forming an IRF fabric

1.5.3 Configuration Procedure

1) Configure Switch A.

Configure the unit ID as 1.

```
<H3C> system-view
[H3C] change unit-id 1 to 1
```

Configure the unit name as unit 1.

```
[H3C] set unit 1 name unit1
```

Configure the fabric name as hello.

```
[H3C] sysname hello
```

Configure the authentication mode as simple password and the password as welcome.

```
[hello] irf-fabric authentication-mode simple welcome
```

2) Configure Switch B.

Configure the unit ID as 2.

```
<H3C> system-view
[H3C] change unit-id 1 to 2
```

Configure the unit name as unit 2.

```
[H3C] set unit 1 name unit2
```

Configure the fabric name as hello.

```
[H3C] sysname hello
```

Configure the authentication mode as simple password and the password as welcome.

```
[hello] irf-fabric authentication-mode simple welcome
```

Configurations on Switch C and Switch D are similar with the above configurations.

Table of Contents

Chapter 1 Cluster 1-1
1.1 Cluster Overview 1-1
1.1.1 Introduction to HGMP V2 1-1
1.1.2 Introduction to NDP 1-2
1.1.3 Introduction to NTDP 1-3
1.1.4 Introduction to Cluster 1-3
1.1.5 Switch Roles for a Cluster 1-5
1.2 Cluster Configuration on Management Device 1-7
1.2.1 Management Device Cluster Configuration Tasks 1-7
1.2.2 Enabling NDP Globally and on Specific Ports 1-8
1.2.3 Configuring NDP-Related Parameters 1-8
1.2.4 Enabling NTDP Globally and on a Specific Port 1-8
1.2.5 Configuring NTDP-Related Parameters 1-9
1.2.6 Enabling the Cluster Function 1-9
1.2.7 Configuring Cluster Parameters 1-10
1.2.8 Configuring Interaction for the Cluster 1-11
1.2.9 Configuring NM Interface for the Cluster 1-12
1.3 Cluster Configuration on Member Device 1-12
1.3.1 Member Device Cluster Configuration Tasks 1-12
1.3.2 Enabling NDP Globally and on Specific Ports 1-13
1.3.3 Enabling NTDP Globally and on a Specific Port 1-14
1.3.4 Enabling the Cluster Function 1-14
1.3.5 Accessing Shared FTP/TFTP Server from a Member Device 1-14
1.4 Cluster Member Configuration 1-15
1.5 Displaying and Maintaining Cluster Configuration 1-15
1.6 Cluster Configuration Example 1-16
1.6.1 Basic Cluster Configuration Example 1-16
1.6.2 NM Interface Configuration Example 1-20

Chapter 1 Cluster

1.1 Cluster Overview

1.1.1 Introduction to HGMP V2

The cluster function is implemented through Huawei group management protocol version 2 (HGMP V2). With HGMP V2, a network administrator can manage multiple switches through the public IP address of a switch known as a management device. The managed switches under the management device are called member devices. The management device and the member devices together compose a cluster. Normally, member devices do not have public IP addresses, but you can manage and maintain them through the management device, which can redirect your management and maintenance operations to their intended destinations. Figure 1-1 illustrates a typical cluster application.

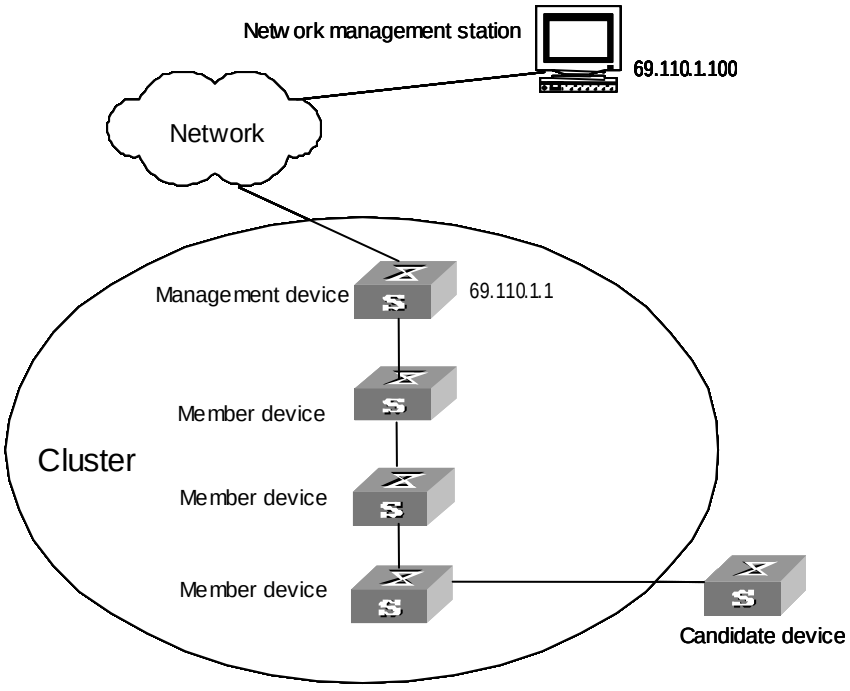


Figure 1-1 Cluster illustration

HGMP V2 has the following advantages:

- It eases the configuration and management of multiple switches: You just need to configure a public IP address for the management device instead of for all the devices in the cluster; and then you can configure and manage all the member

devices through the management device without the need to log onto them one by one.

- It provides the topology discovery and display function, which assists in monitoring and maintaining the network.
- It allows you to configure and upgrade multiple switches at the same time.
- It enables you to manage your remotely devices conveniently regardless of network topology and physical distance.
- It saves IP address resource.

HGMP V2 comprises the following three protocols:

- Neighbor discovery protocol (NDP): This protocol is able to discover directly connected neighbor devices and provide information about those devices, including device type, software/hardware version, connecting port, and some other information such as device ID, port full/half duplex mode, product version, and Boot ROM version.
- Neighbor topology discovery protocol (NTDP): This protocol is able to discover network topology and provide network topology information. It collects device and device connection information in your network and allows you to adjust the range of topology discovery.
- Cluster management protocol: This protocol provides the member recognition and member management functions. It works in conjunction with the network management software to implement large-scale network management. Member recognition means that the management device locates and recognizes each member in the cluster so that it can redirects configuration and management commands to the its members. Member management means that the management device manages such events as adding a member and removing a member, and such cluster parameter settings as handshake interval, cluster management VLAN and shared FTP server settings.

Cluster-related configurations will be described in later sections.

1.1.2 Introduction to NDP

NDP is a protocol used to discover adjacent nodes and provide information about them. NDP operates at the data link layer, and therefore it supports different network layer protocols.

NDP is able to discover directly connected neighbors and provide the following neighbor information: device type, software/hardware version, and connecting port. In addition, it may provide the following neighbor information: device ID, port full/half duplex mode, product version, Boot ROM version and so on.

An NDP-enabled device maintains an NDP neighbor table. Each entry in the NDP table can automatically ages out. You can also clear the current NDP information manually to have neighbor information collected again.

An NDP-enabled device regularly broadcasts NDP packet through all its active ports. An NDP packet carries a holdtime field, which indicates how long the receiving devices will keep the NDP packet data. The receiving devices store the information carried in the NDP packet into the NDP table but do not forward the NDP packet. When they receive another NDP packet, if the information carried in the packet is different from the stored one, the corresponding entry in the NDP table is updated, otherwise only the holdtime of the entry is updated.

1.1.3 Introduction to NTDP

NTDP is a protocol used to collect network topology information. NTDP provides information required for cluster management: it collects topology information about the switches within the specified hop count, so as to provide the information of which devices can be added to a cluster.

Based on the neighbor information stored in the neighbor table maintained by NDP, NTDP on the management device advertises NTDP topology collection requests to collect the NDP information of each device in a specific network range as well as the connection information of all its neighbors. The information collected will be used by the management device or the network management software to implement required functions.

When a member device finds any change on its neighbors through its NDP table, it informs the management device through handshake packets, and the management device triggers its NTDP to perform specific topology collection, so that its NTDP can discover topology changes in real time.

Note:

To implement NTDP, you need to enable NTDP globally and on specific ports on both management device and member/candidate devices, and configure NTDP parameters on only management device. You need not configure NTDP parameters on member/candidate devices because they adopt NTDP parameter settings delivered from the management device when NTDP is running.

1.1.4 Introduction to Cluster

A cluster must have one and only one management device. Note the following when creating a cluster:

- You need to designate a management device for the cluster. The management device of a cluster is the portal of the cluster. That is, any operations from outside the network intended for the member devices of the cluster, such as accessing,

configuring, managing, and monitoring, can only be implemented through the management device.

- The management device of the cluster recognizes and controls all the member devices in the cluster, no matter where they are located in the network and how they are connected.
- The management device collects topology information about all member/candidate devices to provide useful information for you to establish the cluster.
- By collecting NDP/NTDP information, the management device learns network topology, so as to manage and monitor network devices.
- Before performing any cluster-related configuration task, you must first enable the cluster function.

Note:

On the management device, you need to enable the cluster function and configure cluster parameters. On the member/candidate devices, however, you only need to enable the cluster function so that they can be managed by the management device.

Additionally, on the management device, you can configure the FTP server, TFTP server, logging host and SNMP host to be shared by the whole cluster. When a member device in the cluster communicates with an external server, the member device first transmits data to the management device, which then forwards the data to the external server. The management device is the default shared FTP/TFTP server for the cluster; it serves as the shared FTP/TFTP server when no shared FTP/TFTP server is configured for the cluster.

The most important function of clusters is to work in conjunction with the network management software to implement large-scale network management. You can specify a network management interface on the management device of a cluster, through which the network administrator can log onto the management device to manage the devices in the cluster.

Note:

- By default, the management VLAN interface is used as the network management interface.
- There is only one network management interface on a management device; any newly configured network management interface will overwrite the old one.

1.1.5 Switch Roles for a Cluster

From the point of view of a cluster, switches may play different roles, which depend on their functionality and status. You can specify the role of a switch, or change the role of a switch following some specific rules.

For a cluster, a switch may play one of the three roles: management device, member device, and candidate device.

Table 1-1 Switch roles for a cluster

Role	Configuration	Functionality
Management device	• The management device is configured with a public IP address. • You can issue management commands to the management device across the Internet, and the management device will further process your commands.	• The management device provides a management interface to all switches in the cluster. • It manages member devices by redirecting commands. That is, it forwards commands to their intended member devices for processing. • It has the following functions: neighbor discovery, topology collection, cluster management and cluster status maintenance, and supports FTP Server and SNMP proxies.
Member device	Normally, a member device is not configured with a public IP address.	• A member device acts as a member in the cluster. • It has the following functions: neighbor discovery, accepting the management of the management device, running commands forwarded by proxies and reporting failures/logs
Candidate device	Normally, a candidate device is not configured with a public IP address.	A candidate device is a switch that does not belong to any cluster; it has cluster capability and can be added to a cluster.

A switch can change from one role to another according to the following rules:

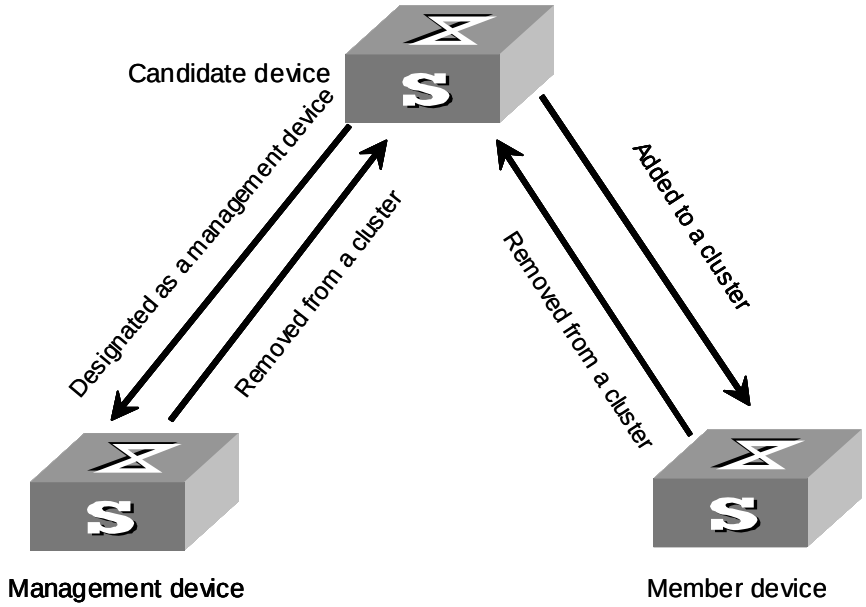


Figure 1-2 Role switching rules

- A candidate device becomes a management device after you designate it as the management device of a cluster (you can do this by building a cluster on the device). Each cluster must have one and only one management device. After you specify the management device of a cluster, the management device discovers and determines candidate devices (by collecting NDP/NTDP information), which you can then add into the cluster through manual configuration.
- A candidate device becomes a member device after being added to a cluster.
- A member device becomes a candidate device after being removed from the cluster.
- The management device becomes a candidate device only after you remove the cluster.

Note:

After a cluster is set up on an S3600 series switch, the switch will collect the topology information of the network at the topology collection interval you set and automatically add the candidate devices it discovers into the cluster. As a result, if the topology collection interval is too short (the default interval is 1 minute), the switches acting as candidate devices will not keep in candidate state for a long time – they will change to member devices within a short time. If you do not want the candidate switches to be automatically added into the cluster, you can set the topology collection interval to 0 (by using the **ntdp timer** command), which specifies not to perform topology collection periodically.

1.2 Cluster Configuration on Management Device

1.2.1 Management Device Cluster Configuration Tasks

Table 1-2 Management device cluster configuration tasks

Operation	Description	Related section
Enable NDP globally and on specific ports	Required	Section 1.2.2 “Enabling NDP Globally and on Specific Ports”
Configure NDP-related parameters	Required	Section 1.2.3 “Configuring NDP-Related Parameters”
Enable NTDP globally and on a specific port	Required	Section 1.2.4 “Enabling NTDP Globally and on a Specific Port”
Configure NTDP-related parameters	Required	Section 1.2.5 “Configuring NTDP-Related Parameters”
Enable the cluster function	Required	Section 1.2.6 “Enabling the Cluster Function”
Configure cluster parameters	Required	Section 1.2.7 “Configuring Cluster Parameters”
Configure interaction for the cluster	Required	Section 1.2.8 “Configuring Interaction for the Cluster”
Configure NM interface for the cluster	Optional	Section 1.2.9 “Configuring NM Interface for the Cluster”

Note:

To reduce the risk of being attacked by malicious users against opened socket and enhance switch security, the S3600 series Ethernet switches provide the following functions, so that a cluster socket is opened only when it is needed:

- Opening UDP port 40000 (used for cluster) only when the cluster function is implemented,
- Closing UDP port 40000 at the same time when the cluster function is closed.

On the management device, the preceding functions are implemented as follows:

- When you create a cluster by using the **build** or **auto-build** command, UDP port 40000 is opened at the same time.
- When you remove a cluster by using the **undo build** or **undo cluster enable** command, UDP port 40000 is closed at the same time.

1.2.2 Enabling NDP Globally and on Specific Ports

Table 1-3 Enable NDP globally and on specific ports

Operation			Command	Description
Enter system view			**system-view**	—
Enable NDP globally			**ndp enable**	Required By default, NDP is enabled globally.
Enable NDP on specified Ethernet ports	In system view		**ndp enable interface** *port-list*	You must choose one of the two ways. By default, NDP is enabled on a port.
	In Ethernet port view	Enter Ethernet port view	**interface** *interface-type interface-number*	
		Enable NDP on the port	**ndp enable**	

1.2.3 Configuring NDP-Related Parameters

Table 1-4 Configure NDP-related parameters

Operation	Command	Description
Enter system view	**system-view**	—
Configure the holdtime of NDP information	**ndp timer aging** *aging-in-seconds*	Optional By default, the holdtime of NDP information is 180 seconds.
Configure the interval to send NDP packets	**ndp timer hello** *seconds*	Optional By default, the interval to send NDP packets is 60 seconds.

1.2.4 Enabling NTDP Globally and on a Specific Port

Table 1-5 Enable NTDP globally and on a specific port

Operation	Command	Description
Enter system view	**system-view**	—
Enable NTDP globally	**ntdp enable**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Enable NTDP on the Ethernet port	**ntdp enable**	Required

1.2.5 Configuring NTDP-Related Parameters

Table 1-6 Configure NTDP-related parameters

Operation	Command	Description
Enter system view	**system-view**	—
Configure the range to collect topology information	**ntdp hop** *hop-value*	Optional By default, the system collects topology information from the devices within three hops.
Configure the device forward delay of topology collection requests	**ntdp timer hop-delay** *time*	Optional By default, the device forward delay is 200 ms.
Configure the port forward delay of topology collection requests	**ntdp timer port-delay** *time*	Optional By default, the port forward delay is 20 ms.
Configure the interval to collect topology information periodically	**ntdp timer** *interval-in-minutes*	Optional By default, the topology collection interval is one minute.
Quit system view	**quit**	—
Start topology collection	**ntdp explore**	Optional

1.2.6 Enabling the Cluster Function

Table 1-7 Enable the cluster function

Operation	Command	Description
Enter system view	**system-view**	—
Enable the cluster function globally	**cluster enable**	Optional By default, the cluster function is enabled.

1.2.7 Configuring Cluster Parameters

I. Manually building a cluster and configuring cluster parameters

Table 1-8 Manually build a cluster and configure cluster parameters

Operation	Command	Description
Enter system view	**system-view**	—
Specify the management VLAN	**management-vlan** *vlan-id*	Required By default, VLAN 1 is used as the management VLAN.
Enter cluster view	**cluster**	—
Configure a IP address pool for the cluster	**ip-pool** *administrator-ip-address* { *ip-mask* | *ip-mask-length* }	Required
Build a cluster	**build** *name*	Required *name*: cluster name.
Configure a multicast MAC address for the cluster	**cluster-mac** *H-H-H*	Optional By default, the cluster multicast MAC address is 0180-C200-000A.
Set the interval for the management device to send multicast packets	**cluster-mac syn-interval** *time-interval*	Optional By default, the interval to send multicast packets is one minutes.
Set the holdtime of member switches	**holdtime** *seconds*	Optional By default, the holdtime is 60 seconds.
Set the interval to send handshake packets	**timer** *interval*	Optional By default, the interval to send handshake packets is 10 seconds.
Quit cluster view	**quit**	—

II. Starting automatic cluster building

Table 1-9 Start automatic cluster building

Operation	Command	Description
Enter system view	**system-view**	—
Enter cluster view	**cluster**	—

Operation	Command	Description
Configure the cluster IP address range	**ip-pool** *administrator-ip-address* { *ip-mask* | *ip-mask-length* }	Required
Start automatic cluster building	**auto-build** [**recover**]	Required Follow prompts to build a cluster.

Note:

- After a cluster is built automatically, ACL 3998 and ACL 3999 will be generated automatically.
- After a cluster is built automatically, ACL 3998 and ACL 3999 can neither be configured/modified nor removed.

1.2.8 Configuring Interaction for the Cluster

Table 1-10 Configure interaction for the cluster

Operation	Command	Description
Enter system view	**system-view**	—
Enter cluster view	**cluster**	Required
Configure a shared FTP server for the cluster	**ftp-server** *ip-address*	Optional By default, the management device acts as the shared FTP server.
Configure a shared TFTP server for the cluster	**tftp-server** *ip-address*	Optional By default, no shared TFTP server is configured.
Configure a shared logging host for the cluster	**logging-host** *ip-address*	Optional By default, no shared logging host is configured.
Configure a shared SNMP host for the cluster	**snmp-host** *ip-address*	Optional By default, no shared SNMP host is configured.

1.2.9 Configuring NM Interface for the Cluster

I. Configuration prerequisites

- The cluster switches are properly connected;
- The shared servers are properly connected to the management switch.

II. Configuration procedure

Table 1-11 Configure NM interface for the cluster

Operation	Command	Description
Enter system view	**system-view**	—
Enter cluster view	**cluster**	Required
Configure the network management (NM) interface for the cluster	**nm-interface Vlan-interface** *vlan-id*	Optional By default, the management VLAN interface is used as the NM interface.

1.3 Cluster Configuration on Member Device

1.3.1 Member Device Cluster Configuration Tasks

Table 1-12 Member device Cluster configuration tasks

Operation	Description	Related section
Enable NDP globally and on specific ports	Required	Section 1.3.2 “Enabling NDP Globally and on Specific Ports”
Enable NTDP globally and on a specific port	Required	Section 1.3.3 “Enabling NTDP Globally and on a Specific Port”
Enable the cluster function	Required	Section 1.3.4 “Enabling the Cluster Function”
Access shared FTP/TFTP server from a member device	Optional	Section 1.3.5 “Accessing Shared FTP/TFTP Server

Note:

To reduce the risk of being attacked by malicious users against opened socket and enhance switch security, the S3600 series Ethernet switches provide the following functions, so that a cluster socket is opened only when it is needed:

- Opening UDP port 40000 (used for cluster) only when the cluster function is implemented,
- Closing UDP port 40000 at the same time when the cluster function is closed.

On member devices, the preceding functions are implemented as follows:

- When you execute the **add-member** command on the management device to add a candidate device to a cluster, the candidate device changes to a member device and its UDP port 40000 is opened at the same time.
- When you execute the **auto-build** command on the management device to have the system automatically add candidate devices to a cluster, the candidate devices change to member devices and their UDP port 40000 is opened at the same time.
- When you execute the **administrator-address** command on a device, the device's UDP port 40000 is opened at the same time.
- When you execute the **delete-member** command on the management device to remove a member device from a cluster, the member device's UDP port 40000 is closed at the same time.
- When you execute the **undo build** command on the management device to remove a cluster, UDP port 40000 of all the member devices in the cluster is closed at the same time.
- When you execute the **undo administrator-address** command on a member device, UDP port 40000 of the member device is closed at the same time.

1.3.2 Enabling NDP Globally and on Specific Ports

Table 1-13 Enable NDP globally and on specific ports

Operation	Command	Description
Enter system view	**system-view**	—
Enable NDP globally	**ndp enable**	Required

Operation			Command	Description
Enable NDP on specified ports	In system view		**ndp enable interface** *port-list*	Required You can choose to enable NDP on some ports in system view or enable NDP on a port in Ethernet port view.
	In Ethernet port view	Enter Ethernet port view	**interface** *interface-type interface-number*	
		Enable NDP on the port	**ndp enable**	

1.3.3 Enabling NTDP Globally and on a Specific Port

Table 1-14 Enable NTDP globally and a specific port

Operation	Command	Description
Enter system view	**system-view**	—
Enable NTDP globally	**ntdp enable**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable NTDP on the port	**ntdp enable**	Required

1.3.4 Enabling the Cluster Function

Table 1-15 Enable the cluster function

Operation	Command	Description
Enter system view	**system-view**	—
Enable the cluster function globally	**cluster enable**	Optional By default, the cluster function is enabled.

1.3.5 Accessing Shared FTP/TFTP Server from a Member Device

Perform the following operations in user view on a member device.

Table 1-16 Access shared FTP/TFTP server from a member device

Operation	Command	Description
Access the shared FTP server of the cluster	**ftp cluster**	Optional

Operation	Command	Description
Download a file from the shared TFTP server of the cluster	**tftp cluster get** *source-file* [*destination-file*]	Optional
Upload a file to the shared TFTP server of the cluster	**tftp cluster put** *source-file* [*destination-file*]	Optional

1.4 Cluster Member Configuration

Table 1-17 Cluster member configuration

Operation	Command	Description
Enter system view	**system-view**	—
Enter cluster view	**cluster**	—
Add a candidate device to the cluster	**add-member** [*member-number*] **mac-address** *H-H-H* [**password** *password*]	Optional
Remove a member device from the cluster	**delete-member** *member-number*	Optional
Reboot a specified member device	**reboot member** { *member-number* | **mac-address** *H-H-H* } [**eraseflash**]	Optional
Return to system view	**quit**	—
Return to user view	**quit**	—
Switch between management device and member device	**cluster switch-to** { *member-number* | **mac-address** *H-H-H* | **administrator** }	Optional You can use this command switch to the view of a member device and switch back.

1.5 Displaying and Maintaining Cluster Configuration

After the above configuration, you can execute the **display** command in any view to display the configuration and running status of cluster, so as to verify your configuration.

Table 1-18 Display and maintain cluster configuration

Operation	Command	Description
Display all NDP configuration and running information (including the interval to send NDP packets, the holdtime, and all neighbors discovered)	**display ndp**	You can execute the **display** command in any view.
Display NDP configuration and running information on specified ports (including the neighbors discovered by NDP on the ports)	**display ndp interface** *port-list*	
Display global NTDP information	**display ntdp**	
Display device information collected by NTDP	**display ntdp device-list** [**verbose**]	
Display status and statistics information about the cluster	**display cluster**	
Display information about the candidate devices of the cluster	**display cluster candidates** [**mac-address** *H-H-H* | **verbose**]	
Display information about the member devices of the cluster	**display cluster members** [*member-number* | **verbose**]	
Clear NDP statistics on ports	**reset ndp statistics** [**interface** *port-list*]	You can execute the **reset** command in user view.

1.6 Cluster Configuration Example

1.6.1 Basic Cluster Configuration Example

I. Network requirements

Three switches compose a cluster, where:

- An S3600 series switch serves as the management device.
- The rest are member devices.

Serving as the management device, the S3600 switch manages the two member devices. The configuration for the cluster is as follows:

- The two member devices connect to the management device through Ethernet1/0/2 and Ethernet1/0/3.
- The management device connects to the Internet through Ethernet1/0/1.

- Ethernet1/0/1 belongs to VLAN 2, whose interface IP address is 163.172.55.1.
- All the devices in the cluster share the same FTP server and TFTP server.
- The FTP server and TFTP server use the same IP address: 63.172.55.1.
- The NMS and logging host use the same IP address: 69.172.55.4.

II. Network diagram

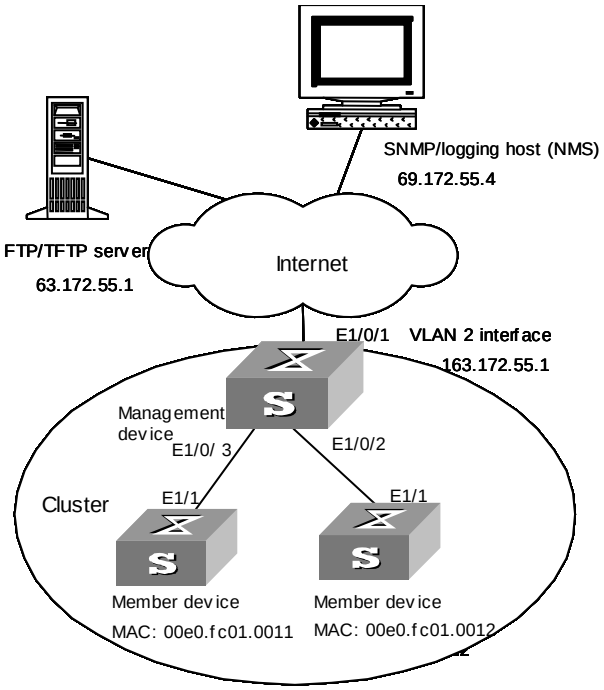


Figure 1-3 Network diagram for HGMP cluster configuration

III. Configuration procedure

1) Configure the member devices (taking one member as an example)

Enable NDP globally and on Ethernet1/1.

```
<H3C> system-view
[H3C] ndp enable
[H3C] interface Ethernet 1/1
[H3C-Ethernet1/1] ndp enable
[H3C-Ethernet1/1] quit
```

Enable NTDP globally and on Ethernet1/1.

```
[H3C] ntdp enable
[H3C] interface Ethernet 1/1
[H3C-Ethernet1/1] ntdp enable
[H3C-Ethernet1/1] quit
```

Enable the cluster function.

```
[H3C] cluster enable
```

2) Configure the management device

Enable NDP globally and on Ethernet1/0/2 and Ethernet1/0/3.

```
<H3C> system-view
[H3C] ndp enable
[H3C] interface Ethernet 1/0/2
[H3C-Ethernet1/0/2] ndp enable
[H3C-Ethernet1/0/2] interface Ethernet 1/0/3
[H3C-Ethernet1/0/3] ndp enable
[H3C-Ethernet1/0/3] quit
```

Set the holdtime of NDP information to 200 seconds.

```
[H3C] ndp timer aging 200
```

Set the interval to send NDP packets to 70 seconds.

```
[H3C] ndp timer hello 70
```

Enable NTDP globally and on Ethernet1/0/2 and Ethernet1/0/3.

```
[H3C] ntdp enable
[H3C] interface Ethernet 1/0/2
[H3C-Ethernet1/0/2] ntdp enable
[H3C-Ethernet1/0/2] interface Ethernet 1/0/3
[H3C-Ethernet1/0/3] ntdp enable
[H3C-Ethernet1/0/3] quit
```

Set the topology collection range to 2 hops.

```
[H3C] ntdp hop 2
```

Set the member device forward delay for topology collection requests to 150 ms.

```
[H3C] ntdp timer hop-delay 150
```

Set the member port forward delay for topology collection requests to 15 ms.

```
[H3C] ntdp timer port-delay 15
```

Set the interval to collect topology information to 3 minutes.

```
[H3C] ntdp timer 3
```

Enable the cluster function.

```
[H3C] cluster enable
```

Enter cluster view.

```
[H3C] cluster
[H3C-cluster]
```

Configure a private IP address pool for the cluster. The IP address pool contains six IP addresses, starting from 172.16.0.1.

```
[H3C-cluster] ip-pool 172.16.0.1 255.255.255.248
```

Name and build the cluster.

```
[H3C-cluster] build aaa
[aaa_0.H3C-cluster]
```

Add the attached two switches to the cluster.

```
[aaa_0.H3C-cluster] add-member 1 mac-address 00e0-fc01-0011
[aaa_0.H3C-cluster] add-member 17 mac-address 00e0-fc01-0012
```

Set the holdtime of member device information to 100 seconds.

```
[aaa_0.H3C-cluster] holdtime 100
```

Set the interval to send handshake packets to 10 seconds.

```
[aaa_0.H3C-cluster] timer 10
```

Configure the shared FTP server, TFTP server, Logging host and SNMP host for the cluster.

```
[aaa_0.H3C-cluster] ftp-server 63.172.55.1
[aaa_0.H3C-cluster] tftp-server 63.172.55.1
[aaa_0.H3C-cluster] logging-host 69.172.55.4
[aaa_0.H3C-cluster] snmp-host 69.172.55.4
```

3) Perform the following operations on the member devices (taking one member as an example)

After adding the devices under the management device to the cluster, perform the following operations on a member device.

Connect the member device to the remote shared FTP server of the cluster.

```
<aaa_1.H3C> ftp cluster
```

Download the file named aaa.txt from the shared TFTP server of the cluster to the member device.

```
<aaa_1.H3C> tftp cluster get aaa.txt
```

Upload the file named bbb.txt from the member device to the shared TFTP server of the cluster.

```
<aaa_1.H3C> tftp cluster put bbb.txt
```

Note:

- After completing the above configuration, you can execute the **cluster switch-to** { *member-number* | **mac-address** *H-H-H* } command on the management device to switch to member device view to maintain and manage a member device. After that, you can execute the **cluster switch-to administrator** command to return to management device view.
- In addition, you can execute the **reboot member** { *member-number* | **mac-address** *H-H-H* } [**eraseflash**] command on the management device to reboot a member device. For detailed information about these operations, refer to the preceding description in this chapter.
- After the above configuration, you can receive logs and SNMP trap messages of all cluster members on the NMS.

1.6.2 NM Interface Configuration Example

I. Network requirements

- Configure VLAN-interface 2 as the NM interface of the switch;
- Configure VLAN 3 as the management VLAN;
- The IP address of the FTP server is 192.168.4.3;
- The S3600 switch is the management switch;
- The S3526E and S2403 switches are member switches.

Table 1-19 Connection information of the management switch

VLAN	IP address	Connection port
VLAN 3 (connect to S3526E)	192.168.5.30/24	Ethernet 1/0/1
VLAN 2 (connect to FTP server)	192.168.4.22/24	Ethernet 1/0/2

II. Network diagram

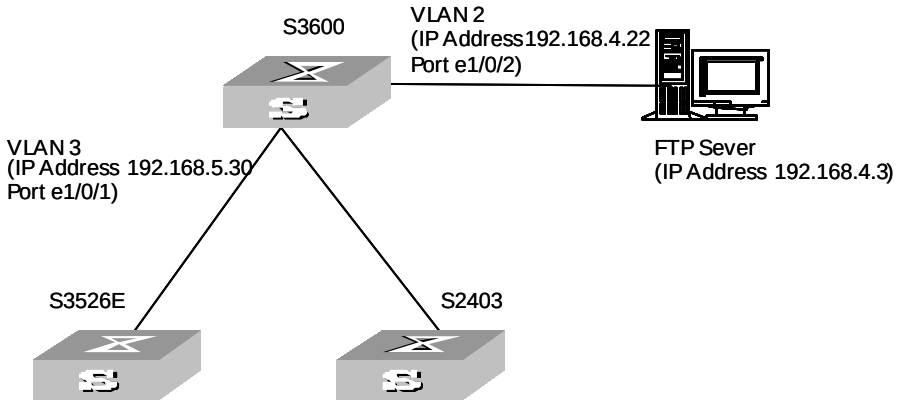


Figure 1-4 Network diagram for NM interface configuration

III. Configuration procedure

Enter system view and configure VLAN 3 as the management VLAN.

```
<H3C> system-view
[H3C] management-vlan 3
```

Add Ethernet 1/0/1 to VLAN 3.

```
[H3C] vlan 3
[H3C-vlan3] port Ethernet 1/0/1
[H3C-vlan3] quit
```

Set the IP address of VLAN-interface 3 to 192.168.5.30.

```
[H3C] interface Vlan-interface 3
[H3C-Vlan-interface3] ip address 192.168.5.30 255.255.255.0
[H3C-Vlan-interface3] quit
```

Add Ethernet 1/0/2 to VLAN 2.

```
[H3C] vlan 2
[H3C-vlan2] port Ethernet 1/0/2
[H3C-vlan2] quit
```

Set the IP address of VLAN-interface 2 to 192.168.4.22.

```
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2] ip address 192.168.4.22 255.255.255.0
[H3C-Vlan-interface2] quit
```

Configure VLAN-interface 2 as the NM interface.

```
[H3C] cluster
[H3C-cluster] nm-interface Vlan-interface 2
```

Table of Contents

Chapter 1 PoE Configuration 1-1
1.1 PoE Overview 1-1
1.1.1 Introduction to PoE 1-1
1.1.2 PoE Features Supported by S3600 1-1
1.2 PoE Configuration Tasks 1-3
1.3 Enabling the PoE Feature on a Port 1-3
1.4 Setting the Maximum Output Power on a Port 1-4
1.5 Setting PoE Management Mode and PoE Priority of a Port 1-4
1.6 Setting the PoE Mode on a Port 1-5
1.7 Configuring the PD Compatibility Detection Feature 1-6
1.8 Configuring PoE Over-Temperature Protection on the Switch 1-6
1.9 Upgrading the PSE Processing Software Online 1-7
1.10 Displaying PoE Configuration 1-7
1.11 PoE Configuration Example 1-8
Chapter 2 PoE Profile Configuration 2-1
2.1 Introduction to PoE Profile 2-1
2.2 PoE Profile Configuration Tasks 2-1
2.3 Displaying PoE Profile Configuration 2-3
2.4 PoE Profile Configuration Example 2-3

Chapter 1 PoE Configuration

1.1 PoE Overview

1.1.1 Introduction to PoE

Power over Ethernet (PoE) uses 10Base-T, 100Base-TX, and 1000Base-T twisted pairs to supply power to the remote powered devices (PD) in the network and implement power supply and data transmission simultaneously.

I. Advantages of PoE

- Reliability: The centralized power supply provides backup convenience, unified management, and safety.
- Easy connection: Network terminals only require an Ethernet cable, but no external power supply.
- Standard: PoE conforms to the 802.3af standard and uses a globally uniform power interfaces;
- Bright application prospect: PoE can be applied to IP phones, wireless access points (APs), chargers for portable devices, card readers, cameras, and data collection.

II. PoE components

- Power sourcing equipment (PSE): PSE is comprised of the power and the PSE functional module. It can implement PD detection, PD power information collection, PoE, power supply monitoring, and power-off for devices.
- Powered device (PD): PDs receive power from the PSE. PDs include standard PDs and nonstandard PDs. Standard PDs conform to the 802.3af standard, including IP phones, WLAN APs, network cameras and so on.
- Power interface (PI): PIs are RJ45 interfaces which connect PSE/PDs to network cables.

1.1.2 PoE Features Supported by S3600

PoE-enabled S3600 series Ethernet switches include:

- S3600-28P-PWR-SI
- S3600-28P-PWR-EI
- S3600-52P-PWR-EI
- S3600-52P-PWR-SI

A PoE-enabled S3600 switch has the following features:

- As the PSE, it supports the IEEE802.3af standard. It can also supply power to some PDs that do not support the 802.3af standard.
- It can deliver data and current simultaneously through data wires (1, 3, 2, and 6) of category-3/5 twisted pairs.
- Through the fixed 24/48 Ethernet electrical ports, it can supply power to up to 24/48 remote Ethernet switches with a maximum distance of 100 m (328 feet).
- Each Ethernet port can supply at most a power of 15,400 mW to a PD.
- When AC power input is adopted for the switch, the maximum total power that can be provided is 300 W. It can determine whether to supply power to the next remote PD it detects depending on its available power.
- When DC power input is adopted for the switch: it is capable of supplying full power to all of the 24/48 ports, that is, 15,400 mW for each port, and the total power is 369.6/739.2 W.
- The PSE processing software on the switch can be upgraded online.
- The switch provides statistics about power supplying on each port and the whole equipment, which you can query through the **display** command.
- The switch provides two modes (**auto** and **manual**) to manage the power feeding to ports in the case of PSE power overload.
- The switch provides over-temperature protection mechanism. Using this mechanism, the switch disables the PoE feature on all ports when its internal temperature exceeds 65 ^{0}C (149 ^{0}F) for self-protection, and restores the PoE feature on all its ports when the temperature drops below 60 ^{0}C (140 ^{0}F).
- The switch supports the PoE profile feature, that is, different PoE policies can be set for different user groups. These PoE policies are each saved in the corresponding PoE profile and applied to ports of the user groups.

Note:

- When using the PoE-enabled S3600 switch to supply power, the PDs need not have any external power supply.
- If a remote PD has an external power supply, the PoE-enabled S3600 switch and the external power supply will be redundant with each other for the PD.
- Only the electrical ports of the PoE-enabled S3600 switch support the PoE feature.

1.2 PoE Configuration Tasks

Table 1-1 PoE configuration tasks

Operation	Description	Related section
Enable the PoE feature on a port	Required	Section 1.3 “Enabling the PoE Feature on a Port”
Set the maximum output power on a port	Optional	Section 1.4 “Setting the Maximum Output Power on a Port”
Set PoE management mode and PoE priority of a port	Optional	Section 1.5 “Setting PoE Management Mode and PoE Priority of a Port”
Set the PoE mode on a port	Optional	Section 1.6 “Setting the PoE Mode on a Port“
Configure the PD compatibility detection feature	Optional	Section 1.7 “Configuring the PD Compatibility Detection Feature”
Configure PoE over-temperature protection on the switch	Optional	Section 1.8 “Configuring PoE Over-Temperature Protection on the Switch”
Upgrade the PSE processing software online	Optional	Section 1.9 “Upgrading the PSE Processing Software Online”

1.3 Enabling the PoE Feature on a Port

Table 1-2 Enable the PoE feature on a port

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the PoE feature on the port	**poe enable**	Required By default, the PoE function on a port is enabled by the default configuration file when the device is delivered

Caution:

By default, the PoE function on a port is enabled by the default configuration file when the device is delivered.

If you delete the default configuration file without specifying another one, the PoE function on a port will be disabled after you restart the device..

1.4 Setting the Maximum Output Power on a Port

The maximum power that can be supplied by a PoE-enabled S3600 switch to its PD is 15,400 mW. In practice, you can set the maximum power on a port depending on the actual power of the PD, in the range of 1,000 to 15,400 mW and in the granularity of 100 mW.

Table 1-3 Set the maximum output power on a port

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the maximum output power on the port	**poe max-power** *max-power*	Required By default, the maximum output power on a port is 15,400 mW

1.5 Setting PoE Management Mode and PoE Priority of a Port

The power supply management mode and the port priority settings will work together to control the power feeding of the switch when the switch PoE is close to its full power load.

When AC power input is adopted for the switch, the maximum total power that can be supplied by the PoE-enabled S3600 switch is 300 W. By default, when the switch PoE reaches its full load in supplying power, it will manage the power supply to its ports in **auto** mode.

- **auto** mode: When the switch is close to its full load in supplying power, it will first supply power to the PDs that are connected to the ports with critical priority, and then supply power to the PDs that are connected to the ports with high priority. For example: Port A has the priority of critical. When the switch PoE is close to its full load and a new PD is now added to port A, the switch will power down the PD

connected to the port with the lowest priority and turn to supply power to this new PD. IF more than one port has the same lowest priority, the switch will power down the PD connected to the port with larger logical port number.

- **manual** mode: When the switch is close to its full load in supplying power, it will not make change to its original power supply status based on its priority when a new PD is added. For example: Port A has the priority critical. When the switch PoE is close to its full load and a new PD is now added to port A, the switch just gives a prompt that a new PD is added and will not supply power to this new PD.

After the PoE feature is enabled on the port, perform the following configuration to set the PoE management mode and PoE priority of a port.

Table 1-4 Set the PoE management mode and PoE priority of a port

Operation	Command	Description
Enter system view	**system-view**	—
Set the PoE management mode for the switch	**poe power-management** { **auto** | **manual** }	Required By default, the PoE management mode is **auto**
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Se the PoE priority of a port	**poe priority** { **critical** | **high** | **low** }	Required By default, the PoE priority of a port is **low**

1.6 Setting the PoE Mode on a Port

After the PoE feature is enabled on the port, perform the following configuration to set the PoE mode on a port.

Table 1-5 Set the PoE mode on a port

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the PoE mode on the port	**poe mode** { **signal** | **spare** }	Required S3600 series Ethernet switches do not support PoE in the **spare** mode currently

1.7 Configuring the PD Compatibility Detection Feature

After the PD compatibility detection feature is enabled, the switch can supply power to the detected PDs that do not conform to the 802.3af standard.

After the PoE feature is enabled, perform the following configuration to enable the PD compatibility detection feature.

Table 1-6 Configure the PD compatibility detection feature

Operation	Command	Description
Enter system view	**system-view**	—
Enable the PD compatibility detection function	**poe legacy enable**	Required By default, the PD compatibility detection feature is disabled

1.8 Configuring PoE Over-Temperature Protection on the Switch

If this function is enabled, the switch disables the PoE feature on all ports when its internal temperature exceeds 65 ^{0}C (149 ^{0}F) for self-protection, and restores the PoE feature settings on all its ports when the temperature drops below 60 ^{0}C (140 ^{0}F).

Table 1-7 Configure PoE over-temperature protection on the switch

Operation	Command	Description
Enter system view	**system-view**	—
Enable the PoE over-temperature protection feature on the switch	**poe temperature-protection enable**	Required By default, the PoE over-temperature protection feature is enabled on the switch

Note:

- When the internal temperature of the switch decreases to 65^{0}C (149^{0}F) below, but 60^{0}C (140^{0}F) above, the switch still disables the PoE feature on all the ports.
- When the internal temperature of the switch increases to 60 ^{0}C (140 ^{0}F) above, but 65^{0}C (149^{0}F) below, the switch still enables the PoE feature on all the ports.

1.9 Upgrading the PSE Processing Software Online

The online upgrading of PSE processing software can update the processing software or repair the software if it is damaged. After downloading the PSE processing software to the Flash of the switch, you can perform the following configuration. Refer to “File System Management” for how to download the PSE processing software.

Table 1-8 Upgrade PSE processing software online

Operation	Command	Description
Enter system view	**system-view**	—
Upgrade the PSE processing software online	**poe update** { **refresh** | **full** } *filename*	Required

Note:

- The **refresh** update mode is to upgrade the valid software in the PSE through refreshing the software, while the **full** update mode is to delete the invalid software in PSE completely and then reload the software.
- Generally, the **refresh** update mode is used to upgrade the PSE processing software.
- When the PSE processing software is damaged (that is, all the PoE commands cannot be successfully executed), you can use the **full** update mode to upgrade and restore the software.
- When the online upgrading procedure is interrupted for some unexpected reason (for example, the device restarts due to some errors), if the upgrade in **full** mode fails after restart, you must upgrade in **full** mode after power-off and restart of the device, and then restart the device manually. In this way, the former PoE configuration is restored.

1.10 Displaying PoE Configuration

After the above configuration, execute the **display** command in any view to see the operation of the PoE feature and verify the effect of the configuration.

Table 1-9 Display PoE information

Operation	Command	Description
Display the PoE status of a specific port or all ports of the switch	**display poe interface** [*interface-type interface-number*]	You can execute the **display** command in any view
Display the PoE power information of a specific port or all ports of the switch	**display poe interface power** [*interface-type interface-number*]	
Display the PSE parameters	**display poe powersupply**	
Display the enabled/disabled status of the PoE over-temperature protection feature on the switch	**display poe temperature-protection**	

1.11 PoE Configuration Example

I. Networking requirements

- The Ethernet 1/0/1 and Ethernet 1/0/2 ports of the S3600-28P-PWR-EI switch are connected to an S2016C switch and an AP respectively; the Ethernet 1/0/24 port is intended to be connected with an important AP.
- The PSE processing software of the S3600-28P-PWR-EI switch is first upgraded online. The remotely accessed PDs are powered by the S3600-28P-PWR-EI switch.
- The power consumption of the accessed AP is 2,500 mW, and the power consumption of the S2016C switch is 12,000 mW.
- It is required to guarantee the power feeding to the PDs connected to the Ethernet1/0/24 port even when the S3600-28P-PWR-EI switch is under full load.

II. Networking diagram

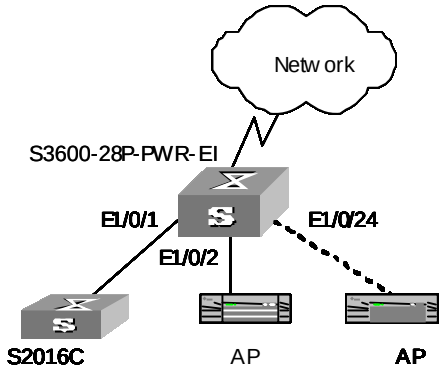


Figure 1-1 Network diagram for PoE

III. Configuration procedure

Upgrade the PSE processing software online.

```
<H3C> system-view
[H3C] poe update refresh 0290_021.s19
```

Enable the PoE feature on Ethernet 1/0/1, Ethernet 1/0/2, and Ethernet 1/0/24.

```
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] poe enable
[H3C-Ethernet1/0/1] quit
[H3C]interface Ethernet 1/0/2
[H3C-Ethernet1/0/2] poe enable
[H3C-Ethernet1/0/2] quit
[H3C] interface Ethernet 1/0/24
[H3C-Ethernet1/0/24] poe enable
[H3C-Ethernet1/0/24] quit
```

Set the maximum output power of Ethernet 1/0/1 and Ethernet 1/0/2 to 12,000 mW and 2,500 mW respectively.

```
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] poe max-power 12000
[H3C-Ethernet1/0/1] interface Ethernet 1/0/2
[H3C-Ethernet1/0/2] poe max-power 2500
[H3C-Ethernet1/0/2] quit
```

Set the PoE priority of Ethernet 1/0/24 to critical to guarantee the power feeding to the AP to which this port connects.

```
[H3C] interface Ethernet 1/0/24
[H3C-Ethernet1/0/24] poe priority critical
[H3C-Ethernet1/0/24] quit
```

Set the power supply management mode on the switch to auto (it is the default mode, so this step can be ignored).

```
[H3C] poe power-management auto
```

Enable the PD compatibility detect of the switch to allow the switch to supply power to part of the devices noncompliant with the 802.3af standard.

```
[H3C] poe legacy enable
```

Chapter 2 PoE Profile Configuration

2.1 Introduction to PoE Profile

On a large-sized network or a network with mobile users, to help network administrators to monitor the PoE features of the switch, S3600 series Ethernet switches provide the PoE profile features.

Features of PoE profile:

- Various PoE profiles can be created. PoE policy configurations applicable to different user groups are stored in the corresponding PoE profiles. These PoE profiles can be applied to the ports used by the corresponding user groups.
- When users connect a PD to a PoE-profile-enabled port, the PoE configurations in the PoE profile will be enabled on the port.

2.2 PoE Profile Configuration Tasks

Table 2-1 Configure PoE profile

Operation		Command	Description
Enter system view		**system-view**	—
Create a PoE profile		**poe-profile** *profilename*	Required Enter PoE profile view while creating the PoE profile
Configure the relevant features in PoE profile	Enable the PoE feature on a port	**poe enable**	Required The PoE feature on a port is disabled by default
	Configure PoE mode for Ethernet ports	**poe mode** { **signal** | **spare** }	Optional By default, PoE mode is set to be **signal**
	Configure the PoE priority for Ethernet ports	**poe priority** { **critical** | **high** | **low** }	Optional By default, PoE priority is set to **low**
	Configure the maximum power for Ethernet ports	**poe max-power** *max-power*	Optional By default, maximum power is set to be 15,400 mW
Quit system view		**quit**	—

<table>
<tr><th colspan="3">Operation</th><th>Command</th><th>Description</th></tr>
<tr><td rowspan="3">Apply the existing PoE profile to the specified Ethernet port</td><td colspan="2">In system view</td><td>apply poe-profile profile-name interface interface-type interface-number [to interface-type interface-number]</td><td rowspan="3">Required
Users can decide whether to configure the settings in system view or port view</td></tr>
<tr><td rowspan="2">In Ethernet port view</td><td>Enter Ethernet port view</td><td>interface interface-type interface-number</td></tr>
<tr><td>Apply the existing PoE profile to the port</td><td>apply poe-profile profile-name</td></tr>
</table>

Note:

A PoE profile is a group of PoE configurations. Multiple PoE features can be set in a PoE profile. When the **apply poe-profile** command is used to apply a PoE profile to a port, some PoE features can be applied successfully while some PoE configurations in it cannot. PoE profiles are applied to S3600 series Ethernet switches according to the following rules:

- When the **apply poe-profile** command is used to apply a PoE profile to a port, the PoE profile is applied successfully only if one PoE feature in the PoE profile is applied properly. When the **display current-configuration** command is used for query, it is displayed that the PoE profile is applied properly to the port.
- If one or more features in the PoE profile are not applied properly on a port, the switch will prompt explicitly which PoE features in the PoE profile are not applied properly on which ports.
- The **display current-configuration** command can be used to query which PoE profiles are applied to a port. However, the command cannot be used to query which PoE features in a PoE profiles are applied successfully.

Caution:

- PoE profile configuration is a global configuration, and applies synchronously in the intelligent resilient framework (IRF) system.
- Combination of Unit creates a new Fabric. In the newly created Fabric, the PoE profile configuration of the Unit with the smallest Unit ID number will become the PoE profile configuration for the Fabric currently in use.
- Split of Fabric results in many new Fabrics. In each newly created Fabric, the PoE profile configuration of each Unit remains the same as it was before the split.

2.3 Displaying PoE Profile Configuration

After the above configuration, execute the **display** command in any view to see the running status of the PoE profile and verify the effect of the configuration by checking the displayed information.

Table 2-2 Display the PoE profile configuration

Operation	Command	Description
Display the detailed information about the PoE profiles created on the switch	**display poe-profile** { **all-profile** | **interface** *interface-type interface-number* | **name** *profile-name* }	You can execute the **display** command in any view

2.4 PoE Profile Configuration Example

I. Network requirements

Ethernent1/0/1 through Ethernet1/0/10 of the S3600-28P-PWR-EI switch are used by users of group A, who have the following requirements:

- The PoE function can be enabled on all ports in use.
- Signal cables are used to supply power.
- The PoE priority for Ethernet1/0/1 through Ethernet1/0/5 is Critical, whereas the PoE priority for Ethernet1/0/6 through Ethernet1/0/10 is High.
- The maximum power for Ethernet1/0/1 through Ethernet1/0/5 ports is 3,000 mW, whereas the maximum power for Ethernet1/0/6 through Ethernet1/0/10 is 15,400 mW.

Based on the above requirements, two PoE profiles are made for users of group A.

- Apply PoE profile 1 for Ethernet1/0/1 through Ethernet 1/0/5;
- Apply PoE profile 2 for Ethernet1/0/6 through Ethernet 1/0/10.

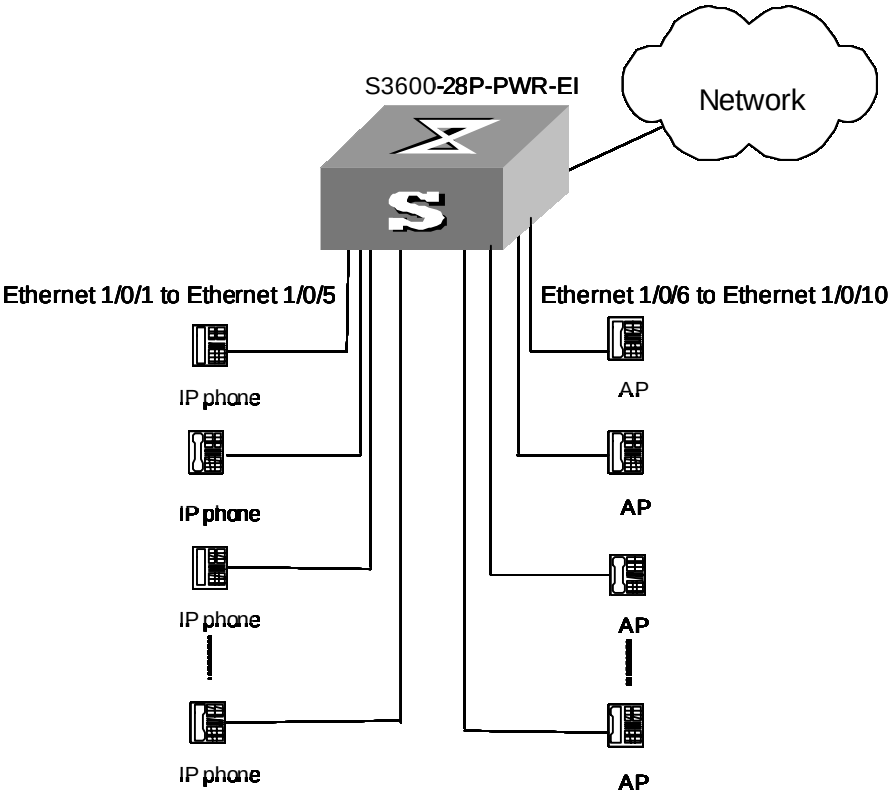


Figure 2-1 PoE profile application

II. Configuration procedure

Create Profile1, and enter PoE profile view.

```
<H3C> system-view
[H3C] poe-profile Profile1
```

In Profile1, add the PoE policy configuration applicable to Ethernet1/0/1 through Ethernet1/0/5 ports for users of group A.

```
[H3C-poe-profile-Profile1] poe enable
[H3C-poe-profile-Profile1] poe mode signal
[H3C-poe-profile-Profile1] poe priority critical
[H3C-poe-profile-Profile1] poe max-power 3000
[H3C-poe-profile-Profile1] quit
```

Display detailed configuration information for Profile1.

```
[H3C] display poe-profile name Profile1
```

Create Profile2, and enter poe-profile view.

```
[H3C] poe-profile Profile2
```

In Profile2, add the PoE policy configuration applicable to Ethernet1/0/6 through Ethernet1/0/10 ports for users of group A.

```
[H3C-poe-profile-Profile2] poe enable
[H3C-poe-profile-Profile2] poe mode signal
[H3C-poe-profile-Profile2] poe priority high
[H3C-poe-profile-Profile2] poe max-power 15400
[H3C-poe-profile-Profile2] quit
```

Display detailed configuration information for Profile2.

```
[H3C] display poe-profile name Profile2
```

Apply the configured Profile1 to Ethernet1/0/1 through Ethernet1/0/5 ports.

```
[H3C] apply poe-profile Profile1 interface Ethernet1/0/1 to Ethernet1/0/5
```

Apply the configured Profile2 to Ethernet1/0/6 through Ethernet1/0/10 ports.

```
[H3C] apply poe-profile Profile2 interface Ethernet1/0/6 to Ethernet1/0/10
```

Table of Contents

Chapter 1 UDP Helper Configuration 1-1
1.1 Introduction to UDP Helper 1-1
1.2 Configuring UDP Helper 1-2
1.3 Displaying and Maintaining UDP Helper 1-3
1.4 Configuration Example 1-3
1.4.1 Network requirements 1-3
1.4.2 Network diagram 1-4
1.4.3 Configuration procedure 1-4

Chapter 1 UDP Helper Configuration

1.1 Introduction to UDP Helper

UDP Helper is to relay specified UDP packets. In other words, UDP Helper functions as a relay that converts UDP broadcast packets into unicast packets and forwards them to a specified server.

With UDP Helper 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.

Note:

Relay forwarding of BOOTP/DHCP broadcast packets is implemented by the DHCP relay module using UDP ports 67 and 68, so these two ports cannot be configured as UDP-Helper relay port.

Table 1-1 lists the default UDP ports that are commonly used to forward broadcast packets in UDP Helper function. With UDP Helper enabled, the system unicasts the broadcast packets of those default UDP ports to a specified destination server. You can also specify other UDP ports to relay broadcast packets.

Table 1-1 List of default UDP ports

Protocol	UDP port number
DNS (Domain Name System)	53
NetBIOS-DS (NetBIOS Datagram Service)	138
NetBIOS-NS (NetBIOS Name Service)	137
TACACS (Terminal Access Controller Access Control System)	49
TFTP (Trivial File Transfer Protocol)	69
Time Service	37

1.2 Configuring UDP Helper

Table 1-2 Configure UDP Helper

Operation	Command	Description
Enter system view	**system-view**	—
Enable UDP Helper	**udp-helper enable**	Required Disabled by default
Specify a UDP port	**udp-helper port** { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }	Optional To use the default UDP ports for relay forwarding, this command can be ignored, otherwise, use this command to perform configuration as required. After UDP-Helper is enabled, the broadcast packets through ports 53, 138, 137, 49, 69 and 37 are relayed by default.
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Configure the destination server to which the UDP packets are to be forwarded	**udp-helper server** *ip-address*	Required No destination server is configured by default.

Note that:

- You need to enable the UDP Helper function before specifying any UDP port to relay UDP broadcast packets; otherwise, the configuration fails.
- The **dns**, **netbios-ds**, **netbios-ns**, **tacacs**, **tftp**, and **time** keywords correspond to the six default ports. You can configure the default ports by specifying port numbers or the corresponding parameters. For example, **udp-helper port** 53 and **udp-helper port dns** specify the same port.
- With the UDP Helper function enabled, the six default ports are specified to be UDP ports to relay UDP broadcast packets, no further configuration is need.
- When you view the configuration information by using the **display current-configuration** command, the UDP Helper configuration on default UDP ports is not displayed. The UDP Helper configuration of a default UDP port is displayed only when UDP Helper is disabled on the port.
- When the UDP helper function is disabled, all configured UDP ports are disabled, including the default ports.
- A UDP helper enabled device can have up to 256 UDP port for packet relay.
- A VLAN interface corresponds to a maximum of 20 destination servers.

- If the destination server is configured on a VLAN interface, the broadcast packets from a VLAN interface to a specific UDP port will be unicast to the destination server configured on that VLAN interface after UDP Helper is enabled.

1.3 Displaying and Maintaining UDP Helper

After performing the above configurations, use the **display** command in any view to display the running status of the UDP Helper configuration, and verify the configuration result. You can use the **reset** command in user view to clear statistics about packets forwarded by UDP Helper.

Table 1-3 Display and maintain UDP Helper configuration

Operation	Command	Description
Display the information of the destination server and the number of packets forwarded to the destination server	**display udp-helper server** [**interface Vlan-interface** *vlan-id*]	You can use the **display** command in any view
Clear statistics about packets forwarded by UDP Helper	**reset udp-helper packet**	You can use the **reset** command in user view

1.4 Configuration Example

1.4.1 Network requirements

PC1 resides on network segment 192.168.1.1/24 and PC2 on 10.2.72.1/24; they are connected by two switches and are routable to each other. It is required to configure UDP Helper on the switch, letting PC1 to search for PC2. (Broadcast packets through port 137 are used for searching.)

1.4.2 Network diagram

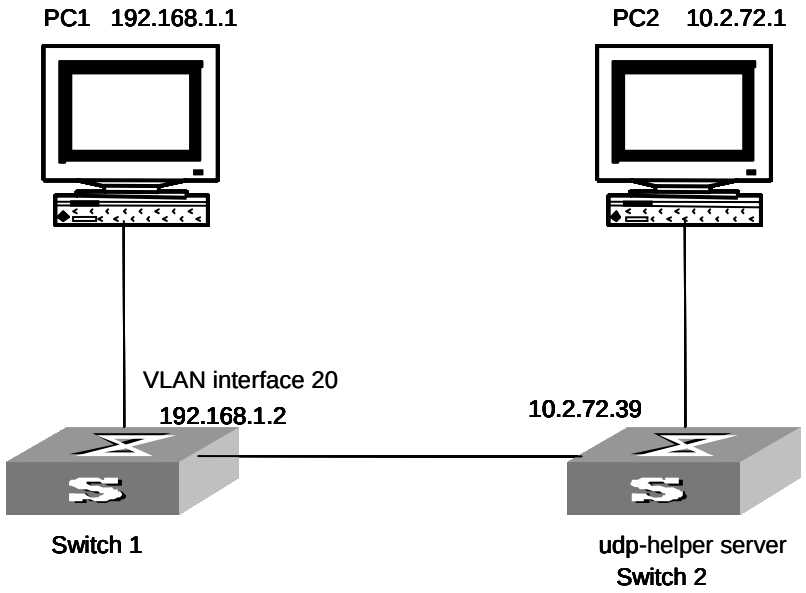


Figure 1-1 Network diagram for UDP Helper configuration

1.4.3 Configuration procedure

Enable UDP Helper on Switch1.

```
<H3C> system-view
[H3C] udp-helper enable
```

Specify port 137 to be the UDP port for forwarding UDP broadcast packets. Port 137 is the default UDP port, as prompted in the command line.

```
[H3C] udp-helper port 137
Port has been configured. Please check the port again.
```

Specify the destination server to which UDP packets are to be forwarded.

```
[H3C] interface Vlan-interface 20
[H3C-Vlan-interface20] udp-helper server 10.2.72.1
```

Table of Contents

Chapter 1 SNMP Configuration 1-1
1.1 SNMP Overview 1-1
1.1.1 SNMP Operation Mechanism 1-1
1.1.2 SNMP Versions 1-1
1.1.3 Supported MIBs 1-2
1.2 Configuring Basic SNMP Functions 1-3
1.3 Configuring Trap 1-6
1.3.1 Configuration Prerequisites 1-6
1.3.2 Configuration Tasks 1-7
1.4 Enabling Logging for Network Management 1-8
1.5 Displaying SNMP 1-8
1.6 SNMP Configuration Example 1-9
1.6.1 SNMP Configuration Example 1-9
Chapter 2 RMON Configuration 2-1
2.1 Introduction to RMON 2-1
2.1.1 Working Mechanism of RMON 2-1
2.1.2 Commonly Used RMON Groups 2-2
2.2 RMON Configuration 2-3
2.2.1 Prerequisites 2-3
2.2.2 Configuring RMON 2-4
2.3 Displaying RMON 2-5
2.4 RMON Configuration Example 2-5

Chapter 1 SNMP Configuration

1.1 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 network nodes. In this way, network administrators can easily retrieve and modify the information about any node on the network. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

As SNMP adopts the polling mechanism and only provides basic function set, it is suitable for small-sized networks with fast-speed and low-cost. SNMP is based on user datagram protocol (UDP) and is thus widely supported by many products.

1.1.1 SNMP Operation Mechanism

SNMP is implemented by two components, namely, network management station (NMS) and agent.

An NMS can be a workstation running client program. At present, the commonly used network management platforms include QuidView, Sun NetManager, IBM NetView, and so on.

Agent is server-side software running on network devices.

An NMS can send GetRequest, GetNextRequest and SetRequest messages to the agents. Upon receiving the requests from the NMS, an agent performs Read or Write operation according to the message types, generate the corresponding Response packets and return them to the NMS.

When a network device operates improperly or changes to other state, the agent on it can also send trap messages on its own initiative to the NMS to report the events.

1.1.2 SNMP Versions

Currently, SNMP agent on a network device supports SNMPv3, and is compatible with SNMPv1 and SNMPv2C.

SNMPv3 adopts user name and password authentication.

SNMPv1 and SNMPv2C adopt community name authentication. The SNMP packets containing invalid community names are discarded. SNMP community name is used to define the relationship between SNMP NMS and SNMP agent. Community name

functions as password. It can limit accesses made by SNMP NMS to SNMP agent. You can perform the following community name-related configuration.

- Specifying MIB view that a community can access.
- Set the permission for a community to access an MIB object to be read-only or read-write. Communities with read-only permissions can only query device information, while those with read-write permission can configure devices as well.
- Set the basic ACL specified by the community name.

1.1.3 Supported MIBs

An SNMP packet carries management variables with it. Management variable is used to describe the management objects of a device. To uniquely identify the management objects of the device, SNMP adopts a hierarchical naming scheme to organize the managed objects. It is like a tree, with each tree node representing a managed object, as shown in Figure 1-1. Each node in this tree can be uniquely identified by a path starting from the root.

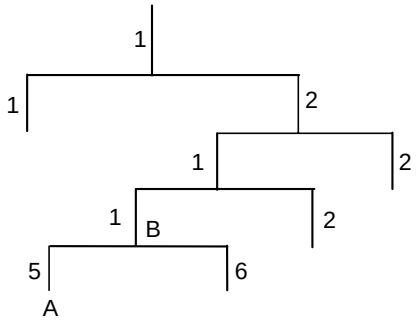


Figure 1-1 Architecture of the MIB tree

The management information base (MIB) describes the hierarchical architecture of the tree and it is the set defined by the standard variables of the monitored network devices. In the above figure, the managed object B can be uniquely identified by a string of numbers {1.2.1.1}. The number string is the object identifier of the managed object.

The common MIBs supported by the system are listed in Table 1-1.

Table 1-1 Common MIBs

MIB attribute	MIB content	Related RFC
Public MIB	MIB II based on TCP/IP network device	RFC1213
	BRIDGE MIB	RFC1493
		RFC2675
	RIP MIB	RFC1724
	RMON MIB	RFC2819
	Ethernet MIB	RFC2665
	OSPF MIB	RFC1253
	IF MIB	RFC1573
Private MIB	DHCP MIB QACL MIB ADBM MIB RSTP MIB VLAN MIB Device management Interface management	—

1.2 Configuring Basic SNMP Functions

SNMPv3 configuration is quite different from that of SNMPv1 and SNMPv2C. Therefore, the configuration of basic SNMP functions is described by SNMP versions, as listed in Table 1-2 and Table 1-3.

Table 1-2 Configure basic SNMP functions (SNMPv1 and SNMPv2C)

Operation	Command	Description
Enter system view	**system-view**	—
Enable SNMP agent	**snmp-agent**	Optional By default, SNMP agent is disabled. You can enable SNMP agent by executing this command or any of the commands used to configure SNMP agent.

<table>
<tr><th colspan="3">Operation</th><th>Command</th><th>Description</th></tr>
<tr><td colspan="3">Set system information</td><td>snmp-agent sys-info { contact sys-contact | location sys-location | version { { v1 | v2c | v3 }* | all } }</td><td>Required
By default, the contact information for system maintenance is "R&D Hangzhou, H3C Technologies Co.,Ltd.", the system location is "Hangzhou China", and the SNMP version is SNMPv3.</td></tr>
<tr><td rowspan="3">Set a community name and access permission</td><td>Direct configuration</td><td>Set a community name</td><td>snmp-agent community { read | write } community-name [acl acl-number | mib-view view-name]*</td><td rowspan="3">Required
• You can set an SNMPv1/SNMPv2C community name through direct configuration.
• Indirect configuration is compatible with SNMPv3. The added user is equal to the community name for SNMPv1 and SNMPv2C.
• You can choose either of them as needed.</td></tr>
<tr><td rowspan="2">Indirect configuration</td><td>Set an SNMP group</td><td>snmp-agent group { v1 | v2c } group-name [read-view read-view] [write-view write-view] [notify-view notify-view] [acl acl-number]</td></tr>
<tr><td>Add a user to an SNMP group</td><td>snmp-agent usm-user { v1 | v2c } user-name group-name [acl acl-number]</td></tr>
<tr><td colspan="3">Set the maximum SNMP packet size for SNMP agent</td><td>snmp-agent packet max-size byte-count</td><td>Optional
By default, the maximum SNMP packet size is 1,500 bytes.</td></tr>
<tr><td colspan="3">Set the device engine ID</td><td>snmp-agent local-engineid engineid</td><td>Optional
By default, the device engine ID is formed by appending device information to the enterprise number.</td></tr>
<tr><td colspan="3">Create/Update the view information</td><td>snmp-agent mib-view { included | excluded } view-name oid-tree</td><td>Optional
By default, the view name is “ViewDefault” and OID is 1.</td></tr>
</table>

Table 1-3 Configure basic SNMP functions (SNMP V3)

Operation	Command	Description
Enter system view	**system-view**	—
Enable SNMP agent	**snmp-agent**	Required By default, SNMP Agent is disabled. You can enable SNMP agent by executing this command or any of the commands used to configure SNMP agent.
Set system information	**snmp-agent sys-info** { **contact** *sys-contact* | **location** sys-l*ocation* | **version** { { **v1** | **v2c** | **v3** }* | **all** } }	Optional By default, the contact information for system maintenance is "R&D Hangzhou, H3C Technologies Co.,Ltd.", the system location is "Hangzhou China", and the SNMP version is SNMPv3.
Set an SNMP group	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]	Required
Add a user to an SNMP group	**snmp-agent usm-user v3** *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode des56** *priv-password*]] [**acl** *acl-number*]	Required
Set the maximum SNMP packet size for SNMP agent	**snmp-agent packet max-size** *byte-count*	Optional By default, the maximum SNMP packet size is 1,500 bytes.
Set the device engine ID	**snmp-agent local-engineid** *engineid*	Optional By default, the device engine ID is formed by appending device information to the enterprise number.

Operation	Command	Description
Create or update the view information	**snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree*	Optional By default, the view name is "ViewDefault" and OID is 1.

Note:

An S3600 Ethernet switch acts as the following to prevent attacks through unused sockets.

- Opening UDP port 161 (which is used by SNMP agents) and UDP port 1024 (which is used by SNMP-trap clients) only when SNMP is enabled.
- Closing UDP port 161 and UDP port 1024 when SNMP is disabled.

This function is achieved in the following way.

- Executing the **snmp-agent** command or any of the commands used to configure SNMP agent causes the SNMP agent being enabled and UDP port 161 and UDP port 1024 being opened.
- Executing the **undo snmp-agent** command causes UDP port 161 and UDP port 1024 being closed as well.

1.3 Configuring Trap

Trap messages refer to those sent by managed devices to the NMS without request. They are used to report some urgent and important events (for example, the rebooting of managed devices).

1.3.1 Configuration Prerequisites

Basic SNMP configuration is performed.

1.3.2 Configuration Tasks

Table 1-4 Configure Trap

Operation		Command	Description
Enter system view		**system-view**	—
Enable the device to send Trap packets		**snmp-agent trap enable** [**configuration** | **flash** | **ospf** [*process-id*] [*ospf-trap-list*] | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system** | **vrrp** [**authfailure** | **newmaster**]]	Optional By default, a port is enabled to send all types of Traps.
Enable the port to send Trap packets	Enter port view or interface view	**interface** *interface-type interface-number*	
	Enable the port or interface to send Trap packets	**enable snmp trap updown**	
	Quit to system view	**quit**	
Set the destination for Trap packets		**snmp-agent target-host trap address udp-domain** { *ip-address* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** {**authentication** | **privacy** }]	Required
Set the source address for Trap packets		**snmp-agent trap source** *interface-type interface-number*	Optional
Set the size of the queue used to hold the Traps to be sent to the destination host		**snmp-agent trap queue-size** *size*	Optional The default is 100.
Set the aging time for Trap packets		**snmp-agent trap life** *seconds*	Optional The default Trap packet aging time is 120 seconds.

1.4 Enabling Logging for Network Management

Table 1-5 Enable logging for network management

Operation	Command	Description
Enter system view	**system-view**	—
Enable logging for network management	**snmp-agent log** { **set-operation** | **get-operation** | **all** }	Optional; By default, SNMP logging is disabled.

Note:

- In the environment of a single device, use the **display logbuffer** command to view the log of the get and set operations requested by the NMS.
- In a fabric environment, use the **display logbuffer** command on the master device to view the log of the set operations requested by the NMS. Use the **display logbuffer** command on the devices receiving the get request to view the log of the get operations requested by the NMS.

1.5 Displaying SNMP

After the above configuration, you can execute the **display** command in any view to view the running status of SNMP, and to verify the configuration.

Table 1-6 Display SNMP

Operation	Command	Description
Display the SNMP information about the current device	**display snmp-agent sys-info** [**contact** | **location** | **version**]*	These commands can be executed in any view.
Display SNMP packet statistics	**display snmp-agent statistics**	
Display the engine ID of the current device	**display snmp-agent** { **local-engineid** | **remote-engineid** }	
Display group information about the device	**display snmp-agent group** [*group-name*]	
Display SNMP user information	**display snmp-agent usm-user** [**engineid** *engineid* | **username** *user-name* | **group** *group-name*]	
Display Trap list information	**display snmp-agent trap-list**	
Display the currently configured community name	**display snmp-agent community** [**read** | **write**]	
Display the currently configured MIB view	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]	

1.6 SNMP Configuration Example

1.6.1 SNMP Configuration Example

I. Network requirements

- An NMS and Switch A are connected through the Ethernet. The IP address of the NMS is 10.10.10.1 and that of the VLAN interface on Switch A is 10.10.10.2.
- Perform the following configuration on Switch A: setting the community name and access permission, administrator ID, contact and switch location, and enabling the switch to sent trap packets.

II. Network diagram

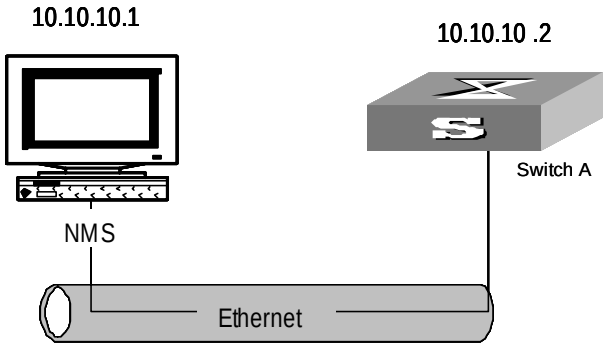


Figure 1-2 Network diagram for SNMP configuration

III. Network procedure

Set the community name, group name and user.

```
<H3C> system-view
[H3C] snmp-agent
[H3C] snmp-agent sys-info version all
[H3C] snmp-agent community write public
[H3C] snmp-agent mib-view include internet 1.3.6.1
[H3C] snmp-agent group v3 managev3group write-view internet
[H3C] snmp-agent usm-user v3 managev3user managev3group
```

Set the VLAN-interface 2 as the interface used by NMS. Add port Ethernet1/0/2, which is to be used for network management, to VLAN 2. Set the IP address of VLAN-interface 2 as 10.10.10.2.

```
[H3C] vlan 2
[H3C-vlan2] port Ethernet 1/0/2
[H3C-vlan2] quit
[H3C] interface Vlan-interface 2
[H3C-Vlan-interface2] ip address 10.10.10.2 255.255.255.0
[H3C-Vlan-interface2] quit
```

Enable the SNMP agent to send Trap packets to the NMS whose IP address is 10.10.10.1. The SNMP community name to be used is “public”.

```
[H3C] snmp-agent trap enable standard authentication
[H3C] snmp-agent trap enable standard coldstart
[H3C] snmp-agent trap enable standard linkup
[H3C] snmp-agent trap enable standard linkdown
[H3C] snmp-agent target-host trap address udp-domain 10.10.10.1 udp-port 5000
params securityname public
```

IV. Configuring the NMS

The S3600 series Ethernet switches support H3C's QuidView NMS. SNMPv3 adopts user name and password authentication. When you use H3C's QuidView NMS, you need to set user names and choose the security level in [Quidview Authentication Parameter]. For each security level, you need to set authorization mode, authorization password, encryption mode, encryption password, and so on. In addition, you need to set timeout time and maximum retry times.

You can query and configure an Ethernet switch through the NMS. For more information, refer to the corresponding manuals of H3C's NMS products.

Note:

Authentication-related configuration on an NMS must be consistent with that of the devices for the NMS to manage the devices successfully.

Chapter 2 RMON Configuration

2.1 Introduction to RMON

Remote monitoring (RMON) is a kind of management information base (MIB) defined by Internet Engineering Task Force (IETF). It is the most important enhancement made to MIB II standards. RMON is mainly used to monitor the data traffic across a network segment or even the entire network, and is currently a commonly used network management standard.

An RMON system comprises of two parts: the network management station (NMS) and the agents running on network devices. RMON agents operate on network monitors or network probes to collect and keep track of the statistics of the traffic across the network segments to which their ports connect, such as the total number of the packets on a network segment in a specific period of time and the total number of packets successfully sent to a specific host.

RMON is fully based on simple network management protocol (SNMP) architecture. As it is compatible with the current SNMP implementations, you can implement RMON without modifying the existing SNMP implementation. RMON enables SNMP to monitor remote network devices more effectively and actively, thus providing a satisfactory means of monitoring remote subnets. With RMON implemented, the communication traffic between NMS and agents can reduced, thus facilitating the management of large-scale internetworks.

2.1.1 Working Mechanism of RMON

RMON allows multiple monitors. It can collect data in the following two ways:

- Using the dedicated RMON probes. When an RMON system operates in this way, the NMS directly obtains management information from the RMON probes and controls the network resources. In this case, all information in the RMON MIB can be obtained.
- Embedding RMON agents into network devices (such as routers, switches and hubs) directly to make the latter capable of RMON probe functions. When an RMON system operates in this way, the NMS collects network management information by exchanging information with the SNMP agents using the basic SNMP commands. However, this way depends on device resources heavily and an NMS operating in this way can only obtain the information about these four groups (instead of all the information in the RMON MIB): alarm group, event group, history group, and statistics group.

An S3600 Ethernet switch implements RMON in the second way. With an RMON agent embedded in, an S3600 Ethernet switch can serve as a network device with the RMON

probe function. Through the RMON-capable SNMP agents running on the Ethernet switch, an NMS can obtain the information about the total traffic, error statistics and performance statistics of the network segments to which the ports of the managed network devices are connected. Thus, the NMS can further manage the networks.

2.1.2 Commonly Used RMON Groups

I. Event group

Event group is used to define the indexes of events and the processing methods of the events. The events defined in an event group are mainly used by entries in the alarm group and extended alarm group to trigger alarms.

You can specify a network device to act in one of the following ways in response to an event:

- Logging the event
- Sending trap messages to the NMS
- Logging the event and sending trap messages to the NMS
- No processing

II. Alarm group

RMON alarm management enables monitoring on specific alarm variables (such as the statistics of a port). When the value of a monitored variable exceeds the threshold, an alarm event is generated, which triggers the network device to act in the preset way. Events are defined in event groups.

With an alarm entry defined in an alarm group, a network device performs the following operations accordingly:

- Sampling the defined alarm variables periodically
- Comparing the samples with the threshold and triggering the corresponding events if the former exceed the latter

III. Extended alarm group

With extended alarm entry, you can perform operations on the samples of alarm variables and then compare the operation results with the thresholds, thus implement more flexible alarm functions.

With an extended alarm entry defined in an extended alarm group, the network devices perform the following operations accordingly:

- Sampling the alarm variables referenced in the defined extended alarm expressions periodically
- Performing operations on the samples according to the defined expressions
- Comparing the operation results with the thresholds and triggering corresponding events if the operation result exceeds the thresholds.

IV. History group

After a history group is configured, the Ethernet switch collects network statistics information periodically and stores the statistics information temporarily for later use. A history group can provide the history data of the statistics on network segment traffic, error packets, broadcast packets, and bandwidth utilization.

With the history data management function, you can configure network devices to collect history data, sample and store data of a specific port periodically.

V. Statistics group

Statistics group contains the statistics of each monitored port on a network device. An entry in a statistics group is an accumulated value counting from the time when the statistics group is created.

The statistics include the number of the following items: collisions, packets with cyclic redundancy check (CRC) errors, undersize (or oversize) packets, broadcast packets, multicast packets, and received bytes and packets.

With the RMON statistics management function, you can monitor the use of a port and make statistics on the errors occurred when the ports are being used.

Note:

It is required to configure the history group and the statistics group in port view because they are port-oriented RMON groups.

2.2 RMON Configuration

2.2.1 Prerequisites

Before performing RMON configuration, make sure the SNMP agents are correctly configured. For the information about SNMP agent configuration, refer to section 1.2 “Configuring Basic SNMP Functions”.

2.2.2 Configuring RMON

Table 2-1 Configure RMON

Operation	Command	Description
Enter system view	**system-view**	—
Add an event entry	**rmon event** *event-entry* [**description** *string*] { **log** | **trap** *trap-community* | **log-trap** *log-trapcommunity* | **none** } [**owner** *text*]	Optional
Add an alarm entry	**rmon alarm** *entry-number alarm-variable sampling-time* { **delta** | **absolute** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]	Optional Before adding an alarm entry, you need to use the **rmon event** command to define the event to be referenced by the alarm entry.
Add an extended alarm entry	**rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-timer* { **delta** | **absolute** | **changeratio** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]	Optional Before adding an extended alarm entry, you need to use the **rmon event** command to define the event to be referenced by the extended alarm entry.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add a history entry	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]	Optional
Add a statistics entry	**rmon statistics** *entry-number* [**owner** *text*]	Optional

Note:

- The **rmon alarm** and **rmon prialarm** commands take effect on existing nodes only.
- For each port, only one RMON statistics entry can be created. That is, if an RMON statistics entry is already created for a given port, you will fail to create another statistics entry with a different index for the same port.

2.3 Displaying RMON

After the above configuration, you can execute the **display** command in any view to display the RMON running status, and to verify the configuration.

Table 2-2 Display RMON

Operation	Command	Description
Display RMON statistics	**display rmon statistics** [*interface-type interface-number* | **unit** *unit-number*]	These commands can be executed in any view.
Display RMON history information	**display rmon history** [*interface-type interface-number* | **unit** *unit-number*]	
Display RMON alarm information	**display rmon alarm** [*entry-number*]	
Display extended RMON alarm information	**display rmon prialarm** [*prialarm-entry-number*]	
Display RMON events	**display rmon event** [*event-entry*]	
Display RMON event logs	**display rmon eventlog** [*event-entry*]	

2.4 RMON Configuration Example

I. Network requirements

- Ensure that the SNMP agents are correctly configured before performing RMON configuration.
- The switch to be tested has a configuration terminal connected to its console port and is connected to a remote NMS through Internet. Create an entry in the Ethernet statistics table to generate statistics on the Ethernet port performance for network management.

II. Network diagram

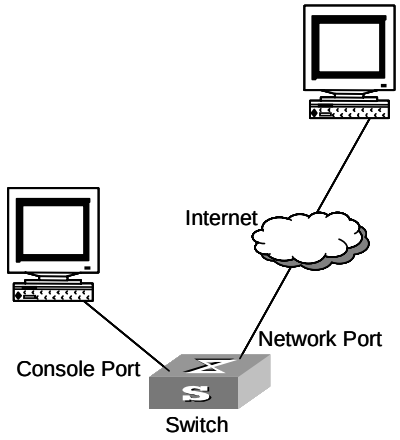


Figure 2-1 Network diagram for RMON configuration

III. Configuration procedures

Configure RMON.

```
<H3C> system-view
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] rmon statistics 1 owner user1-rmon
```

View RMON configuration.

```
[H3C-Ethernet1/0/1] display rmon statistics Ethernet1/0/1
Statistics entry 1 owned by user1-rmon is VALID.
  Interface : Ethernet1/0/1<ifIndex.4227626>
  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:
  64     : 0         ,  65-127  : 0         ,  128-255  : 0
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

Table of Contents

Chapter 1 NTP Configuration 1-1
1.1 Introduction to NTP 1-1
1.1.1 Applications of NTP 1-1
1.1.2 Implementation Principle of NTP 1-2
1.1.3 NTP Implementation Modes 1-4
1.2 Configuring NTP Implementation Modes 1-6
1.2.1 Configuration Prerequisites 1-6
1.2.2 Configuration Procedure 1-7
1.3 Configuring Access Control Right 1-9
1.4 Configuring NTP Authentication 1-9
1.4.1 Configuration Prerequisites 1-10
1.4.2 Configuration Procedure 1-10
1.5 Configuring Optional NTP Parameters 1-12
1.6 Displaying and Debugging NTP 1-13
1.7 Configuration Example 1-13
1.7.1 Configuring NTP Server Mode 1-13
1.7.2 Configuring NTP Peer Mode 1-15
1.7.3 Configuring NTP Broadcast Mode 1-16
1.7.4 Configuring NTP Multicast Mode 1-19
1.7.5 Configuring NTP Server Mode with Authentication 1-21

Chapter 1 NTP Configuration

1.1 Introduction to NTP

Network time protocol (NTP) is a time synchronization protocol defined in RFC1305. It is used for time synchronization between a set of distributed time servers and clients. NTP transmits packets through UDP port 123.

NTP is intended for time synchronization between all devices that have clocks in a network so that the clocks of all devices can keep consistent. Thus, the devices can provide multiple unified-time-based applications.

A local system running NTP can not only be synchronized by other clock sources, but also serve as a clock source to synchronize other clocks. Besides, it can synchronize, or be synchronized by other systems by exchanging NTP packets.

1.1.1 Applications of NTP

NTP is mainly applied to synchronizing the clocks of all devices in a network. For example:

- In network management, the analysis of the log information and debugging information collected from different devices is meaningful and valid only when network devices that generate the information adopts the same time.
- The billing system requires that the clocks of all network devices be consistent.
- Some functions, such as restarting all network devices in a network simultaneously require that they adopt the same time.
- When multiple systems cooperate to handle a rather complex transaction, they must adopt the same time to ensure a correct execution order.
- To perform incremental backup operations between a backup server and a host, you must make sure they adopt the same time.

As setting the system time manually in a network with many devices leads to a lot of workload and cannot ensure the accuracy, it is unfeasible for an administrator to perform the operation. However, an administrator can synchronize the clocks of devices in a network with required accuracy by performing NTP configuration.

NTP has the following advantages:

- Defining the accuracy of clocks by stratum to synchronize the clocks of all devices in a network quickly
- Supporting access control and MD5 authentication
- Sending protocol packets in unicast, multicast, or broadcast mode

Note:

- The clock stratum determines the accuracy, which ranges from 1 to 16. The stratum of a reference clock ranges from 1 to 15. The clock accuracy decreases as the stratum number increases. A stratum 16 clock is in the unsynchronized state and cannot serve as a reference clock.
- The local clock of an S3600 Ethernet switch cannot operate as a reference clock. It can serve as a NTP server only after synchronized.

1.1.2 Implementation Principle of NTP

Figure 1-1 shows the implementation principle of NTP.

Ethernet switch A (LS_A) is connected to Ethernet switch B (LS_B) through Ethernet ports. Both have their own system clocks, and they need to synchronize the clocks of each other through NTP. To help you to understand the implementation principle, we suppose that:

- Before the system clocks of LS_A and LS_B are synchronized, the clock of LS_A is set to 10:00:00 am, and the clock of LS_B is set to 11:00:00 am.
- LS_B serves as the NTP server, that is, the clock of LS_A will be synchronized to that of LS_B.
- It takes one second to transfer an NTP packet from LS_A to LS_B or from LS_A to LS_B.

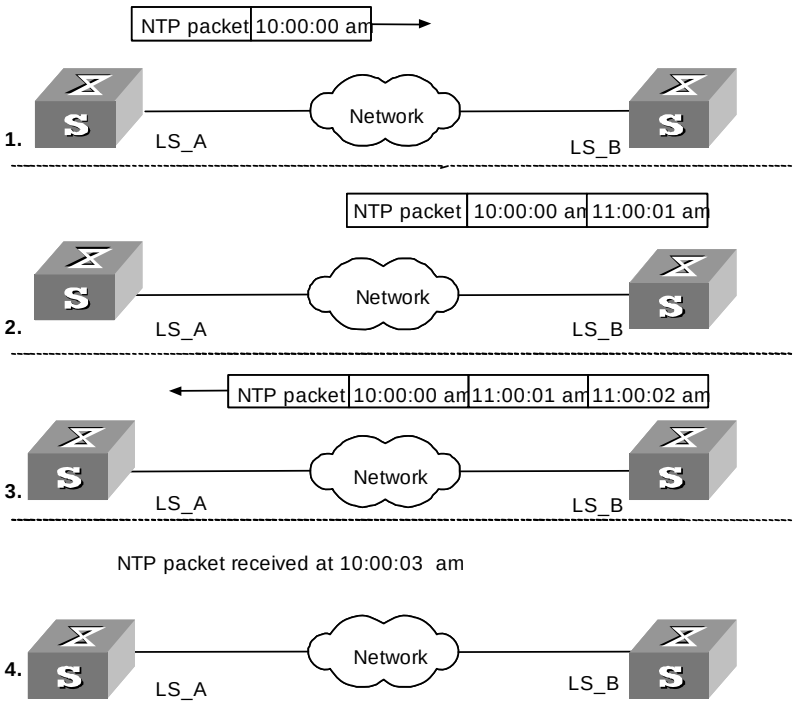


Figure 1-1 Implementation principle of NTP

The procedure of synchronizing the system clock is as follows:

- LS_A sends an NTP packet to LS_B, with a timestamp 10:00:00 am (T_1) identifying when it is sent.
- When the packet arrives at LS_B, LS_B inserts its own timestamp 11:00:01 am (T_2) into the packet.
- When the NTP packet leaves LS_B, LS_B inserts its own timestamp 11:00:02 am (T_3) into the packet.
- When receiving a response packet, LS_A inserts a new timestamp 10:00:03 am (T_4) into it.

At this time, LS_A has enough information to calculate the following two parameters:

- Delay for an NTP packet to make a round trip between LS_A and LS_B:

$$Delay = (T_4 - T_1) - (T_3 - T_2).$$

- Time offset of LS_A relative to LS_B:

$$Offset = ((T_2 - T_1) + (T_3 - T_4))/2.$$

LS_A can then set its own clock according to the above information to synchronize its clock to that of LS_B.

For detailed information, refer to RFC1305.

1.1.3 NTP Implementation Modes

According to the network structure and the position of the local Ethernet switch in the network, the local Ethernet switch can work in multiple NTP modes to synchronize the clock.

I. Client/server mode

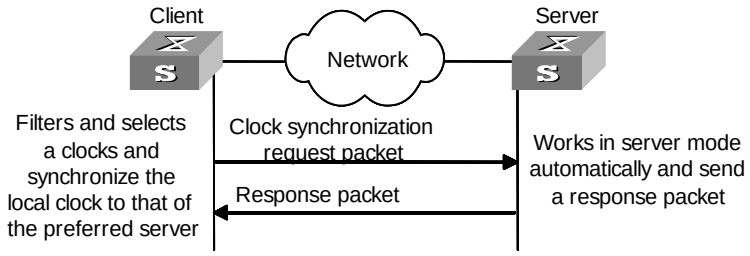


Figure 1-2 Client/sever mode

II. Peer mode

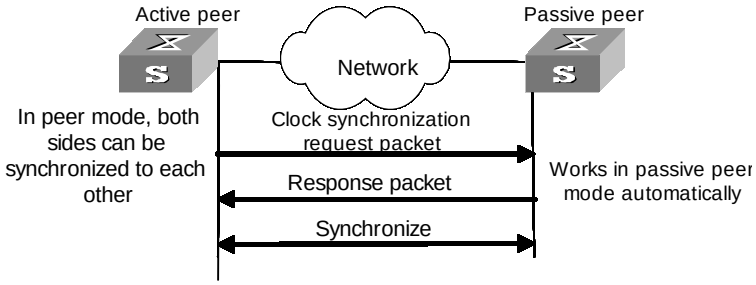


Figure 1-3 Peer mode

In the peer mode, the local S3600 Ethernet switch serves as the active peer and sends clock synchronization request packets first, while the remote server serves as the passive peer automatically.

If both of the peers have reference clocks, the one with a smaller stratum number is adopted.

III. Broadcast mode

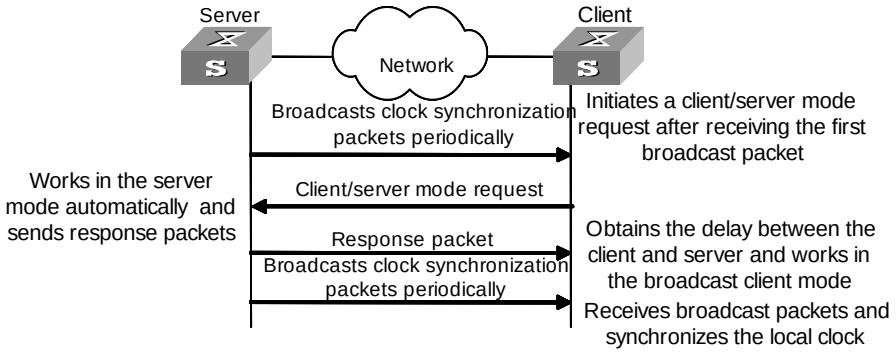


Figure 1-4 Broadcast mode

IV. Multicast mode

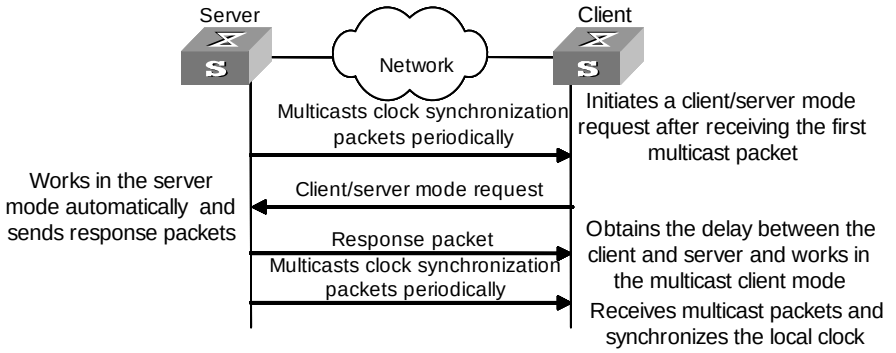


Figure 1-5 Multicast mode

Table 1-1 describes how the above mentioned NTP modes are implemented on S3600 series Ethernet switches.

Table 1-1 NTP implementation modes on S3600 series Ethernet switches

NTP implementation mode	Configuration on S3600 series switches
Client/server mode	Configure the local S3600 Ethernet switch to operate in the NTP server mode. In this mode, the remote server serves as the local time server, while the local switch serves as the client.
Peer mode	Configure the local S3600 switch to operate in NTP peer mode. In this mode, the remote server serves as the peer of the S3600 switch, and the local switch serves as the active peer.

NTP implementation mode	Configuration on S3600 series switches
Broadcast mode	• Configure the local S3600 Ethernet switch to operate in NTP broadcast server mode. In this mode, the local switch broadcasts NTP packets through the VLAN interface configured on the switch. • Configure the S3600 switch to operate in NTP broadcast client mode. In this mode, the local S3600 switch receives broadcast NTP packets through the VLAN interface configured on the switch.
Multicast mode	• Configure the local S3600 Ethernet switch to operate in NTP multicast server mode. In this mode, the local switch sends multicast NTP packets through the VLAN interface configured on the switch. • Configure the local S3600 Ethernet switch to operate in NTP multicast client mode. In this mode, the local switch receives multicast NTP packets through the VLAN interface configured on the switch.

Caution:

An S3600 Ethernet switch can operate in the NTP peer, NTP broadcast server, or NTP multicast server mode only after its clock is synchronized.

1.2 Configuring NTP Implementation Modes

An S3600 Ethernet switch can operate in one of the following NTP modes:

- NTP client mode
- NTP server mode
- NTP peer mode
- NTP broadcast server mode
- NTP broadcast client mode
- NTP multicast server mode
- NTP multicast client mode

1.2.1 Configuration Prerequisites

You need to perform configurations only on the client (or the active peer) when you want an S3600 Ethernet switch to operate in NTP server mode (or NTP peer mode). However, you need to perform configurations on both the server and client when you want the switch to operate in NTP broadcast mode or NTP multicast mode.

1.2.2 Configuration Procedure

Table 1-2 Configure NTP implementation modes

Operation	Command	Description
Enter system view	**system-view**	—
Configure the switch to operate in NTP client mode	**ntp-service unicast-server** { *remote-ip* | *server-name* } [**authentication-keyid** *key-id* | **priority** | **source-interface Vlan-interface** *vlan-id* | **version** *number*]*	Optional By default, no Ethernet switch operates in NTP client mode.
Configure the switch to operate in NTP peer mode	**ntp-service unicast-peer** { *remote-ip* | *peer-name* } [**authentication-keyid** *key-id* | **priority** | **source-interface Vlan-interface** *vlan-id* | **version** *number*]*	Optional By default, no Ethernet switch operates in NTP peer mode.
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Configure the switch to operate in the NTP broadcast client mode	**ntp-service broadcast-client**	Optional By default, no Ethernet switch operates in NTP broadcast client mode.
Configure the switch to operate in NTP broadcast server mode	**ntp-service broadcast-server** [**authentication-keyid** *key-id* | **version** *number*]*	Optional By default, no Ethernet switch operates in NTP broadcast server mode.
Configure the switch to operate in NTP multicast client mode	**ntp-service multicast-client** [*ip-address*]	Optional By default, no Ethernet switch operates in NTP multicast client mode.
Configure the switch to operate in NTP multicast server mode	**ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*]*	Optional By default, no Ethernet switch operates in NTP multicast server mode.

Note:

To reduce the risk of being attacked by malicious users against opened socket and enhance switch security, the S3600 series Ethernet switches provide the following functions, so that a socket is opened only when it is needed:

- Opening UDP port 123 (used for NTP) when NTP is enabled;
- Close UDP port 123 when NTP is disabled.

The preceding functions are implemented as follows:

- When you enable NTP by using the **ntp-service unicast-server**, **ntp-service unicast-peer**, **ntp-service broadcast-client**, **ntp-service broadcast-server**, **ntp-service multicast-client**, or **ntp-service multicast-server** command, UDP port 123 is opened at the same time.
- When you disable NTP from operating in any modes by using the **undo** forms of the preceding six commands, UDP port 123 is closed at the same time.

I. NTP client mode

- The remote server specified by the *remote-ip* or *server-name* argument serves as the NTP server. The local S3600 Ethernet switch serves as the client. The clock of the client is synchronized to the NTP server, while the clock of the NTP server is not synchronized to the client.
- The IP address specified by the *remote-ip* argument cannot be a broadcast address, a multicast address, or the IP address used by the local reference clock.

II. NTP peer mode

- The remote server specified by the *remote-ip* or *peer-name* argument serves as the peer of the local Ethernet switch, and the local Ethernet switch operates in the active peer mode. The clock of the local switch can be synchronized to the remote server or used to synchronize the clock of the remote server.
- The IP address specified by the *remote-ip* argument cannot be a broadcast address, a multicast address, or the IP address used by the local reference clock.

III. NTP broadcast server mode

When an S3600 Ethernet switch operates in NTP broadcast server mode, it broadcasts clock synchronization packets periodically. The devices in NTP broadcast client mode will respond to these packets and start the clock synchronization process.

IV. NTP multicast server mode

When an S3600 Ethernet switch operates in NTP multicast server mode, it multicasts clock synchronization packets periodically. The devices in the NTP multicast client mode will respond to these packets and start the clock synchronization process. The switch operating in this mode can support up to 1,024 multicast clients.

Note:

- The total number of the servers and peers configured for a switch is up to 128.
- After the configuration, an S3600 Ethernet switch does not establish connections with peers if it operates in NTP server mode. Whereas if it operates in any of the other modes, it establishes connections with peers.
- If an S3600 Ethernet switch operates in passive peer mode, NTP broadcast client mode, or NTP multicast client mode, it establishes connections with peers dynamically. If it operates in any of the other modes, it establishes connections with peers statically.

1.3 Configuring Access Control Right

The access control right to the NTP server only provides a minimal degree of security measure. A more secure way is to perform identity authentication.

The right of an access request received by the NTP server is matched from the highest to the lowest in order of **peer**, **server**, **synchronization**, and **query**.

Table 1-3 Configure the access control right to the local NTP server

Operation	Command	Description
Enter system view	**system-view**	—
Configure the access control right to the local NTP server	**ntp-service access** { **peer** | **server** | **synchronization** | **query** } *acl-number*	Optional By default, the access control right to the local NTP server is **peer**.

1.4 Configuring NTP Authentication

In networks with higher security requirements, the NTP authentication function must be enabled to run NTP. Through password authentication on the client and the server, the client is synchronized only to the server that passes the authentication. This improves network security.

1.4.1 Configuration Prerequisites

NTP authentication configuration involves:

- Configuring NTP authentication on the client
- Configuring NTP authentication on the server

Observe the following principles when configuring NTP authentication:

- If the NTP authentication function is not enabled on the client, the client can be synchronized to a server no matter whether the NTP authentication function is enabled on the server (assuming that other related configurations are performed).
- You need to couple the NTP authentication with a trusted key.
- Configurations on the server and the client must be consistent.
- The client with the NTP authentication function enabled is only synchronized to the server that provides a trusted key.

1.4.2 Configuration Procedure

I. Configuring NTP authentication on the client

Table 1-4 Configure NTP authentication on the client

Operation	Command	Description
Enter system view	**system-view**	—
Enable the NTP authentication function globally	**ntp-service authentication enable**	Required By default, the NTP authentication function is disabled.
Configure the NTP authentication key	**ntp-service authentication-keyid** *key-id* **authentication-model md5** *value*	Required By default, no NTP authentication key is configured.
Configure the specified key to be a trusted key	**ntp-service reliable authentication-keyid** *key-id*	Required By default, no trusted key is configured.
Associate the specified key with the corresponding NTP server	NTP client mode: **ntp-service unicast-server** { *remote-ip* | *server-name* } **authentication-keyid** *key-id*	• In NTP client mode and NTP peer mode, you need to associate the specified key with the corresponding NTP server on the client. • You can associate the NTP server with the authentication key while configuring NTP mode. You can also use this command to associate them after configuring NTP mode.
	Peer mode: **ntp-service unicast-peer** { *remote-ip* | *peer-name* } **authentication-keyid** *key-id*	

Note:

- NTP authentication requires that the authentication keys configured for the server and the client are the same. Besides, the authentication keys must be trusted keys. Otherwise, the client cannot be synchronized with the server.
- In NTP server mode and NTP peer mode, you need to associate the specified key with the corresponding NTP server (active peer) on the client (passive peer). In these two modes, multiple servers (active peers) may be configured for a client/passive peer, and therefore, the authentication key is required to determine which server the client is synchronized to.

II. Configuring NTP authentication on the server

Table 1-5 Configure NTP authentication on the server

Operation	Command	Description
Enter system view	**system-view**	—
Enable NTP authentication	**ntp-service authentication enable**	Required By default, the NTP authentication function is disabled.
Configure an NTP authentication key	**ntp-service authentication-keyid** *key-id* **authentication-mode md5** *value*	Required By default, no NTP authentication key is configured.
Configure the specified key to be a trusted key	**ntp-service reliable authentication-keyid** *key-id*	Required By default, no trusted authentication key is configured.
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Associate the specified key with the corresponding NTP server	Broadcast server mode: **ntp-service broadcast-server authentication-keyid** *key-id*	• In NTP broadcast server mode and NTP multicast server mode, you need to associate the specified key with the corresponding NTP server on the server • You can associate an NTP server with an authentication key while configuring NTP mode. You can also use this command to associate them after configuring the NTP mode.
	Multicast server mode: **ntp-service multicast-server authentication-keyid** *key-id*	

Note:

The procedure for configuring NTP authentication on the server is the same as that on the client. Besides, the client and the server must be configured with the same authentication key.

1.5 Configuring Optional NTP Parameters

Optional NTP parameters are:

- Local VLAN interface that sends NTP packets
- Number of dynamic sessions that can be established locally
- VLAN interface disabled from receiving NTP packets

Table 1-6 Configure optional NTP parameters

Operation	Command	Description
Enter system view	**system-view**	—
Configure a local interface that sends NTP packets	**ntp-service source-interface Vlan-interface** *vlan-id*	Optional
Configure the number of sessions that can be established locally	**ntp-service max-dynamic-sessions** *number*	Optional By default, up to 100 dynamic sessions can be established locally.
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Disable an interface from receiving NTP packets	**ntp-service in-interface disable**	Optional By default, a VLAN interface receives NTP packets.

Caution:

- If a sending interface is specified in the **ntp-service unicast-server** command or the **ntp-service unicast-peer** command, the source IP address of an NTP packet is the address of this interface.
- Dynamic connections can be established when a switch operates in passive peer mode, NTP broadcast client mode, or NTP multicast client mode. In other modes, the connections established are static.

1.6 Displaying and Debugging NTP

After the above configurations, you can execute **display** commands in any view to display the running status of switch, and verify the effect of the configurations.

Table 1-7 Display and debug NTP

Operation	Command	Description
Display the status of NTP services	**display ntp-service status**	The **display** commands can be executed in any view
Display the information about the sessions maintained by NTP	**display ntp-service sessions** [**verbose**]	
Display the brief information about NTP servers along the path from the local device to the reference clock source	**display ntp-service trace**	

1.7 Configuration Example

1.7.1 Configuring NTP Server Mode

I. Network requirements

The local clock of H3C1 is set to the NTP master clock, with a stratum level of 2.

Note:

H3C1 is a switch that allows the local clock to serve as the NTP master clock.

An S3600 Ethernet switch considers H3C1 as the NTP server and operates in client mode, while H3C1 operates in server mode automatically.

II. Network diagram

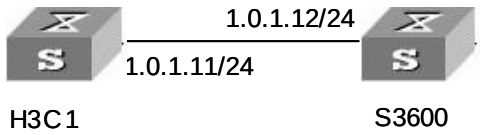


Figure 1-6 Network diagram for the NTP server mode configuration

III. Configuration procedure

Perform the following configurations on the S3600 switch.

View the NTP status of the S3600 switch before synchronization.

```
<S3600> display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 60.0002 Hz
 Actual frequency: 60.0002 Hz
 Clock precision: 2^18
 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)
```

Set H3C1 to the NTP server of the S3600 switch.

```
<S3600> system-view
[S3600] ntp-service unicast-server 1.0.1.11
```

(After the above configurations, the S3600 switch is synchronized to H3C1.) View the NTP status of the S3600 switch.

```
[S3600] 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: 2^18
 Clock offset: 0.0000 ms
 Root delay: 9.54 ms
 Root dispersion: 26.42 ms
 Peer dispersion: 10.96 ms
 Reference time: 07:05:43.263 UTC Apr 25 2006(C7F848C7.438348F5)
```

The above output information indicates that the S3600 switch is synchronized to H3C1, and the stratum level of its clock is 3, one level lower than that of H3C1.

View the information about NTP sessions of the S3600 switch. (You can see that the S3600 switch establishes a connection with H3C1.)

```
[S3600] display ntp-service sessions
     source        reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345]1.0.1.11    127.127.1.0     2     255   64   39    0.0    9.5    5.1
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

1.7.2 Configuring NTP Peer Mode

I. Network requirements

The local clock of H3C2 is set to the NTP master clock, with the clock stratum level of 2.

An S3600 Ethernet switch considers H3C2 as the NTP server and serves as the client, while H3C2 operates in server mode automatically. In addition, H3C3 considers the S3600 Ethernet switch as its peer.

Note:

This example assumes that:

- H3C2 is a switch that allows its local clock to be the master clock.
- H3C3 is a switch that allows its local clock to be the master clock and the stratum level of its clock is 1.

II. Network diagram

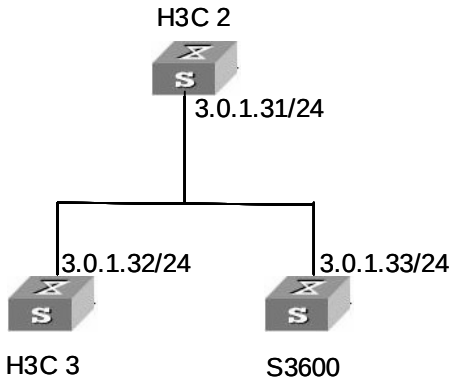


Figure 1-7 Network diagram for NTP peer mode configuration

III. Configuration procedure

1) Configure the S3600 series switch.

Set H3C2 to the NTP server.

```
<S3600> system-view
[S3600] ntp-service unicast-server 3.0.1.31
```

2) Configure H3C3 (after the S3600 Ethernet switch is synchronized to H3C2).

Enter system view.

```
<H3C3> system-view
[H3C3]
```

Set the S3600 Ethernet switch to the peer of H3C3.

```
[H3C3] ntp-service unicast-peer 3.0.1.33
```

The S3600 Ethernet switch and H3C3 are a pair of peers. H3C3 operates in active peer mode, while the S3600 Ethernet switch operates in passive peer mode. Because the stratum level of the local clock of H3C3 is 1, and that of the S3600 Ethernet switch is 3, the S3600 Ethernet switch is synchronized to H3C3.

View the status of the S3600 Ethernet switch after synchronization.

```
[S3600] display ntp-service status
 Clock status: synchronized
 Clock stratum: 2
 Reference clock ID: 3.0.1.32
 Nominal frequency: 60.0002 Hz
 Actual frequency: 60.0002 Hz
 Clock precision: 2^18
 Clock offset: 0.0000 ms
 Root delay: 31.28 ms
 Root dispersion: 0.08 ms
 Peer dispersion: 27.31 ms
 Reference time: 07:07:59.823 UTC Apr 25 2006(C7F8494F.D2E568A5)
```

The output information indicates that the S3600 Ethernet switch is synchronized to H3C3 and the stratum level of its local clock is 2, one level lower than that H3C3.

View the information about the NTP sessions of the S3600 Ethernet switch (you can see that a connection is established between the S3600 Ethernet switch and H3C3).

```
[S3600] display ntp-service sessions
     source        reference       stra reach poll  now offset  delay disper
**************************************************************************
[2]3.0.1.32       LOCL            1      14   64   60   -1.0    0.0    1.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

1.7.3 Configuring NTP Broadcast Mode

I. Network requirements

The local clock of H3C3 is set to the NTP master clock, with a stratum level of 2. NTP packets are broadcast through Vlan-interface2.

Configure S3600-1 and S3600-2 to listen to broadcast packets through their own Vlan-interface2.

Note:

This example assumes that H3C3 is a switch that supports the local clock being the master clock.

II. Network diagram

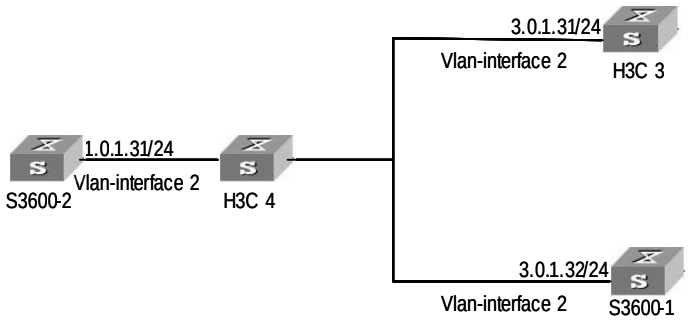


Figure 1-8 Network diagram for the NTP broadcast mode configuration

III. Configuration procedure

1) Configure H3C3.

Enter system view.

```
<H3C3> system-view
[H3C3]
```

Enter Vlan-interface2 view.

```
[H3C3] interface Vlan-interface 2
[H3C3-Vlan-interface2]
```

Set H3C3 to the broadcast server, which sends broadcast packets through Vlan-interface2.

```
[H3C3-Vlan-interface2] ntp-service broadcast-server
```

2) Configure S3600-1.

Enter system view.

```
<S3600-1> system-view
[S3600-1]
```

Enter Vlan-interface2 view.

```
[S3600-1] interface Vlan-interface 2
[S3600-1-Vlan-interface2]
```

Set S3600-1 to a broadcast client.

```
[S3600-1-Vlan-interface2] ntp-service broadcast-client
```

3) Configure S3600-2

Enter system view.

```
<S3600-2> system-view
[S3600-2]
```

Enter Vlan-interface2 view.

```
[S3600-2] interface Vlan-interface 2
[S3600-2-Vlan-interface2]
```

Set S3600-2 to a broadcast client.

```
[S3600-2-Vlan-interface2] ntp-service broadcast-client
```

After the above configurations, S3600-1 and S3600-2 will listen to broadcast packets through their own Vlan-interface2, and H3C3 will send broadcast packets through Vlan-interface2. Because S3600-2 and H3C3 do not share the same network segment, S3600-2 cannot receive broadcast packets from H3C3, while S3600-1 is synchronized to H3C3 after receiving broadcast packets from H3C3.

View the status of S3600-1 after synchronization.

```
[S3600-1] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 60.0002 Hz
 Actual frequency: 60.0002 Hz
 Clock precision: 2^18
 Clock offset: -9.1060 ms
 Root delay: 15.84 ms
 Root dispersion: 3.52 ms
 Peer dispersion: 29.62 ms
 Reference time: 07:15:14.403 UTC Apr 25 2006(C7F84B02.6735F3D7)
```

The output information indicates that S3600-1 is synchronized to H3C3, with the clock stratum level of 3, one level lower than that of H3C3.

View the information about the NTP sessions of S3600-1 and you can see that a connection is established between S3600-1 and H3C3.

```
[S3600-1] display ntp-service sessions
    source         reference      stra reach poll  now offset   delay disper
**************************************************************************
[1]3.0.1.31       127.127.1.0     2       14   64   60   -1.0    0.0    1.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

1.7.4 Configuring NTP Multicast Mode

I. Network requirements

The local clock of H3C3 is set to the NTP master clock, with a clock stratum level of 2. H3C3 advertises multicast packets through Vlan-interface2.

S3600-1 and S3600-2 respectively listen to multicast packets through their own Vlan-interface2.

Note:

This example assumes that H3C3 is a switch that supports the local clock being the master clock.

II. Network diagram

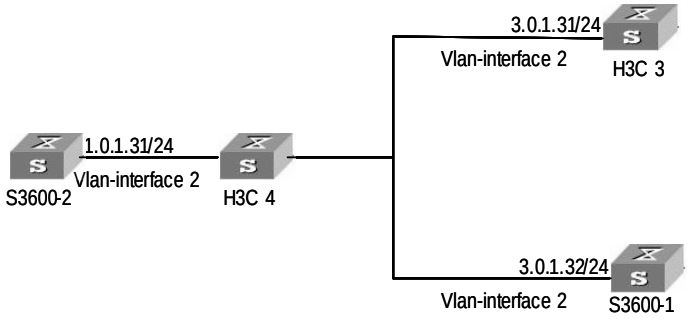


Figure 1-9 Network diagram for NTP multicast mode configuration

III. Configuration procedure

1) Configure H3C3.

Enter system view.

```
<H3C3> system-view
[H3C3]
```

Enter VLAN-interface2 view.

```
[H3C3] interface Vlan-interface 2
```

Set H3C3 to a multicast server.

```
[H3C3-Vlan-interface2] ntp-service multicast-server
```

2) Configure S3600-1.

Enter system view.

```
<S3600-1> system-view
```

```
[S3600-1]
```

Enter Vlan-interface2 view.

```
[S3600-1] interface Vlan-interface 2
```

Set S3600-1 to a multicast client.

```
[S3600-1-Vlan-interface2] ntp-service multicast-client
```

3) Configure S3600-2.

Enter system view.

```
<S3600-2> system-view
[S3600-2]
```

Enter Vlan-interface2 view.

```
[S3600-2] interface Vlan-interface 2
```

Set S3600-2 to a multicast client.

```
[S3600-2-Vlan-interface2] ntp-service multicast-client
```

After the above configurations, S3600-1 and S3600-2 respectively listen to multicast packets through their own Vlan-interface2, and H3C3 advertises multicast packets through Vlan-interface2. Because S3600-2 and S3600-3 do not share the same network segment, S3600-2 cannot receive multicast packets from H3C3, while S3600-1 is synchronized to H3C3 after receiving multicast packets from H3C3.

View the status of S3600-1 after synchronization.

```
[S3600-1] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 60.0002 Hz
 Actual frequency: 60.0002 Hz
 Clock precision: 2^18
 Clock offset: 0.0000 ms
 Root delay: 63.21 ms
 Root dispersion: 0.30 ms
 Peer dispersion: 46.13 ms
 Reference time: 07:18:32.952 UTC Apr 25 2006(C7F84BC8.F3BBD7B2)
```

The output information indicates that S3600-1 is synchronized to H3C3, with a clock stratum level of 3, one stratum level lower than that H3C3.

View the information about the NTP sessions of S3600-1 (You can see that a connection is established between S3600-1 and H3C3).

```
[S3600-1] display ntp-service sessions
   source        reference       stra reach poll  now offset  delay disper
**************************************************************************
```

```
[1]3.0.1.31     127.127.1.0      2        1   64   20    0.0   15.4    0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

1.7.5 Configuring NTP Server Mode with Authentication

I. Network requirements

The local clock of H3C1 is set to the NTP master clock, with a clock stratum level of 2.

An S3600 Ethernet switch considers H3C1 as the NTP server and operates in client mode, while H3C1 operates in server mode automatically. In addition, the NTP authentication function is enabled on both sides.

Note:

This example assumes that H3C1 is a switch that supports the local clock being the NTP master clock.

II. Network diagram

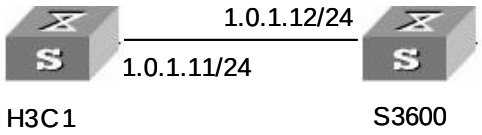


Figure 1-10 Network diagram for NTP se rver mode with authentication configuration

III. Configuration procedure

1) Configure the S3600 Ethernet switch.

Enter system view.

```
<S3600> system-view
[S3600]
```

Set H3C1 to the NTP server.

```
[S3600] ntp-service unicast-server 1.0.1.11
```

Enable the NTP authentication function.

```
[S3600] ntp-service authentication enable
```

Configure an MD5 authentication key, with the key ID being **42** and the key being **aNiceKey**.

```
[S3600] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

Specify the key as a trusted key.

```
[S3600] ntp-service reliable authentication-keyid 42
```

```
[S3600] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

After the above configurations, S3600 is ready to synchronize with H3C1. Because the NTP authentication function is not enabled on H3C1, S3600 will fail to be synchronized to H3C1.

To synchronize the S3600 Ethernet switch, you need to perform the following configurations on H3C1.

Enable the NTP authentication function on H3C1.

```
[H3C1] system-view
[H3C1] ntp-service authentication enable
```

Configure an MD5 authentication key, with the key ID being **42** and the key being **aNiceKey**.

```
[H3C1] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

Specify the key as a trusted key.

```
[H3C1] ntp-service reliable authentication-keyid 42
```

(After the above configurations, the S3600 Ethernet switch can be synchronized to H3C1.) View the status of S3600 after synchronization.

```
[S3600] 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: 2^18
 Clock offset: 0.0000 ms
 Root delay: 9.54 ms
 Root dispersion: 26.42 ms
 Peer dispersion: 10.96 ms
 Reference time: 07:05:43.263 UTC Apr 25 2006(C7F848C7.438348F5)
```

The output information indicates that S3600 is synchronized to H3C1, with a clock stratum level of 3, one stratum level lower than that H3C1.

View the information about NTP sessions of S3600 (You can see that a connection is established between S3600 and H3C1).

```
<S3600> display ntp-service sessions
     source        reference       stra reach poll  now offset  delay disper
**************************************************************************
    [5]1.0.1.11    127.127.1.0     2    255   64   39    0.0    9.5    5.1
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

Table of Contents

Chapter 1 SSH Terminal Service 1-1
1.1 SSH Terminal Service 1-1
1.1.1 Introduction to SSH 1-1
1.1.2 SSH Server Configuration 1-3
1.1.3 Configuring the SSH Client 1-11
1.1.4 Configuring the Device as an SSH Client 1-19
1.1.5 Displaying SSH Configuration 1-21
1.1.6 SSH Server Configuration Example 1-22
1.1.7 SSH Client Configuration Example 1-25
Chapter 2 SFTP Service 2-1
2.1 SFTP Service 2-1
2.1.1 Introduction to SFTP 2-1
2.1.2 SFTP Server Configuration 2-1
2.1.3 SFTP Client Configuration 2-2
2.1.4 SFTP Configuration Example 2-6

Chapter 1 SSH Terminal Service

1.1 SSH Terminal Service

1.1.1 Introduction to SSH

Secure shell (SSH) provides secure communication and powerful authentication for remote user login to a switch over an insecure network, thus preventing assaults such as IP address spoofing, plain-text password interception.

Acting as an SSH server, a switch allows for the connections of multiple SSH clients. Through SSH Client, a user can establish a connection to a switch or UNIX host running SSH Server.

Figure 1-1 and Figure 1-2 shows two ways to establish SSH connection between client and server.

- Establishing SSH connection through a LAN

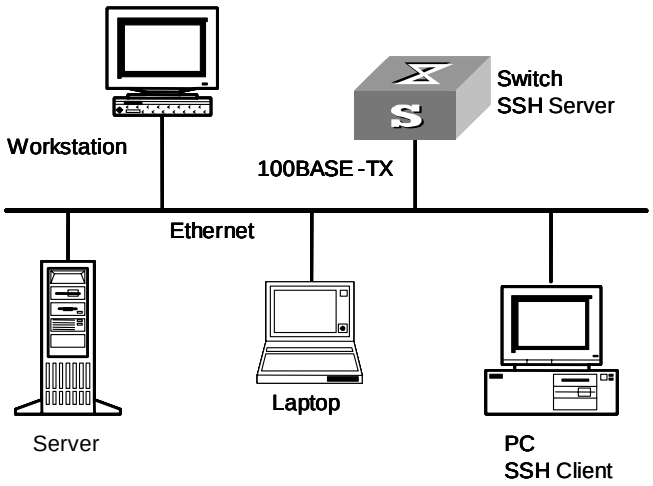


Figure 1-1 Establish SSH connection through a LAN

- Establishing SSH connection through a WAN

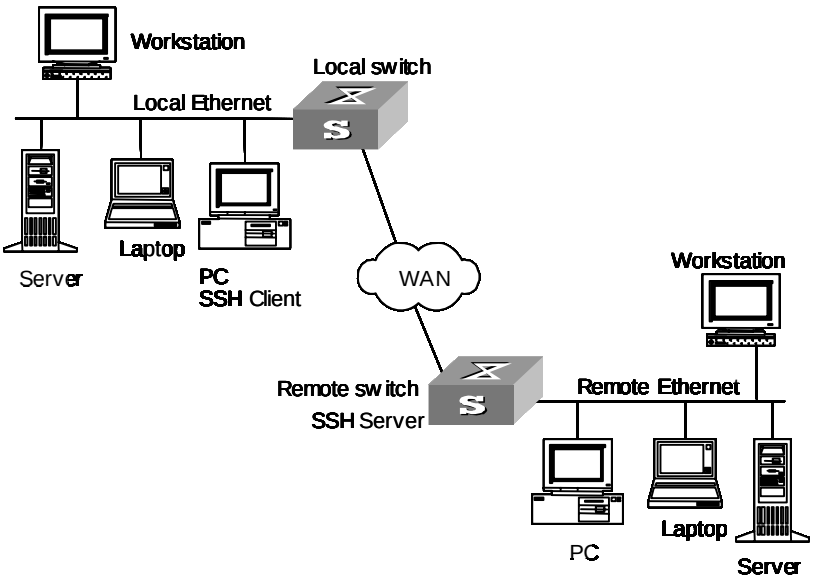


Figure 1-2 Establish SSH connection through a WAN

Note:

At present, the device supports two SSH versions: SSH2 and SSH1. Unless otherwise noted, SSH refers to SSH2 throughout this document.

The communication process between a SSH client and server goes through the following five stages.

1) Version negotiation stage:

- The client sends a TCP connection request to the server.
- When a TCP connection is established, the two ends begin to negotiate an SSH version.
- If they get a successful negotiation, they go to the key negotiation stage. Otherwise the server terminates the TCP connection.

2) Key and algorithm negotiation stage:

- The server and the client send key algorithm negotiation packets to each other, which include the supported server-side public key algorithm list, encryption algorithm list, MAC algorithm list, and compression algorithm list.
- Based on the received algorithm negotiation packets, the server and the client figure out the algorithms to be used.
- The server and the client use the DH key exchange algorithm and parameters such as the host key pair to generate the session key and session ID.

Through the above steps, the server and the client get the same session key, which is to be used to encrypt and decrypt data exchanged between the server and the client later. The server and the client use session ID in the authentication stage.

3) Authentication negotiation stage:

- The client sends its username information to the server.
- The server starts to authenticate the user. If the user is configured as having no authentication on the server, the following step is skipped and the session request stage starts directly.
- The server authenticates the user in some way (see the following note), till the authentication succeeds or the connection is terminated due to authentication timeout.

Note:

SSH provides two kinds of authentication: password authentication and RSA authentication.

(1) Password authentication works as follows:

- The client sends the username and password to the server.
- The server compares the received username and password against those configured locally. The user passes the authentication if the server finds a match for both username and password.

(2) RSA authentication works as follows:

- Configure the RSA public key of the client at the server.
- The client sends the member module of its RSA public key to the server.
- The server checks the validity of the member module. If it is valid, the server generates a random number, which is sent to the client after being encrypted with RSA public key of the client.
- Both the server and the client calculate authentication data by using the random number and session ID.
- The client sends the authentication data it calculates to the server.
- The server compares the received authentication data with the authentication data on itself. If they are identical, the authentication succeeds.

---

4) Session request stage. The client sends a session request to the server, which processes the request and establish a session.
5) Interactive session stage. Both ends exchange data till the session ends.

1.1.2 SSH Server Configuration

The following table describes SSH Server configuration tasks.

Table 1-1 SSH2.0 Server configuration tasks

Operation	Command	Related section
Configure user interface(s) to support specified protocol(s)	**protocol inbound**	Section “Configuring user interface(s) to support specified protocol(s)"
Generate local RSA key pairs	**rsa local-key-pair create**	Section “Generating or destroying local RSA key pairs"
Destroy local RSA key pairs	**rsa local-key-pair destroy**	
Create an SSH user	**ssh user** *username*	Section “Create an SSH user”
Specify a default authentication type for SSH users	**ssh authentication-type default**	Section”Configuring authentication type for a user"
Configure authentication type for an SSH user	**ssh user** *username* **authentication-type**	
Set SSH authentication timeout time	**ssh server timeout**	Section “Configuring SSH management
Set SSH authentication retry times	**ssh server authentication-retries**	
Set server key update interval	**ssh server rekey-interval**	
Configure SSH server to be compatible with SSH1.x clients	**ssh server compatible-ssh1x enable**	
Configure a client public key for an SSH user	**ssh user** *username* **assign rsa-key** *keyname*	Section “Configuring a client public key for a user"

I. Configuring user interface(s) to support specified protocol(s)

Table 1-2 Configure user interface(s) to support specified protocol(s)

Operation	Command	Description
Enter system view	**system-view**	—
Enter the view of one or multiple user interfaces	**user-interface** [*type-keyword*] *number* [*ending-number*]	Required
Set the login authentication method	**authentication-mode scheme** [**command-authorization**]	Required

Operation	Command	Description
Configure the user interface(s) to support specified protocol(s)	**protocol inbound** { **all** |**ssh** | **telnet** }	Optional By default, both Telnet and SSH are supported.

Caution:

- If you have configured a user interface to support SSH protocol, to ensure a successful login to the user interface, you must configure AAA authentication for the user interface by using the **authentication-mode scheme** command.
- For a user interface, if you have executed the **authentication-mode password** or **authentication-mode none** command, the **protocol inbound ssh** command cannot be executed; if you have executed the **protocol inbound ssh** command, neither of the **authentication-mode password** and **authentication-mode none** commands can be executed.

II. Generating or destroying local RSA key pairs

This configuration task is used to generate or destroy the server's RSA key pairs, which are named in the format of switch name plus "_Host", and switch name plus "_Server", for example, H3C_Host and H3C_Server.

After you issue the **rsa local-key-pair create** command, the system prompts you to input a key length.

- In SSH1.x, the key length is in the range of 512 to 2,048 (bits).
- In SSH2.0, the key length is in the range of 1024 to 2048 (bits). To keep compatible with SSH1.x, SSH2.0 allows client keys to be 512 to 2,048 bits in length. But the server's key length must not be shorter than 1,024 bits; otherwise, clients cannot be authenticated.

Table 1-3 Generate or destroy local RSA key pairs

Operation	Command	Description
Enter system view	**system-view**	—
Generate local RSA key pairs	**rsa local-key-pair create**	Required
Destroy local RSA key pairs	**rsa local-key-pair destroy**	Optional

Caution:

- For a successful SSH login, you must first generate the RSA key pairs of the server.
- You just need to execute the **rsa local-key-pair create** command once, and need not execute the command again after the system is rebooted.
- If you re-execute the **rsa local-key-pair create** command, the system will ask whether you want to replace the original key pairs with new ones.
- For a fabric made up of multiple devices, you need to execute the **rsa local-key-pair create** command on the management device to ensure that all devices in the fabric have the same local RSA key pairs.

Note:

After the **rsa local-key-pair create** command is executed, you can execute the **display rsa local-key-pair public** command, which will display:

- Two public keys (in H3C_Host and H3C_Server) if the switch works in SSH1.x-compatible mode.
- Only one public key (in H3C_Host) if the switch works in SSH2.0 mode.

III. Create an SSH user

Table 1-4 Create an SSH user

Operation	Command	Description
Enter system view	**system-view**	—
Create an SSH user	**ssh user** *username*	Required

For an SSH user created by using this command, if you do not specify an authentication type by using the **ssh user authentication-type** command for this user, this SSH user adopts the default authentication type. On the other hand, if the default authentication type is not specified, you need to specify an authentication type for this SSH user.

IV. Configuring authentication type for a user

For a new user, you must specify the authentication type. Otherwise, the user cannot access the switch.

Table 1-5 Configure authentication type for a user

Operation	Command	Description
Enter system view	**system-view**	—
Specify a default authentication type for SSH users	**ssh authentication-type default** { **password** | **rsa** | **password-publickey** | **all** }	At least one required; By default, no authentication type is specified for an SSH user, and the user can not access the switch.
Configure authentication type for an SSH user	**ssh user** *username* **authentication-type** { **password** | **password-publickey** | **rsa**| **all** }	

Note that:

- The **ssh authentication-type default** command is used to configure the default authentication type for all SSH users.
- The **ssh user** *username* **authentication-type** command is used to configure an authentication type for a specific SSH user.
- When both commands are configured with different authentication types, for the specific user (user specified by the *username* argument), the authentication type specified by the **ssh user** *username* **authentication-type** command will take effect instead of that specified for all SSH users.

Caution:

- If **RSA** authentication type is configured for a user, the RSA public key of the client user must be configured on the switch.
- By default, no authentication type is specified for a new user, and the new user cannot access the switch.
- For the **password-publickey** authentication type: SSH1 client users can access the switch as long as they pass any of the two kinds of authentications. SSH2 client users can access the switch only when they pass both kinds of authentications.
- For the **password** authentication type, *username* should be consistent with the valid user name defined in AAA; for the **RSA** authentication type, *username* is the SSH local user name, so that there is no need to configure a local user in AAA.
- If the default authentication type for SSH users is password and local AAA authentication is adopted, you need not use the **ssh user** command to create an SSH user. Instead, you can use the **local-user** command to create a user name and its password and then set the service type of the user to SSH.
- If the default authentication type for SSH users is password and remote authentication (RADIUS authentication, for example) is adopted, you need not use the **ssh user** command to create an SSH user, because it is created on the remote server. And the user can use its username and password configured on the remote server to access the network.
- If you use the **ssh user** *username* **authentication-type** command to specify an authentication type for an inexistent SSH user, the system will create the SSH user automatically.
- If the RSA authentication type is specified, you can use the **user privilege level** command to set the level of the commands available to the SSH users logging into the server. Additionally, the command levels accessible to the users adopting RSA authentication are the same.
- If the password authentication type is specified, the command levels accessible to SSH users logging into the server are determined through AAA. In this case, the command level may vary with users.

V. Configuring SSH management

The configuration of SSH management includes the setting of authentication timeout time, authentication retry times, server key update interval, and SSH compatible mode. After the configuration, the SSH management function is able to prevent illegal activities such as malicious password guessing, thus ensure the security of SSH connections.

Table 1-6 Configure SSH management

Operation	Command	Description
Enter system view	**system-view**	—
Set SSH authentication timeout time	**ssh server timeout** *seconds*	Optional By default, the timeout time is 60 seconds.
Set SSH authentication retry times	**ssh server authentication-retries** *times*	Optional By default, the number of retry times is 3.
Set server key update interval	**ssh server rekey-interval** *hours*	Optional By default, the system does not update server keys.
Configure SSH server to be compatible with SSH1.x clients	**ssh server compatible-ssh1x enable**	Optional By default, SSH server is compatible with SSH1.x clients.

VI. Configuring a client public key for a user

On the switch, you can configure a client public key (generated randomly on a client) for a client user. This configuration is not required for password authentication type.

There are two methods to configure a client public key for a user.

1) Manual configuration

First, perform the following operations on a client:

- Use the SSH1.5/2.0 client software to randomly generate a RSA key pair.
- Use the SSHKEY.exe program to transform the public key in the RSA key pair to PKCS (public-key cryptography standards) format.

Then, perform the following operations on the server:

Table 1-7 Configure client public key for a user

Operation	Command	Description
Enter system view	**system-view**	—
Enter public key view	**rsa peer-public-key** *keyname*	Required
Enter public key edit view to input a client public key	**public-key-code begin**	—

Operation	Command	Description
Configure the client public key	Enter the content of the public key	Required When you input the key data, spaces are allowed between the characters you input (because the system can remove the spaces automatically); you can also press <Enter> to continue your input at the next line. But the key you input should be a hexadecimal digit string coded in the public key format.
Return to public key view from public key edit view	**public-key-code end**	The system saves the public key data you input when exiting public key edit view.
Return to system view from public key view	**peer-public-key end**	—
Assign a client public key to an SSH user	**ssh user** *username* **assign rsa-key** *keyname*	Required *Keyname* is the name of an existing public key. If the user has already been assigned with a public key, the newly assigned public key overwrites the old one.

Note:

- The above method requires you to transform the format of the public key on the client, and then manually configure the transformed public key on the server. So, the method is relatively more complex.
- If you use the **ssh user** *username* **assign rsa-key** command to assign an public key for an inexistent SSH user, the system will create the SSH user automatically.
- When configuring the public key for a client manually, you can copy the local host public key configuration on the client and then paste it to the server.

2) Automatic configuration

First, perform the following operations on a client:

- Use the SSH1.5/2.0 client software to randomly generate a RSA key pair.
- Use FTP/TFTP to transfer the corresponding public key file to the Flash memory of the server.

Then, perform the following operations on the server:

Table 1-8 Automatic configuration

Operation	Command	Description
Enter system view	**system-view**	—
Transform the format of the key in a client public key file and automatically configure a client public key on the server	**rsa peer-public-key** *keyname* **import sshkey** *filename*	*filename* must be consistent with the name of a public key file in the Flash memory.

Note:

The above method does not require you to manually configure a public key. So the method is relatively simple and is the recommended method.

VII. Specifying a source IP address/interface for the SSH server

You can perform the following configurations to specify a source IP address or a source interface for the SSH server, thus enhancing traffic manageability.

Table 1-9 Specify a source IP address/interface for the SSH server

Operation	Command	Description
Enter system view	**system-view**	—
Specify a source IP address for the SSH server	**ssh-server source-ip** *ip-address*	Optional
Specify a source interface for the SSH server	**ssh-server source-interface** *interface-type interface-number*	Optional

1.1.3 Configuring the SSH Client

A variety of SSH client software are available, such as PuTTY and OpenSSH. For an SSH client to establish a connection with an SSH server, you must complete these configuration tasks:

- Specifying the IP address of the server.
- Selecting the protocol for remote connection as SSH. Usually, a client can use a variety of remote connection protocols, such as Telnet, Rlogin, and SSH. To establish an SSH connection, you must select SSH.
- Selecting the SSH version. Since the device supports SSH Server 2.0 now, select 2.0 or lower for the client.

- Specifying the RSA private key file. On the server, if RSA authentication is enabled for an SSH user and a public key is set for the user, the private key file corresponding to the public key must be specified on the client. RSA key pairs are generated by a tool of the client software.

The following takes the client software of PuTTY, PuTTYGen and SSHKEY as examples to illustrate how to configure the SSH client:

I. Generating the Client Keys

To generate the client key pair, run PuTTYGen.exe, choose **SSH-2 RSA** under **Parameters** and click **Generate**.

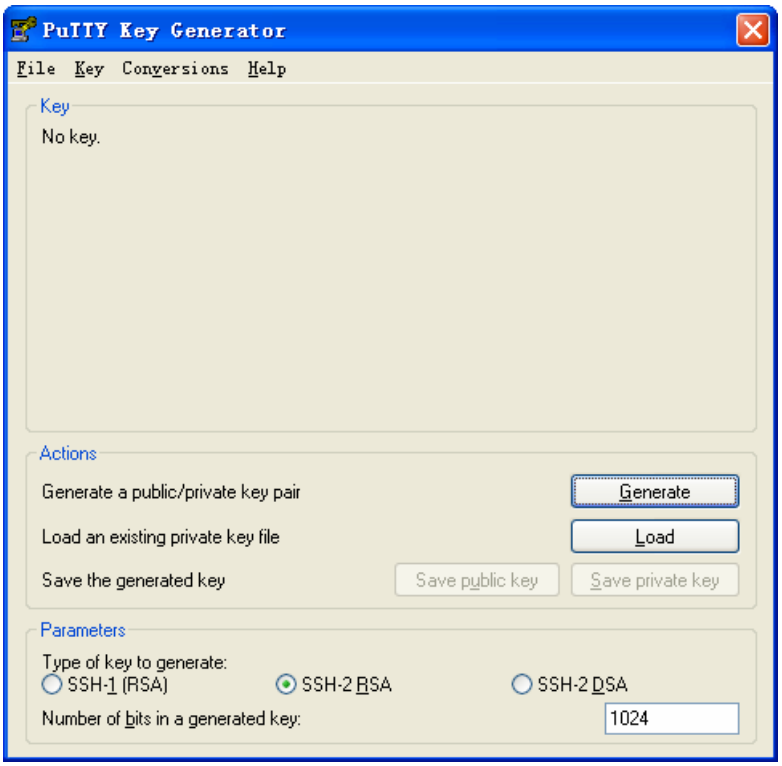


Figure 1-3 Generating the client keys (1)

Note that while generating the key pair, you must move the mouse continuously and keep the mouse off the green process bar in the blue box of shown in Figure 1-4. Otherwise, the process bar stops moving and the key pair generating process is stopped.

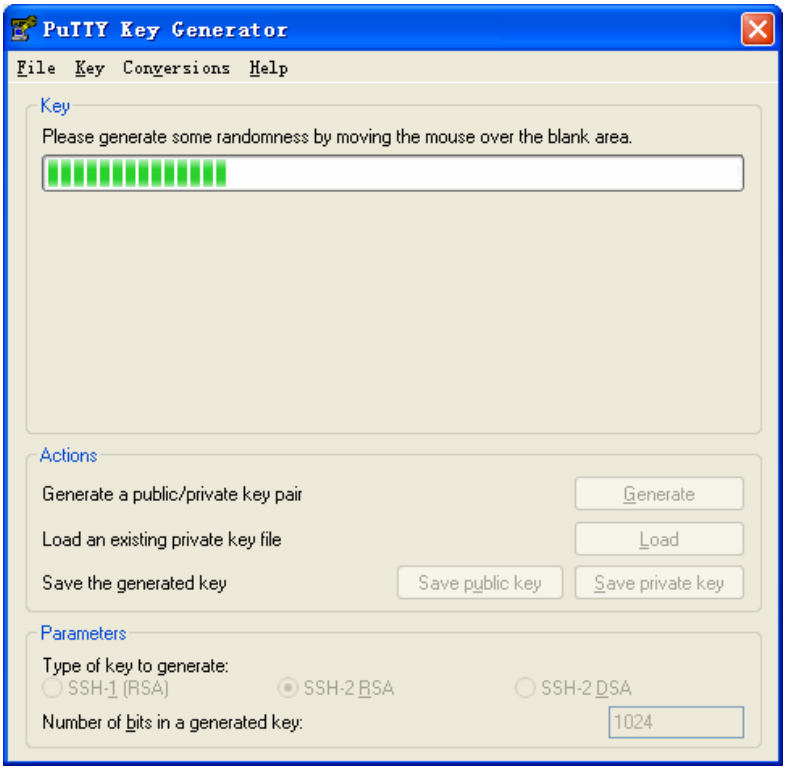


Figure 1-4 Generating the client keys (2)

After the key pair is generated, click **Save public key** and enter the name of the file for saving the public key (**public** in this case) to save the public key.

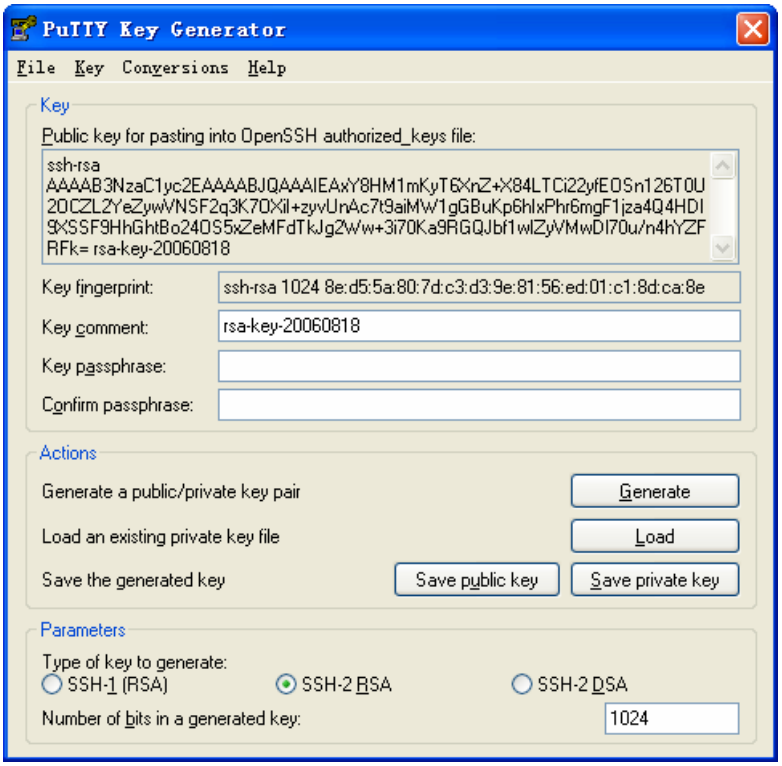


Figure 1-5 Generating the client keys (3)

Likewise, to save the private key, click **Save private key**. A warning window pops up to prompt you whether to save the private key without any precaution. Click **Yes** and enter the name of the file for saving the public key (**private** in this case) to save the private key.

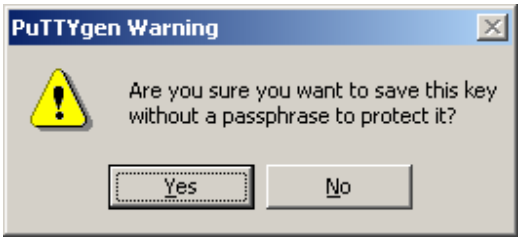


Figure 1-6 Generating the client keys (4)

To generate RSA public key in PKCS format, run SSHKEY.exe, click **Browse** and select the public key file, and then click **Convert**.

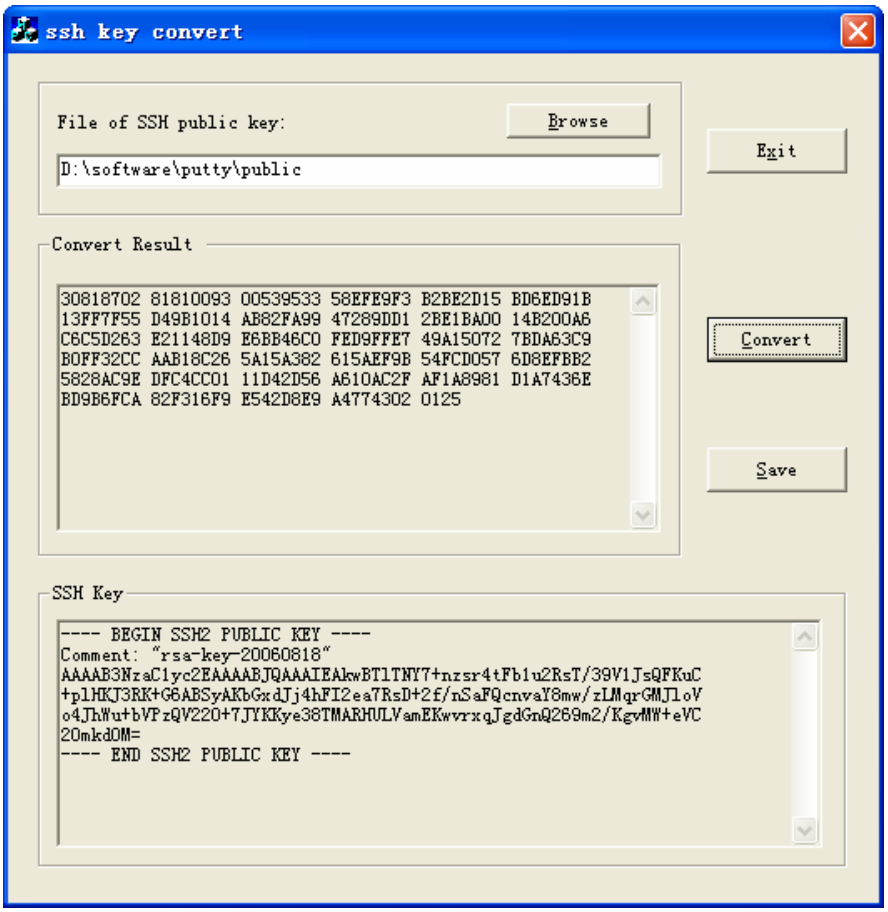


Figure 1-7 Generating the client keys (5)

II. Specifying the IP address of the Server

Launch PuTTY.exe. The following window appears.

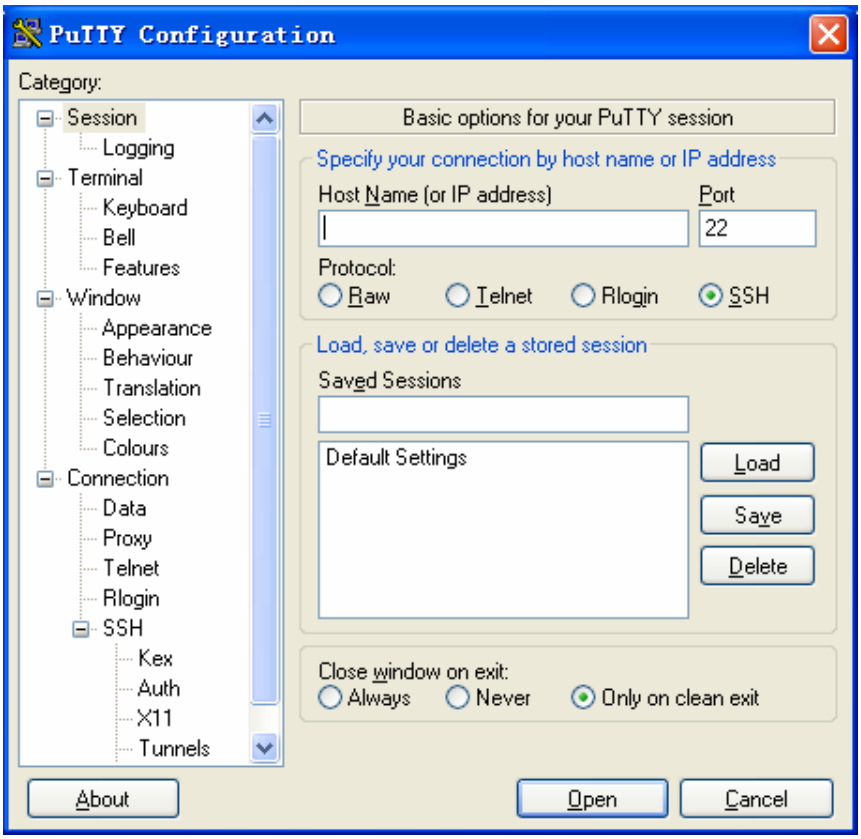


Figure 1-8 SSH client configuration interface 1

In the **Host Name (or IP address)** text box, enter the IP address of the server, Note that there must be a route available between the IP address of the server and the client.

III. Selecting the Protocol for Remote Connection

As shown in Figure 1-8, select **SSH** under **Protocol**.

IV. Selecting the SSH Version

From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in Figure 1-9 appears.

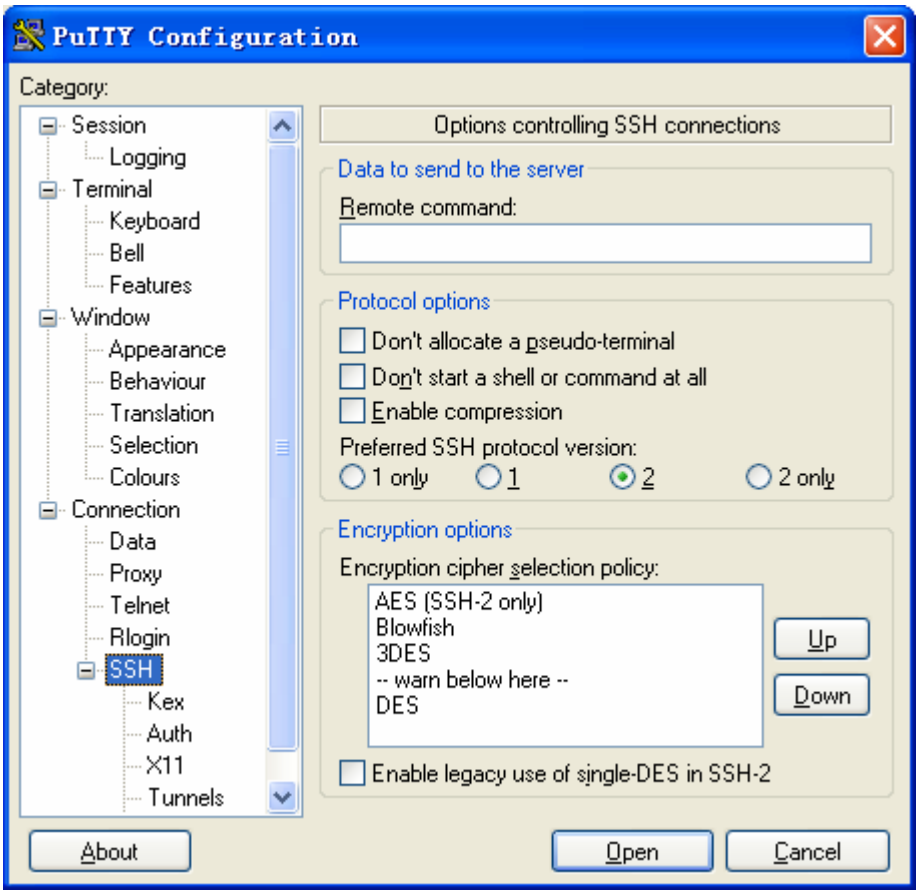


Figure 1-9 SSH client configuration interface 2

Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

Note:

Some SSH client software, for example, Tectia client software, supports the DES algorithm only when the ssh1 version is selected. The PuTTY client software supports DES algorithm negotiation ssh2.

V. Opening an SSH Connection with RSA

If the client needs to use RSA authentication, you must specify the RSA private key file. If the client needs to use password authentication, this is not required.

From the category on the left of the window, Select **Connection/SSH/Auth**. The following window appears.

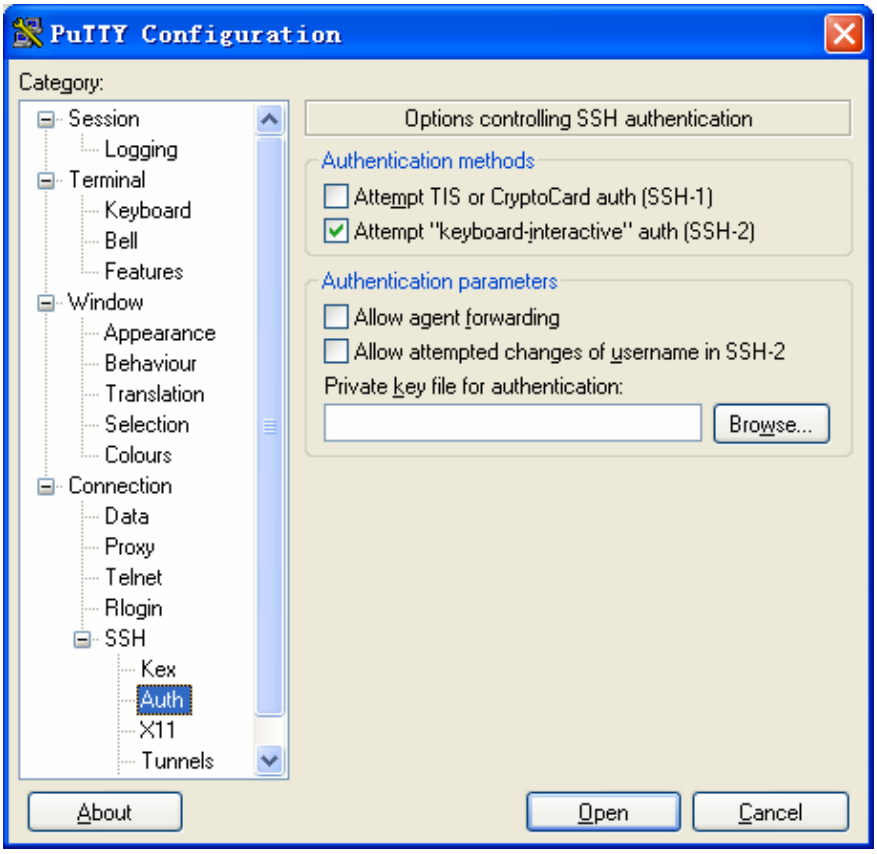


Figure 1-10 SSH client configuration interface 3

Click **Browse…** to bring up the file selection window, navigate to the private key file and click **OK**.

VI. Opening an SSH Connection with Password

1) From the window shown in Figure 1-10, click **Open**. The following SSH client interface appears. If the connection is normal, you will be prompted to enter the username and password, as shown in Figure 1-11.

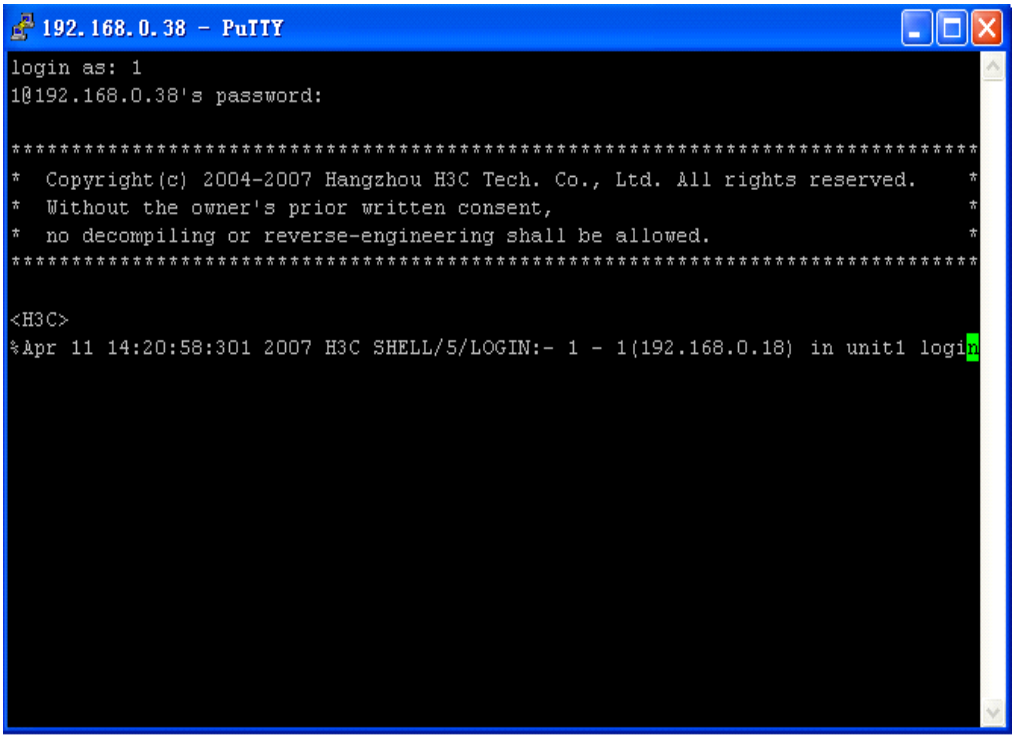


Figure 1-11 SSH client interface

2) Enter the username and password to establish an SSH connection.
3) To log out, enter the **quit** command.

1.1.4 Configuring the Device as an SSH Client

When the device connects to the SSH server as an SSH client, you can configure the SSH client to authenticate the SSH server during the first access.

- The first authentication means that when the SSH client accesses the server for the first time and is not configured with the server host public key, the user can choose to continue accessing the server and save the host public key on the client for future authentication of the server.
- With first authentication not supported, the client cannot authenticate the server if it is not configured with the server host public key. In this case, you must configure the host public key of the server and specify the key name on the client beforehand, so that the client can authenticate the server.

You can configure the client to use a specified IP address or interface to access the SSH.

I. configure the device as an SSH client that supports first authentication

Table 1-10 Configure the device as an SSH client that supports first authentication

Operation	Command	Description
Enter system view	**system-view**	—
Enable the client to run initial authentication	**ssh client first-time enable**	Optional By default, the client is enabled to run initial authentication.
Start the client to establish a connection with an SSH server	**ssh2** { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **des** | **aes128** } | **prefer_stoc_cipher** { **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *	Required In this command, you can also specify the preferred key exchange algorithm, encryption algorithms and HMAC algorithms between the server and client. HMAC: Hash-based message authentication code

II. configure the device as an SSH client that does not support first authentication

Table 1-11 Configure the device as an SSH client that does not support first authentication

Operation	Command	Description
Enter system view	**system-view**	—
Disable the SSH client from performing first authentication for the SSH server to be accessed	**undo ssh client first-time**	Required By default, the SSH client performs first authentication.
Enter public key view	**rsa peer-public-key** *keyname*	Optional
Enter public key edit view	**public-key-code begin**	—
Configure the public key for the server	Input the public key directly	— The input public key string can contain spaces and enters. The public key to be configured must be a hexadecimal string coded in the public format.

Operation	Command	Description
Quit to public key view	**public-key-code end**	— The input public keys are saved when you quit the public key edit view.
Quit to system view	**peer-public-key end**	—
Specify the name of the host public key of the SSH server to be accessed on the SSH client	**ssh client** { *server-ip* | *server-name* } **assign rsa-key** *keyname*	Required
Connect the SSH client to the SSH server, and specify the preferred key exchange algorithm, the preferred encryption algorithm and the preferred HMAC algorithm for the SSH client and the SSH server	**ssh2** { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **des** | **aes128** } | **prefer_stoc_cipher** { **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *	Required

III. Specifying a source IP address/interface for the SSH client

You can perform the following configuration to specify a source IP address or a source interface for the SSH2.0 client, thus enhancing traffic manageability.

Table 1-12 Specify a source IP address/interface for the SSH client

Operation	Command	Description
Enter system view	**system-view**	—
Specify a source IP address for the SSH2.0 client.	**ssh2 source-ip** *ip-address*	Optional
Specify a source interface for the SSH2.0 client	**ssh2 source-interface** *interface-type interface-number*	Optional

1.1.5 Displaying SSH Configuration

After the above configuration, you can execute the **display** command in any view to display the configuration information and running status of SSH, so as to verify your configuration.

Table 1-13 Display SSH configuration

Operation	Command	Description
Display host and server public keys	**display rsa local-key-pair public**	You can execute the **display** command in any view.
Display client RSA public key(s)	**display rsa peer-public-key** [**brief** | **name** *keyname*]	
Display SSH status and session information	**display ssh server** { **status** | **session** }	
Display SSH user information	**display ssh user-information** [*username*]	
Display the current source IP address or the IP address of the source interface specified for the SSH server.	**display ssh-server source-ip**	
Display the mappings between host public keys and SSH servers saved on a client	**display ssh server-info**	
Display the current source IP address specified for the SSH2.0 Client.	**display ssh2 source-ip**	

1.1.6 SSH Server Configuration Example

I. Network requirements

As shown in Figure 1-12, The PC (SSH Client) running an SSH2.0-supported client software, establish a local connection with the switch (SSH Server) to ensure the security of data exchange.

II. Network diagram

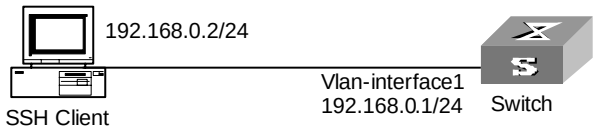


Figure 1-12 Network diagram for SSH server configuration

III. Configuration procedure

The configuration procedure varies with login authentication modes. However, you must complete the following three configuration tasks before any configuration procedure.

```
<H3C> system-view
[H3C] rsa local-key-pair create
```

Then, you must create a VLAN interface on the switch and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[H3C-Vlan-interface1] quit
```

Finally, you must configure an IP address (192.168.0.2 in this case) for the SSH client. This IP address and that of the VLAN interface on the switch must be in the same network segment.

1) Set user authentication method.

Settings for the two authentication types are described respectively in the following:

- Password authentication

Set AAA authentication on user interfaces.

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
```

Configure the user interfaces to support SSH.

```
[H3C-ui-vty0-4] protocol inbound ssh
[H3C-ui-vty0-4] quit
```

Set login protocol to SSH, specify commands of level 3, and authentication password to "abc" for user clinet001.

```
[H3C] local-user client001
[H3C-luser-client001] password simple abc
[H3C-luser-client001] service-type ssh level 3
[H3C-luser-client001] quit
[H3C] ssh user client001 authentication-type password
```

Note:

You can use the default SSH authentication timeout time and authentication retry times. After the above settings, run the SSH2.0-supported client software on a host connected to the switch, and log into the switch with the username client001 and password "abc".

- RSA public key authentication

Set AAA authentication on the user interfaces.

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
```

Set the user interfaces to support SSH.

```
[H3C-ui-vty0-4] protocol inbound ssh
```

Set the command level for the login users to 3.

```
[H3C-ui-vty0-4] user privilege level 3
[H3C-ui-vty0-4] quit
```

Set login protocol to SSH and authentication type to RSA for user client001.

```
[H3C] ssh user client001 authentication-type rsa
```

At this time, the client supporting SSH2.0 will generate a random RSA key pair, including public key and private key. You need to add the RSA public key, a hexadecimal character string encoded by the SSHKEY.EXE software in accordance with the public key cryptography standards (PKCS), to the rsa peer-public-key on the specified SSH server in the following way.

Configure the client public key on the server, with a key name of Switch001.

```
[H3C] rsa peer-public-key Switch001
[H3C-rsa-public-key] public-key-code begin
[H3C-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[H3C-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[H3C-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[H3C-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[H3C-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[H3C-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[H3C-rsa-key-code] public-key-code end
[H3C-rsa-public-key] peer-public-key end
```

or

```
[H3C] rsa peer-public-key Switch001 import sshkey Switch001
```

Specify a public key of Switch001 for user client001.

```
[H3C] ssh user client001 assign rsa-key Switch001
```

For the RSA authentication, you not only need to configure the IP address, protocol type, and protocol version of the SSH server, but also need to specify an RSA private key file (generated by the client software at random) on the client. After the SSH connection is established, enter the username as prompted to go into the configuration interface of the switch.

1.1.7 SSH Client Configuration Example

I. Network requirements

As shown in Figure 1-13:

- Switch A serves as an SSH client, with a user name of client001.
- Switch B serves as an SSH server, with an IP address of 10.165.87.136.

II. Network diagram

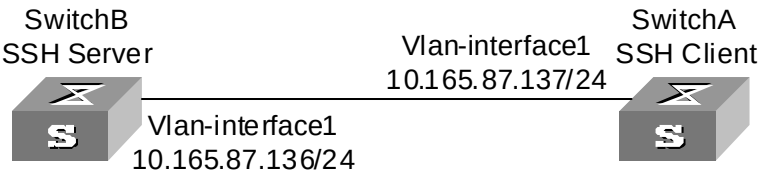


Figure 1-13 Network diagram for SSH client configuration

III. Configuration procedure

1) Configure SwitchB

Create an RSA host key pair and server key pair

```
<H3C> system-view
[H3C] rsa local-key-pair create
```

Create a VLAN interface and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[H3C-Vlan-interface1] quit
```

Set the authentication method of the user interface to AAA for SSH client.

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
```

Set the protocol that a remote user uses to login as SSH.

```
[H3C-ui-vty0-4] protocol inbound ssh
[H3C-ui-vty0-4] quit
```

Set login protocol to SSH, specify commands of level 3, and authentication password to "abc" for user clinet001.

```
[H3C] local-user client001
[H3C-luser-client001] password simple abc
[H3C-luser-client001] service-type ssh level 3
[H3C-luser-client001] quit
```

Set the SSH authentication method to password. The SSH authentication timeout period, number of SSH authentication attempts and server key pair update interval can be the default values.

```
[H3C] ssh user client001 authentication-type password
```

Note:

If you set the SSH authentication method to RSA, you need to configure a host public key of Switch A. For the specific configuration, refer to .1.1.6 SSH Server Configuration Example.

2) Configure SwitchA

Configure an IP address (10.165.87.137 in this case) for the VLAN interface on SwitchA. This IP address and that of the VLAN interface on SwitchB must be in the same network segment.

```
<H3C> system-view
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[H3C-Vlan-interface1] quit
```

Establish an SSH connection to server 10.165.87.136.

```
[H3C] ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):n
Enter password:

**************************************************************************
* Copyright(c) 2004-2007 Hangzhou H3C Tech. Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                *
**************************************************************************

<H3C>
```

Chapter 2 SFTP Service

2.1 SFTP Service

2.1.1 Introduction to SFTP

Secure FTP (SFTP) is a new feature introduced in SSH2.0.

Since SFTP is based on SSH, it can provides security for remote users to log into the switch and perform file management and transfer operations (such as system update), thus providing more security for data transfer. Through the SFTP client function, you can securely log into a remote device and perform file transfer operations securely.

2.1.2 SFTP Server Configuration

The following sections describe SFTP Server configuration tasks:

- Configuring service type for an SSH user
- Enabling SFTP Server
- Setting connection idle timeout

I. Configuring service type for an SSH user

Table 2-1 Configure service type for an SSH user

Operation	Command	Description
Enter system view	**system-view**	—
Configure service type for an SSH user	**ssh user** *username* **service-type** { **stelnet** | **sftp** | **all** }	Optional By default, the service type available for a user is **stelnet**.

Caution:

If you use the **ssh user** *username* **service-type** command to specify a service type for an inexistent SSH user, the system will create the SSH user automatically.

II. Enabling SFTP Server

Table 2-2 Enable SFTP Server

Operation	Command	Description
Enter system view	**system-view**	—
Enable SFTP Server	**sftp server enable**	Required By default, SFTP Server is disabled.

III. Setting connection idle timeout time

You can set the idle timeout time for SFTP connections, so that the system can automatically release a user connection when the user connection is idle for a time longer than the time threshold you set.

Table 2-3 Set connection idle timeout time

Operation	Command	Description
Enter system view	**system-view**	—
Set idle timeout time for SFTP connections	**sftp timeout** *time-out-value*	Required By default, the connection idle timeout time is 10 minutes.

2.1.3 SFTP Client Configuration

The following table describes SFTP Client configuration tasks:

Table 2-4 SFTP Client configuration tasks

Operation	Command Keyword	View	Description
Start SFTP Client	**sftp**	System view	Required
Stop SFTP Client	**bye**	SFTP client view	Optional
	exit		
	quit		

Operation		Command Keyword	View	Description
SFTP directory operations	Change the current directory	**cd**	SFTP client view	Optional
	Return to the upper directory	**cdup**		
	Display the current directory	**pwd**		
	Display the file list in a directory	**dir**		
		ls		
	Create a new directory	**mkdir**		
	Delete a directory	**rmdir**		
SFTP file operations	Rename a file on the remote SFTP server	**rename**	SFTP client view	Optional
	Download a file from the remote SFTP server	**get**		
	Upload a local file to the remote SFTP server	**put**		
	Display the file list in a directory	**dir**		
		ls		
	Delete a file from the SFTP server	**delete**		
		remove		
Get help information about SFTP client commands		**help**	SFTP client view	Optional

I. Starting SFTP Client

You can start SFTP Client to establish a connection to a remote SFTP server and enter STP client view.

Table 2-5 Start SFTP Client

Operation	Command	Description
Enter system view	**system-view**	—
Start SFTP Client	**sftp** { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **des** | **aes128** } | **prefer_stoc_cipher** { **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *	Required

II. Stopping SFTP Client

Table 2-6 Stop SFTP Client

Operation	Command	Description
Enter system view	**system-view**	—
Enter SFTP client view	**sftp** { *host-ip* | *host-name* }	—
Stop SFTP Client	**bye**	The three commands have the same function.
	exit	
	quit	

III. Performing SFTP directory operations

SFTP directory operations include: changing or displaying the current directory, creating or deleting a directory, displaying file or directory information in a specific directory.

Table 2-7 Perform SFTP directory operation

Operation	Command	Description
Enter system view	**system-view**	—
Enter SFTP client view	**sftp** { *host-ip* | *host-name* }	—
Change the current directory	**cd** *remote-path*	Optional
Return to the upper directory	**cdup**	
Display the current directory	**pwd**	

Operation	Command	Description
Display the file list of a directory	**dir** [**-a** | **-l**] [*remote-path*]	Optional The **dir** and **ls** commands have the same function.
	ls [**-a** | **-l**] [*remote-path*]	
Create a directory on the SFTP server	**mkdir** *remote-path*	Optional
Delete a directory from the SFTP server	**rmdir** *remote-path*&<1-10>	

IV. Performing SFTP file operations

SFTP file operations include: renaming a file, downloading a file, uploading a file, displaying the file list, and deleting a file.

Table 2-8 Performing SFTP file operations

Operation	Command	Description
Enter system view	**system-view**	Optional
Enter SFTP client view	**sftp** { *host-ip* | *host-name* }	
Rename a file on the remote SFTP server	**rename** *old-name new-name*	
Download a file from the remote SFTP server	**get** *remote-file* [*local-file*]	
Upload a file to the remote SFTP server	**put** *local-file* [*remote-file*]	
Display the file list of a directory	**dir** [**-a** | **-l**] [*remote-path*]	Optional The **dir** and **ls** commands have the same function.
	ls [**-a** | **-l**] [*remote-path*]	
Delete a file from the SFTP server	**delete** *remote-file*&<1-10>	Optional The **delete** and **remove** commands have the same function.
	remove *remote-file*&<1-10>	

V. Displaying help information

You can use the command here to display help information (such as syntax and parameters) about an SFTP client command.

Table 2-9 Display help information about an SFTP client command

Operation	Command	Description
Enter system view	**system-view**	—
Enter SFTP client view	**sftp** { *host-ip* | *host-name* }	—
Display help information about one or all SFTP client commands	**help** [**all** | *command-name*]	Optional

VI. Specifying a source IP address or source interface for the SFTP client

You can use the command here to specify a source IP address or source interface for the SFTP client, thus enhancing traffic manageability.

Table 2-10 Specify a source IP address/interface for the SFTP client

Operation	Command	Description
Enter system view	**system-view**	—
Specify a source IP address for the SFTP client	**sftp source-ip** *ip-address*	Optional
Specify a source interface for the SFTP client	**sftp source-interface** *interface-type interface-number*	Optional
Display the current source IP address or the IP address of the source interface specified for the SFTP client	**display sftp source-ip**	Optional You can execute this command in any view.

2.1.4 SFTP Configuration Example

I. Network requirements

As shown in Figure 2-1: an SSH connection is established between SwitchA and SwitchB. SwitchA, an SFTP client, uses the username client001 and password abc to login to SwitchB for file management and file transfer.

II. Network diagram

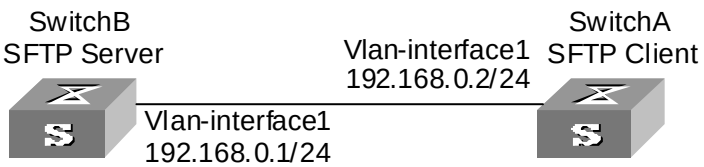


Figure 2-1 Network diagram for SFTP configuration

III. Configuration procedure

1) Configure Switch B (SFTP server)

```
<H3C>system-view
[H3C] rsa local-key-pair create
```

Create a VLAN interface on SwitchB and assign an IP address, which the SSH client uses as the destination for SSH connection.

```
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[H3C-Vlan-interface1] quit
```

Set the authentication method on the user interface to AAA.

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
```

Set the protocol that a remote user uses to login as SSH.

```
[H3C-ui-vty0-4] protocol inbound ssh
[H3C-ui-vty0-4] quit
```

Create local user client001.

```
[H3C] local-user client001
[H3C-luser-client001] password simple abc
[H3C-luser-client001] service-type ssh
[H3C-luser-client001] quit
```

Set the SSH authentication method to password. The SSH authentication timeout period, number of SSH authentication attempts and server key pair update interval can be default values.

```
[H3C] ssh user client001 authentication-type password
```

Note:

If you set the SSH authentication method to RSA, you need to configure the host public key of SwitchA. For the specific configuration, refer to .SSH Server Configuration Example.

Specify SFTP service for SSH user abc.

```
[H3C] ssh user client001 service-type sftp
```

Enable SFTP Server.

```
[H3C] sftp server enable
```

2) Configure Switch A (SFTP client)

Configure an IP address (192.168.0.2 in this case) for the VLAN interface on SwitchA. This IP address and that of the VLAN interface on SwitchB must be in the same network segment.

```
<H3C> system-view
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[H3C-Vlan-interface1] quit
```

Establish a connection to the remote SFTP server and enter SFTP client view.

```
[H3C] sftp 192.168.0.1
Input Username: client001
Trying 192.168.0.1 ...
Press CTRL+K to abort
Connected to 192.168.0.1 ...

The Server is not authenticated. Do you continue access it? [Y/N]:y
Do you want to save the server's public key? [Y/N]:n
Enter password:

sftp-client>
```

Display the current directory on the SFTP server, delete file z and verify the operation.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.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
The following files will be deleted:
flash:/z
Are you sure to delete it?(Y/N):y
This operation may take a long time.Please wait...

File successfully Removed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
```

Create directory new1 and verify the operation.

```
sftp-client> mkdir new1
New directory created
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.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
```

Rename directory new1 to new2 and verify the operation.

```
sftp-client> rename new1 new2
File successfully renamed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
```

Download file pubkey2 and rename it to public.

```
sftp-client> get pubkey2 public
This operation may take a long time, please wait...

Remote  file:flash:/pubkey2 --->  Local file: public..

Downloading file successfully ended
```

Upload the file pu to the SFTP server and rename it to puk. Verify the operations.

```
sftp-client> put pu puk
This operation may take a long time, please wait...
Local file: pu --->  Remote file: flash:/puk
Uploading file successfully ended
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.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 pub
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:36 puk
sftp-client>
```

Stop SFTP Client.

```
sftp-client> quit
Bye
[H3C]
```

Table of Contents

Chapter 1 File System Management Configuration 1-1
1.1 File Attribute Configuration 1-1
1.1.1 Introduction to File Attributes 1-1
1.1.2 Configuring File Attributes 1-2
1.2 File System Configuration 1-3
1.2.1 Introduction to File System 1-3
1.2.2 Introduction to Configuration Tasks on the File System 1-3
1.2.3 Directory Operations 1-4
1.2.4 File Operations 1-5
1.2.5 Flash Memory Operations 1-6
1.2.6 Prompt Mode Configuration 1-7
1.2.7 File System Configuration Example 1-7
1.3 Configuration File Backup and Restoration 1-8
1.3.1 Operation Prerequisites 1-9
1.3.2 Operation Procedure 1-9
Chapter 2 FTP/TFTP Lighting Configuration 2-1
2.1 FTP Lighting Configuration 2-1
2.1.1 Introduction to FTP 2-1
2.1.2 FTP Lighting Procedure 2-1
2.2 TFTP Lighting Configuration 2-3
2.2.1 Introduction to TFTP 2-3
2.2.2 TFTP Lighting Procedure 2-4

Chapter 1 File System Management Configuration

1.1 File Attribute Configuration

1.1.1 Introduction to File Attributes

An app file is an executable file, with .bin as the extension. A configuration file is used to store and restore configuration, with .cfg as the extension. A Web file is used for Web-based network management, with .web as the extension.

The app file, configuration file, and Web file have three kinds of attributes: main, backup and none, as described in Table 1-1.

Table 1-1 Descriptions on file attributes

Attribute name	Description	Feature	Identifier
main	Identifies main startup files. The main startup file is used first for a switch to start up.	In the Flash memory, there can be only one app file, one configuration file and one Web file with the main attribute.	(*)
backup	Identifies backup startup files. The backup startup file is used after a switch fails to start up using the main startup file.	In the Flash memory, there can be only one app file, one configuration file and one Web file with the backup attribute.	(b)
none	Identifies files that are neither of main attribute nor backup attribute.	—	None

Note:

A file can have both the main and backup attributes. Files of this kind are labeled *b.

If a newly created file is configured to be with the main attribute, the existing file with the main attribute in the Flash memory will be changed to other attribute. This ensures that there can be only one app file, one configuration file and one Web file with the main attribute in the Flash memory. This circumstance also applies to the file with the backup attribute in the Flash memory.

File operations and file attribute operations are independent. For example, if you delete a file with the main attribute from the Flash memory, the other files in the flash memory

will not possess the main attribute. If you download a file with the same name as the original file with the main attribute to the flash memory, the file will possess the main attribute.

After the BootROM of a switch is upgraded, the original default APP startup file has the main attribute.

1.1.2 Configuring File Attributes

You can configure and view the main attribute or backup attribute of the startup file used for the next startup of a switch, and change the main or backup attribute of the file.

Perform the configuration listed in Table 1-2 in user view. The **display** commands can be executed in any view.

Table 1-2 Configure file attributes

To do…	Use the command…	Remarks
Configure the app file with the main attribute for the next startup	**boot boot-loader** *file-url* [**fabric**]	Optional
Set the app file with the backup attribute for the next startup	**boot boot-loader backup-attribute** *file-url* [**fabric**]	Optional
Configure the Web file and its attribute	**boot web-package** *webfile* { **backup** | **main** }	Optional
Switch the file attributes between main and backup	**boot attribute-switch** { **all** | **app** | **configuration** | **web** } **fabric**	Optional
Specify to enable user to use the customized password to enter the BOOT menu	**startup bootrom-access enable**	Optional By default, the user is enabled to use the customized password to enter the BOOT menu.
Display the information about the app file used as the startup file	**display boot-loader** [**unit** *unit-id*]	Optional This command can be executed in any view.

Caution:

- Before configuring the main or backup attribute for a file in the fabric, make sure the file already exists on all devices in the fabric.
- The configuration of the main or backup attribute of a Web file takes effect immediately without restarting the switch.
- After upgrading a Web file, you need to specify the new Web file in the Boot menu after restarting the switch. Otherwise, the Web server cannot function normally.
- Currently, a configuration file has the extension of cfg and resides in the root directory of the Flash memory.

1.2 File System Configuration

1.2.1 Introduction to File System

To facilitate management on the Flash memory, Ethernet switches provide the file system module. The file system allows users to create/delete a directory, display the current work directory, display the contents of a directory, and access files.

By default, a switch prompts for confirmation before executing the commands which have potential risks (for example, deleting and overwriting files).

1.2.2 Introduction to Configuration Tasks on the File System

Table 1-3 Configuration tasks on the file system

Configuration task	Description	Related section
Directory operation	Optional	Section 1.2.3 “Directory Operations”
File operation	Optional	Section 1.2.4 “File Operations”
Flash memory operation	Optional	Section 1.2.5 “Flash Memory Operations”
Prompt mode configuration	Optional	Section 1.2.6 “Prompt Mode Configuration”

Note:

For Ethernet switches that support intelligent resilient framework (IRF), you can input a file path and file name in one of the following ways:

- In URL (universal resource locator) format and starting with “unit[No.]>flash:/” ([No.] represents the unit ID of a switch). This method is used to specify a file on a specified unit. For example, if the unit ID of a switch is 1, the URL of a file named text.txt and residing in the root directory must be “unit1>flash:/text.txt”.
- In URL format and starting with “flash:/”. This method can be used to specify a file in the Flash memory of the current unit.
- Entering the path name or file name directly. This method can be used to specify a path or a file in the current work directory.

1.2.3 Directory Operations

The file system provides directory-related functions, such as:

- Creating/deleting a directory
- Displaying the current work directory, or contents in a specified directory

Table 1-4 describes the directory-related operations.

Perform the following configuration in user view.

Table 1-4 Directory operations

To do…	Use the command…	Remarks
Create a directory	**mkdir** *directory*	Optional
Delete a directory	**rmdir** *directory*	Optional Only empty directories can be deleted.
Display the current work directory	**pwd**	Optional
Display the information about specific directories and files	**dir** [/**all**] [/**fabric** | *file-url*]	Optional
Enter a specified directory	**cd** *directory*	Optional

Note:

In the output information of the **dir** /**all** command, deleted files (that is, those in the recycle bin) are embraced in brackets.

1.2.4 File Operations

The file system also provides file-related functions, such as:

- Deleting a file
- Restoring a deleted file
- Deleting a file permanently
- Managing a configuration file
- Renaming a file
- Copying a file
- Moving a file
- Displaying the content of a file
- Displaying the information about a file
- Checking file system

Perform the following configuration in user view. Note that the **execute** command should be executed in system view, and the **display** command can be executed in any view.

Table 1-5 File operations

To do…	Use the command…	Remarks
Delete a file	**delete** [**/unreserved**] *file-url* **delete** { **running-files** | **standby-files** } [**/fabric**] [**/unreserved**]	Optional A deleted file can be restored if you delete it by executing the **delete** command without specifying the **/unreserved** keyword. You can use the **undelete** command to restore a deleted file of this kind.
Delete a file from the recycle bin	**reset recycle-bin** [*file-url*] [**/force**] **reset recycle-bin** [**/fabric**]	Optional
Upgrade the software of the whole fabric	**update fabric** *file-name*	Optional Use this command only after all traffics are stopped.
Rename a file	**rename** *fileurl-source fileurl-dest*	Optional
Copy a file	**copy** *fileurl-source fileurl-dest*	Optional
Move a file	**move** *fileurl-source fileurl-dest*	Optional
Display the content of a file	**more** *file-url*	Optional Currently, the file system only supports displaying the contents of a file in texts.

To do…	Use the command…	Remarks
Display the information about a directory or a file	**dir** [**/all**] [**/fabric** | *file-url*]	Optional
Execute the specified batch file	**execute** *filename*	Optional This command should be executed in system view.

Caution:

- For deleted files whose names are the same, only the latest deleted file is kept in the recycle bin and can be restored.
- The files which are deleted by the **delete** command without the **/unreserved** keyword are actually moved to the recycle bin and thus still take storage space. You can clear the recycle bin by using the **reset recycle-bin** command.
- Use the **update fabric** command after all traffic flows are stopped.
- The **dir /all** command displays the files in the recycle bin in square brackets.
- If the configuration files are deleted, the switch adopts the default configuration parameters when it starts up next time.

1.2.5 Flash Memory Operations

Perform the following Flash memory operations.

Table 1-6 Operations on the Flash memory

To do…	Use the command…	Remarks
Format the Flash memory	**format** *device*	Required
Restore space on the Flash memory	**fixdisk** *device*	Required

Caution:

The format operation leads to the loss of all files, including the configuration files, on the Flash memory and is irretrievable.

1.2.6 Prompt Mode Configuration

You can set the prompt mode of the current file system to **alert** or **quiet**. In alert mode, the file system will give a prompt for confirmation if you execute a command which may cause data loss, for example, deleting or overwriting a file. In quiet mode, such prompt will not be displayed.

Table 1-7 Configuration on prompt mode of file system

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the prompt mode of the file system	**file prompt** { **alert** | **quiet** }	Required By default, the prompt mode of the file system is **alert**.

1.2.7 File System Configuration Example

Display all the files in the root directory of the file system on the local unit.

```
<H3C> dir /all
Directory of unit1>flash:/

   1 (*)   -rw-   5822215  Jan 01 1970 00:07:03   s3600.bin
   2       -rwh         4  Apr 01 2000 23:55:49   snmpboots
   3       -rwh       428  Apr 02 2000 00:47:30   hostkey
   4       -rwh       572  Apr 02 2000 00:47:38   serverkey
   5       -rw-      1220  Apr 02 2000 00:06:57   song.cfg
   6       -rw-   5026103  Jan 01 1970 00:04:34   s3600v1r1.bin
   7       -rwh        88  Apr 01 2000 23:55:53   private-data.txt
   8 (*)   -rw-      1376  Apr 02 2000 01:56:28   config.cfg

15367 KB total (4634 KB free)

(*) -with main attribute   (b) -with backup attribute
(*b) -with both main and backup attribute
```

Copy the file flash:/config.cfg to flash:/test/, with 1.cfg as the name of the new file.

```
<H3C> copy flash:/config.cfg flash:/test/1.cfg
Copy unit1>flash:/config.cfg to unit1>flash:/test/1.cfg?[Y/N]:y
..
%Copy file unit1>flash:/config.cfg to unit1>flash:/test/1.cfg...Done.
```

Display the file information after the copy operation.

```
<H3C> dir /all
```

```
Directory of unit1>flash:/

   1 (*)   -rw-   5822215  Jan 01 1970 00:07:03   s3600.bin
   2       -rwh         4  Apr 01 2000 23:55:49   snmpboots
   3       -rwh       428  Apr 02 2000 00:47:30   hostkey
   4       -rwh       572  Apr 02 2000 00:47:38   serverkey
   5       -rw-      1220  Apr 02 2000 00:06:57   song.cfg
   6       -rw-   5026103  Jan 01 1970 00:04:34   s3600v1r1.bin
   7       -rwh        88  Apr 01 2000 23:55:53   private-data.txt
   8 (*)   -rw-      1376  Apr 02 2000 01:56:28   config.cfg
   9       drw-         -  Apr 04 2000 04:50:07   test

15367 KB total (4631 KB free)

(*) -with main attribute   (b) -with backup attribute
(*b) -with both main and backup attribute

<H3C> dir unit1>flash:/test/
Directory of unit1>flash:/test/

   1       -rw-      1376  Apr 04 2000 04:50:30   1.cfg

15367 KB total (2025 KB free)

(*) -with main attribute   (b) -with backup attribute
(*b) -with both main and backup attribute
```

1.3 Configuration File Backup and Restoration

Formerly, you can only back up and restore the configuration file of the units one by one in a fabric system.

By using the configuration backup and restoration feature, you can easily back up and restore the configuration files in the whole fabric as well as in a specific unit.

In the backup process, the system first saves the current configuration of a unit to the startup configuration file, and then uploads the file to the TFTP server. In the restore process, the system downloads the startup configuration file from the TFTP server to the local unit.

The configurations of different units in the fabric system can be saved in different .cfg configuration files on the TFTP server. These configuration files correspond to different unit IDs.

1.3.1 Operation Prerequisites

Before performing the following operations, you must first ensure that:

- The relevant units support TFTP client.
- The TFTP server is started and reachable.

1.3.2 Operation Procedure

Perform the following operations in user view.

Table 1-8 Back up and restore configuration file

To do…	Use the command…	Remarks
Back up the current configuration of a specified unit	**backup unit** *unit-id* **current-configuration to** { *dest-addr* | *dest-hostname* } *filename.cfg*	Optional
Back up the current configuration of the whole fabric system	**backup fabric current-configuration to** { *dest-addr* | *dest-hostname* } *filename.cfg*	Optional
Restore the startup configuration of a specified unit	**restore unit** *unit-id* **startup-configuration from** { *source-addr* | *source-hostname* } *filename.cfg*	Optional
Restore the startup configuration of the whole fabric system	**restore fabric startup-configuration from** { *source-addr* | *source-hostname* } *filename.cfg*	Optional

Chapter 2 FTP/TFTP Lighting Configuration

2.1 FTP Lighting Configuration

2.1.1 Introduction to FTP

File transfer protocol (FTP) is a commonly used protocol to transfer files over the Internet and IP networks. Before the emergence of World Wide Web (WWW), users transfer files with command lines mostly using the FTP.

FTP is an application-layer protocol in the TCP/IP protocol suite. It is used for file transfer between remote server and local host.

The Ethernet switch provides the following FTP services:

- FTP server: A user runs FTP client on a PC and logs into an FTP server (the network administrator should configure the IP address of the FTP server before the user log in). Then the user can access the files on the FTP server.
- FTP client: A user runs a terminal emulation program or Telnet program on a PC and connects to the Ethernet switch which acts as an FTP client. After that, the user enter the **ftp** X.X.X.X command (where, X.X.X.X represents the IP address of an FTP server) to establish a connection between the Ethernet switch and a remote FTP server. Then, the user can access the files on the remote FTP server.

2.1.2 FTP Lighting Procedure

Caution:

The FTP server and the FTP client must be reachable to each other.

I. Enabling FTP server on the switch

After FTP server is enabled on an S3600 switch, the seven-segment digital LED on the front panel of the switch will rotate clockwise when an FTP client is uploading file to the FTP server (the S3600 switch), and will stop rotating when the file uploading is finished, as show in Figure 2-1.

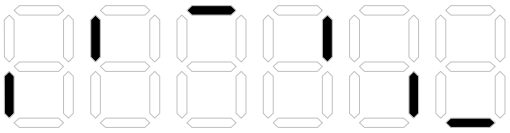


Figure 2-1 Clockwise rotating of the seven-segment digital LED

Table 2-1 Configuration for file upload from an FTP client to the switch acting as FTP server

Device	To do…	Use the command…	Remarks
FTP server (S3600)	Enable FTP server	**ftp sever enable**	Required By default, FTP server is disabled.
	Add a local user and enter local user view	**local-user** *user-name*	Required
	Set a password for the local user	**password** { **simple** | **cipher** } *password*	Required
	Set the password display mode for local users	**local-user password-display-mode** { **auto** | **cipher-force** }	Optional By default, the mode is **auto** (that is, the switch displays user passwords in the modes configured when the passwords are set).
FTP client	Log into the remote FTP server	—	Required For detailed configuration, refer to the configuration instruction relevant to FTP client.
	Upload file from the FTP client to the FTP server	—	Required For detailed configuration, refer to the configuration instruction relevant to FTP client.

II. Enabling FTP client on the switch

After FTP client is enabled on an S3600 switch, the seven-segment digital LED on the front panel of the switch will rotate clockwise when the FTP client (the S3600 switch) is downloading file from an FTP server, and will stop rotating when the file downloading is finished, as show in Figure 2-1.

Table 2-2 Configuration for file download from an FTP server to the switch acting as an FTP client

Device	To do…	Use the command…	Remarks
FTP server	Enable FTP server	—	Required For detailed configuration, refer to the configuration instruction relevant to FTP server.
	Configure authentication/authorization of the FTP server	—	Required For detailed configuration, refer to the configuration instruction relevant to FTP server.
FTP client	Log into the remote FTP server	**ftp** [*ipaddress* [*port*]]	Required • The switch acts as an FTP client by default. • The user should first obtain an FTP user name and password, then log into the remote FTP server. Only after that, can the user obtain the access rights of corresponding directory and file. • When the user logs into the FTP server, the switch enters FTP client command view.
	Download files from the remote FTP server and save the files to the local device	**get** *remotefile* [*localfile*]	Required If no local file name is specified, the system will save the file from the remote FTP server to the local device using the original file name.

2.2 TFTP Lighting Configuration

2.2.1 Introduction to TFTP

Compared with FTP, trivial file transfer protocol (TFTP) does not provide complex interactive access interface and authentication control, and is suitable for the environments that do not need complex interaction. TFTP is implemented based on user datagram protocol (UDP).

The TFTP file transfer is initiated by a client in the following scenarios:

- When a file needs to be downloaded, the client sends a read request to the TFTP server. It then receives data from the server and sends acknowledgement to the server.
- When a file needs to be uploaded, the client sends a write request to the TFTP server. It then sends data to the server and receives acknowledgement from the server.

TFTP can transfer files in two formats:

- Binary: used to transfer programs.
- ASCII code: used to transfer text files.

Before configuring TFTP, the network administrator should first configure the IP addresses of the TFTP client and server and ensure that the client and the server are reachable to each other.

The switch can only act as a TFTP client.

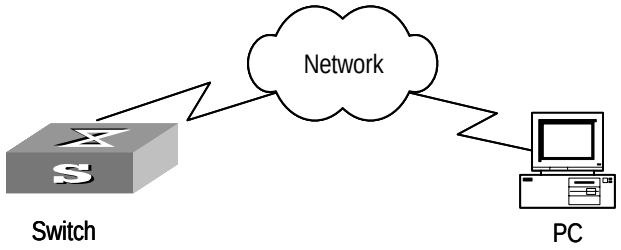


Figure 2-2 Network diagram for TFTP configuration

2.2.2 TFTP Lighting Procedure

Caution:

The TFTP server and the TFTP client must be reachable to each other.

After TFTP client is enabled on an S3600 switch, the seven-segment digital LED on the front panel of the switch will rotate clockwise when the TFTP client (the S3600 switch) is downloading file from a TFTP server, and will stop rotating when the file downloading is finished, as show in Figure 2-1.

Table 2-3 Download file from an TFTP server to the switch acting as an TFTP client

Device	To do…	Use the command…	Remarks
TFTP server	Enable TFTP server	—	Required For detailed configuration, refer to the configuration instruction relevant to TFTP server.
TFTP client	Log into a remote TFTP server, download and save a remote file to the local device	**tftp** *tftp-server* **get** *source-file* [*dest-file*]	Required This command should be executed in user view.

Table of Contents

Chapter 1 FTP and TFTP Configuration 1-1
1.1 FTP Configuration 1-1
1.1.1 Introduction to FTP 1-1
1.1.2 FTP Configuration: A Switch Operating as an FTP Server 1-2
1.1.3 Configuration Example: A Switch Operating as an FTP Server 1-6
1.1.4 FTP Configuration: A Switch Operating as an FTP Client 1-8
1.1.5 Configuration Example: A Switch Operating as an FTP Client 1-11
1.2 TFTP Configuration 1-13
1.2.1 Introduction to TFTP 1-13
1.2.2 TFTP Configuration 1-15
1.2.3 TFTP Configuration Example 1-17

Chapter 1 FTP and TFTP Configuration

1.1 FTP Configuration

1.1.1 Introduction to FTP

FTP (file transfer protocol) is commonly used in IP-based networks to transmit files. Before World Wide Web comes into being, files are transferred through command lines, and the most popular application is FTP. At present, although E-mail and Web are the usual methods for file transmission, FTP still has its strongholds.

As an application layer protocol, FTP is used for file transfer between remote server and local host. FTP uses TCP ports 20 and 21 for data transfer and control command transfer respectively. Basic FTP operations are described in RFC 959.

FTP-based file transmission is performed in the following two modes:

- Binary mode for program file transfer.
- ASCII mode for text file transfer.

An Ethernet switch can act as an FTP client or the FTP server in FTP-employed data transmission:

- FTP server

An Ethernet switch can operate as an FTP server to provide file transmission services for FTP clients. You can log into a switch operating as an FTP server by running an FTP client program on your PC to access files on the FTP server. Before you log into the FTP server, the administrator must configure an IP address for it.

Table 1-1 describes the configurations needed when a switch operates as an FTP server.

Table 1-1 Configurations needed when a switch operates as an FTP server

Device	Configuration	Default	Description
Switch	Enable the FTP server function	The FTP server function is disabled by default	You can run the **display ftp-server** command to view the FTP server configuration on the switch.
	Configure the authentication information on the FTP server	—	Configure user names and passwords.
	Configure the connection idle time	The default idle time is 30 minutes.	—

Device	Configuration	Default	Description
PC	Log into the switch through an FTP client application.	—	—

Caution:

The FTP-related functions require that the route between a FTP client and the FTP server is reachable.

- FTP client

A switch can operate as an FTP client, through which you can access files on FTP servers. In this case, you need to establish a connection between your PC and the switch through a terminal emulation program or Telnet and then execute the **ftp** X.X.X.X command on your PC. (X.X.X.X is the IP address of an FTP server.)

Table 1-2 describes the configurations needed when a switch operates as an FTP client.

Table 1-2 Configurations needed when a switch operates as an FTP client

Device	Configuration	Default	Description
Switch	Run the **ftp** command to log into a remote FTP server directly	—	To log into a remote FTP server and operates files and directories on it, you need to obtain a user name and password first.
FTP server	Enable the FTP server and configure the corresponding information including user names, passwords, and user authorities	—	—

1.1.2 FTP Configuration: A Switch Operating as an FTP Server

I. Prerequisites

A switch operates as an FTP server. A remote PC operates as an FTP client. The network operates properly, as shown in Figure 1-1.

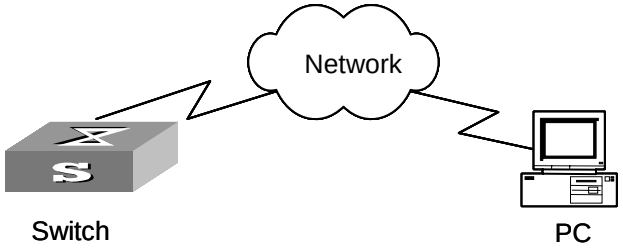


Figure 1-1 Network diagram for FTP configurations

The following configurations are performed on the FTP server:

- Creating local users
- Setting local user passwords
- Setting the password display mode for the local users
- Configuring service types for the local users

For commands used in these configurations, refer to the "AAA-RADIUS-HWTACACS-EAD" module of this manual for: **local-user**, **local-user password-display-mode**, **password**, and **service-type**.

II. Configuration procedure

Table 1-3 Configure an FTP server

Operation	Command	Description
Enter system view	**system-view**	—
Enable the FTP server function	**ftp server enable**	Required By default, the FTP server function is disabled.
Set the connection idle time	**ftp timeout** *minutes*	Optional The default connection idle time is 30 minutes.

Note:

- Only one user can access an S3600 Ethernet switch at a given time when the latter operates as an FTP server. FTP services are implemented in this way: An FTP client sends FTP requests to the FTP server. The FTP server receives the requests, perform operations accordingly, and return the results to the FTP client.
- To prevent unauthorized accesses, an FTP server disconnects a FTP connection when it does not receive requests from the FTP client for a specific period of time known as the connection idle time.
- Operating as an FTP server, an S3600 Ethernet switch cannot receive a file whose size exceeds its storage space. The clients that attempt to upload such a file will be disconnected with the FTP server due to lack of storage space on the FTP server.
- When you log in to a Fabric consisting of multiple switches through an FTP client, after the FTP client passes authentication, you can log in to the master device of the Fabric.

Note:

To protect unused sockets again attacks, the S3600 Ethernet switch provides the following functions:

- TCP 21 is enabled only when you start the FTP server.
- TCP 21 is disabled when you shut down the FTP server.

To use FTP services, a user must provide a user name and a password for being authenticated by the FTP server.

III. Specifying the source interface and source IP address for an FTP server

You can specify the source interface and source IP address for an FTP server to enhance server security. After this configuration, FTP clients can access this server only through the IP address of the specified interface or the specified IP address.

Note:

Source interface refers to the existing VLAN interface or Loopback interface on the device. Source IP address refers to the IP address configured for the interface on the device. Each source interface corresponds to a source IP address. Therefore, specifying a source interface for the FTP server is the same as specifying the IP address of this interface as the source IP address.

Table 1-4 Specify the source interface and source IP address for an FTP server

Operation	Command	Description
Enter system view	**system-view**	—
Specify the source interface for an FTP server	**ftp-server source-interface** *interface-type interface-number*	Optional
Specifying the source IP address for an FTP server	**ftp-server source-ip** *ip-address*	Optional

Note:

- The specified interface must be an existing one. Otherwise a prompt appears to show the configuration fails.
- The value of argument *ip-address* must be an IP address on the device where the configuration is performed. Otherwise a prompt appears to show the configuration fails.
- You may specify only one source interface or source IP address for the FTP at one time. That is, only one of the commands **ftp-server source-interface** and **ftp-server source-ip** can be valid at one time. If you execute both of them, the new setting will overwrite the original one.

IV. Disconnecting a specified user

On the FTP server, you can disconnect a specified user from the FTP server to secure the network.

Table 1-5 Disconnect a specified user

Operation	Command	Description
Enter system view	**system-view**	—
On the FTP server, disconnect a specified user from the FTP server	**ftp disconnect** *user-name*	Required

Note:

If you attempt to disconnect a user that is uploading/downloading data to/from the FTP server that is acted by an S3600 Ethernet switch, the S3600 Ethernet switch will disconnect the user after the data transmission is completed.

V. Displaying FTP server information

After the above configurations, you can run the **display** command in any view to display the running information of the FTP server and verify your configurations.

Table 1-6 Display FTP server information

Operation	Command	Description
Display the information about FTP server configurations on a switch	**display ftp-server**	These commands can be executed in any view.
Display the source IP address set for an FTP server	**display ftp-server source-ip**	
Display the login FTP client on an FTP server	**display ftp-user**	

1.1.3 Configuration Example: A Switch Operating as an FTP Server

I. Network requirements

A switch operates as an FTP server and a remote PC as an FTP client.

- Create a user account on the FTP server with the user name “switch” and password “hello”.
- Configure the IP address 1.1.1.1 for a VLAN interface on the switch, and 2.2.2.2 for the PC. Ensure the route between the two is reachable.

The switch application named switch.bin is stored on the PC. Upload it to the FTP server through FTP to upgrade the application of the switch, and download the switch configuration file named config.cfg from the switch to backup the configuration file.

II. Network diagram

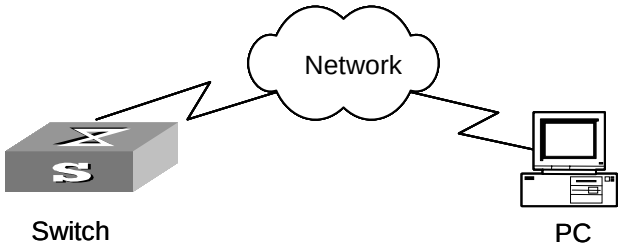


Figure 1-2 Network diagram for FTP configurations

III. Configuration procedure

1) Configure the switch

Log into the switch. (You can log into a switch through the Console port or by Telneting to the switch. See the “Login” module for detailed information.)

```
<H3C>
```

Start the FTP service on the switch and set the user name and the corresponding password.

```
<H3C> system-view
[H3C] ftp server enable
[H3C] local-user switch
[H3C-luser-switch] password simple hello
[H3C-luser-switch] service-type ftp
```

2) Run an FTP client application on the PC to connect to the FTP server. Upload the application named switch.bin to the root directory of the Flash memory of the FTP server, and download the configuration file named config.cfg from the FTP server. The following takes the command line window tool provided by Windows as an example:

Enter the command line window and switch to the directory where the file switch.bin is located. In this example it is in the root directory of C:\.

```
C:\>
```

Access the Ethernet switch through FTP. Input the user name “switch” and password “hello” to log in and enter FTP view.

```
C:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
User (1.1.1.1:(none)): switch
331 Password required for switch.
Password:
230 User logged in.
ftp>
```

Upload the switch.bin file.

```
ftp> put switch.bin
200 Port command okay.
150 Opening ASCII mode data connection for switch.bin.
226 Transfer complete.
```

Download the config.cfg file.

```
ftp> get config.cfg
200 Port command okay.
150 Opening ASCII mode data connection for config.cfg.
226 Transfer complete.
ftp: 3980 bytes received in 8.277 seconds 0.48Kbytes/sec.
```

This example uses the command line window tool provided by Windows. When you log into the FTP server through another FTP client, refer to the corresponding instructions for operation description.

Caution:

- If available space on the Flash memory of the switch is not enough to hold the file to be uploaded, you need to delete files from the Flash memory to make room for the file.
- H3C series switch is not shipped with FTP client applications. You need to purchase and install it by yourself.

3) After uploading the application, you can update the application on the switch.

Use the **boot boot-loader** command to specify the uploaded file (switch.bin) to be the startup file used when the switch starts the next time, and restart the switch. Thus the switch application is upgraded.

```
<H3C> boot boot-loader switch.bin
<H3C> reboot
```

Note:

For information about the **boot boot-loader** command and how to specify the startup file for a switch, refer to the “System Maintenance and Debugging” module of this manual.

1.1.4 FTP Configuration: A Switch Operating as an FTP Client

I. Basic configurations on an FTP client

The function for a switch to operate as an FTP client is implemented by an application module built in the switch. Thus a switch can operate as an FTP client without any configuration. You can perform FTP-related operations (such as creating/removing a directory) by executing FTP client commands on a switch operating as an FTP client connecting with the remote FTP server. Table 1-7 lists the operations that can be performed on an FTP client.

Table 1-7 Basic configurations on an FTP client

Operation	Command	Description
Enter FTP Client view	**ftp** [**cluster** | *remote-server* [*port-number*]]	—
Specify to transfer files in ASCII characters	**ascii**	Optional By default, files are transferred in ASCII characters.
Specify to transfer files in binary streams	**binary**	Optional
Set the data transfer mode to passive	**passive**	Optional By default, the passive mode is adopted.
Change the work directory on the remote FTP server	**cd** *pathname*	Optional
Change the work directory to be the parent directory	**cdup**	Optional
Get the local work path on the FTP client	**lcd**	Optional
Display the work directory on the FTP server	**pwd**	Optional
Create a directory on the remote FTP server	**mkdir** *pathname*	Optional
Remove a directory on the remote FTP server	**rmdir** *pathname*	Optional
Delete a specified file	**delete** *remotefile*	Optional
Query the specified files	**dir** [*filename*] [*localfile*]	Optional
Query a specified remote file	**ls** [*remotefile*] [*localfile*]	Optional
Download a remote file	**get** *remotefile* [*localfile*]	Optional
Upload a local file to the remote FTP server	**put** *localfile* [*remotefile*]	Optional
Rename a file on a remote host.	**rename** *remote-source remote-dest*	Optional
Switch to another FTP user	**user** *username* [*password*]	Optional
Connect to a remote FTP server	**open** { *ip-address* | *server-name* } [*port*]	Optional

Operation	Command	Description
Terminate the current FTP connection without exiting FTP client view	**disconnect**	Optional
Terminate the current FTP connection without exiting FTP client view	**close**	Optional
Terminate the current FTP connection and quit to user view	**quit**	Optional
Terminate the current FTP connection and quit to user view	**bye**	Optional
Display the on-line help on a specified command concerning FTP	**remotehelp** [*protocol-command*]	Optional
Enable verbose function	**verbose**	Optional The verbose function is enabled by default.

II. Specifying the source interface and source IP address for an FTP client

You can specify the source interface and source IP address for a switch acting as an FTP client, so that it can connect to a remote FTP server.

Table 1-8 Specify the source interface and source IP address for an FTP client

Operation	Command	Description
Specify the source interface only used for the current connection	**ftp** { **cluster** | *remote-server* } **source-interface** *interface-type interface-number*	Optional
Specify the source IP address only used for the current connection	**ftp** { **cluster** | *remote-server* } **source-ip** *ip-address*	Optional
Enter system view	**system-view**	—
Specify an interface as the fixed source interface to be used in each connection	**ftp source-interface** *interface-type interface-number*	Optional
Specify an IP address as the fixed source IP address to be used in each connection	**ftp source-ip** *ip-address*	Optional

Operation	Command	Description
Display the fixed source IP address used by a FTP client to connect to a FTP server	**display ftp source-ip**	This command can be executed in any view.

Note:

- The specified interface must be an existing one. Otherwise a prompt appears to show the configuration fails.
- The value of argument *ip-address* must be the IP address of the device where the configuration is performed. Otherwise a prompt appears to show the configuration fails.
- The source interface/source IP address set for one connection is prior to the fixed source interface/source IP address set for each connection. That is, for a connection between an FTP client and an FTP server, if you specify the source interface/source IP address only used for the connection this time, and the specified source interface/source IP address is different from the fixed one, the former will be used for the connection this time.
- Only one fixed source interface or source IP address can be set for the FTP client at one time. That is, only one of the commands **ftp source-interface** and **ftp source-ip** can be effective at one time. If you execute both of them, the new setting will overwrite the original one.

1.1.5 Configuration Example: A Switch Operating as an FTP Client

I. Network requirements

A switch operates as an FTP client and a remote PC as an FTP server.

- Create a user account on the FTP server with the user name “switch” and password “hello”, and authorize the user “switch” with read and write permissions on the directory named “Switch” on the PC.
- Configure the IP address 1.1.1.1 for a VLAN interface on the switch, and 2.2.2.2 for the PC. Ensure the route between the two is reachable.

The switch application named switch.bin is stored on the PC. Download it to the switch through FTP to upgrade the switch application, and upload the switch configuration file named config.cfg to the “switch” directory of the PC to backup the configuration file.

II. Network diagram

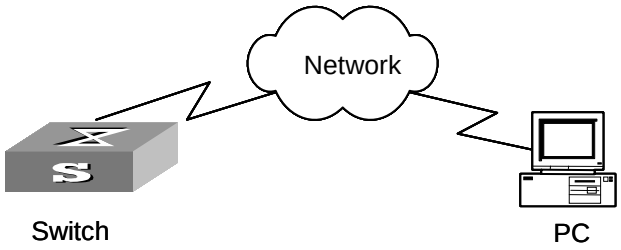


Figure 1-3 Network diagram for FTP configurations

III. Configuration procedure

1) Perform FTP server–related configurations on the PC, that is, create a user account on the FTP server with user name “switch” and password “hello”. (For detailed configuration, refer to the configuration instruction relevant to the FTP server software.)
2) Configure the switch.

Log into the switch. (You can log into a switch through the Console port or by Telneting to the switch. See the “Login” module for detailed information.)

```
<H3C>
```

Caution:

If available space on the Flash memory of the switch is not enough to hold the file to be uploaded, you need to delete files from the Flash memory to make room for the file.

Connect to the FTP server using the **ftp** command in user view. You need to provide the IP address of the FTP server, the user name and the password as well.

```
<H3C> 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]
```

Enter the authorized directory on the FTP server.

```
[ftp] cd switch
```

Run the **put** command to upload the configuration file named config.cfg to the FTP server.

```
[ftp] put config.cfg
```

Run the **get** command to download the file named switch.bin to the Flash memory of the switch.

```
[ftp] get switch.bin
```

Run the **quit** command to terminate the FTP connection and quit to user view.

```
[ftp] quit
<H3C>
```

Run the **boot boot-loader** command to specify the downloaded file (switch.bin) to be the startup file used when the switch starts the next time, and then restart the switch. Thus the switch application is upgraded.

```
<H3C> boot boot-loader switch.bin
<H3C> reboot
```

Note:

For information about the **boot boot-loader** command and how to specify the startup file for a switch, refer to the “System Maintenance and Debugging” module of this manual.

1.2 TFTP Configuration

1.2.1 Introduction to TFTP

Compared with FTP, TFTP (trivial file transfer protocol) features simple interactive access interface and no authentication control. Therefore TFTP is applicable in the networks where client-server interactions are relatively simple. TFTP is implemented based on UDP. It transfers data through UDP port 69. Basic TFTP operations are described in RFC1986.

TFTP transmission is initiated by clients, as described in the following:

- To download a file, a client sends Read Request packets to the TFTP server, then receives data from the TFTP server, and sends acknowledgement packets to the TFTP server.
- To upload a file, a client sends Write Request packets to the TFTP server, then sends data to the TFTP server, and receives acknowledgement packets from the TFTP server.

When you download a file that is larger than the free space of the switch's flash memory:

- If the TFTP server supports file size negotiation, file size negotiation will be initiated between the switch and the server and the file download operation will be aborted if the free space of the switch's flash memory is found to be insufficient.
- If the TFTP server does not support file size negotiation, the switch will receive data from the server until the flash memory is full. If there is more data to be downloaded, the switch will prompt that the space is insufficient and delete the data partially downloaded. File download fails.

TFTP-based file transmission can be performed in the following modes:

- Binary mode for program files transfer.
- ASCII mode for text files transfer.

Note:

- Before performing TFTP-related configurations, you need to configure IP addresses for the TFPT client and the TFTP server, and make sure the route between the two is reachable.
- A switch can only operate as a TFTP client.

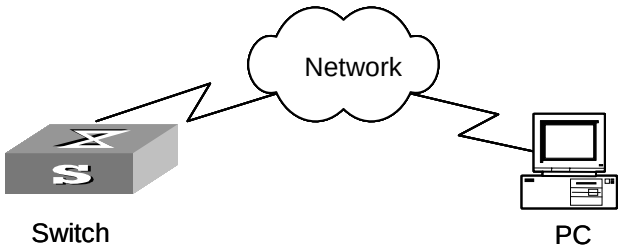


Figure 1-4 Network diagram for TFTP configuration

Table 1-9 describes the operations needed when a switch operates as a TFTP client.

Table 1-9 Configurations needed when a switch operates as a TFTP client

Device	Configuration	Default	Description
Switch	Configure an IP address for the VLAN interface of the switch and make sure the route between the IP address of the VLAN interface and that of the TFTP server is reachable.	—	TFTP applies to networks where client-server interactions are comparatively simple. It requires the routes between TFTP clients and TFTP servers are reachable.
	You can log into a TFTP server directly to upload or download files through TFTP commands.	—	—
TFTP server	The TFTP server is started and the TFTP work directory is configured.	—	—

1.2.2 TFTP Configuration

I. Prerequisites

A switch operates as a TFTP client and a remote PC as the TFTP server. The network operates properly, as shown in Figure 1-4.

II. Basic TFTP configurations

Table 1-10 Basic TFTP configurations

Operation	Command	Description
Download a file through TFTP	**tftp** *tftp-server* **get** *source-file* [*dest-file*]	Optional
Upload a file through TFTP	**tftp** *tftp-server* **put** *source-file* [*dest-file*]	Optional
Enter system view	**system-view**	—
Set the TFTP file transmission mode	**tftp** { **ascii** | **binary** }	Optional By default, the **binary** file transmission mode is adopted.
Specify the ACL adopted when a switch attempts to connect a TFTP server	**tftp-server acl** *acl-number*	Optional

III. Specifying the source interface and source IP address for a TFTP client

You can specify the source interface and source IP address for a switch operating as a TFTP client, so that it can connect with a remote TFTP server through the IP address of the specified interface or the specified IP address.

Table 1-11 Specify the source interface and source IP address for a TFTP client

Operation	Command	Description
Specify the source interface only used for the current connection	**tftp** *tftp-server* **source-interface** *interface-type interface-number* { **get** *source-file* [*dest-file*] | **put** *source-file-url* [*dest-file*] }	Optional
Specify the source IP address only used for the current connection	**tftp** *tftp-server* **source-ip** *ip-address* { **get** *source-file* [*dest-file*] | **put** *source-file-url* [*dest-file*] }	Optional
Enter system view	**system-view**	—
Specify an interface as the fixed source interface to be used in each connection	**tftp source-interface** *interface-type interface-number*	Optional
Specify an IP address as the fixed source IP address to be used in each connection	**tftp source-ip** *ip-address*	Optional
Display the fixed source IP address used by a TFTP client to connect to a TFTP server	**display tftp source-ip**	This command can be executed in any view.

Note:

- The specified interface must be an existing one, and otherwise a prompt appears to show the configuration fails.
- The value of argument *ip-address* must be an IP address on the device where the configuration is performed, and otherwise a prompt appears to show the configuration fails.
- The source interface/source IP address set for one connection is prior to the fixed source interface/source IP address set for each connection. That is, for a connection between a TFTP client and a TFTP server, if you specify the source interface/source IP address only used for the connection this time, and the specified source interface/source IP address is different from the fixed one, the former will be used for the connection this time.
- You may specify only one source interface or source IP address for the TFTP client at one time. That is, only one of the commands **tftp source-interface** and **tftp source-ip** can be effective at one time. If both commands are configured, the one configured later will overwrite the original one.

1.2.3 TFTP Configuration Example

I. Network requirements

A switch operates as a TFTP client and a PC as the TFTP server.

- The TFTP work directory is configured on the TFTP server.
- The IP address of a VLAN interface on the switch is 1.1.1.1. The port through which the switch connects with the PC belongs to the VLAN. The IP address of the PC is 1.1.1.2.

The application named switch.bin is stored on the PC. Download it (switch.bin) to the switch through TFTP, and upload the configuration file named config.cfg to the work directory on the PC to backup the configuration file.

II. Network diagram

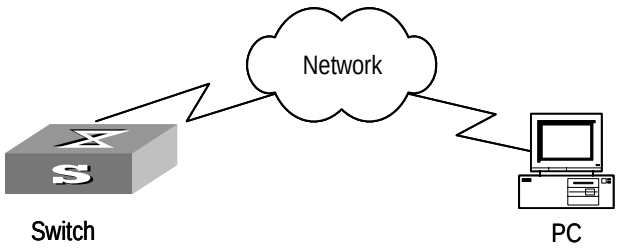


Figure 1-5 Network diagram for TFTP configurations

III. Configuration procedure

1) Start the TFTP server and configure the work directory on the PC.
2) Configure the switch.

Log into the switch. (You can log into a switch through the Console port or by Telneting to the switch. See the “Login” module for detailed information.)

```
<H3C>
```

Caution:

If available space on the Flash memory of the switch is not enough to hold the file to be uploaded, you need to delete files from the Flash memory to make room for the file.

Enter system view

```
<H3C> system-view
[H3C]
```

Configure the IP address of a VLAN interface on the switch to be 1.1.1.1, and ensure that the port through which the switch connects with the PC belongs to this VLAN. (This example assumes that the port belongs to VLAN 1.)

```
[H3C] interface Vlan-interface 1
[H3C-Vlan-interface1] ip address 1.1.1.1 255.255.255.0
[H3C-Vlan-interface1] quit
```

Download the switch application named switch.bin from the TFTP server to the switch.

```
<H3C> tftp 1.1.1.2 get switch.bin switch.bin
```

Upload the switch configuration file named config.cfg to the TFTP server.

```
<H3C> tftp 1.1.1.2 put config.cfg config.cfg
```

Use the **boot boot-loader** command to specify the downloaded file (switch.bin) to be the startup file used when the switch starts the next time, and restart the switch. Thus the switch application is upgraded.

```
<H3C> boot boot-loader switch.bin
<H3C> reboot
```

Note:

For information about the **boot boot-loader** command and how to specify the startup file for a switch, refer to the “System Maintenance and Debugging” module of this manual.

Table of Contents

Chapter 1 Information Center 1-1
1.1 Information Center Overview 1-1
1.2 Information Center Configuration 1-4
1.2.1 Enabling Synchronous Terminal Output 1-5
1.2.2 Enabling Information Output to a Log Host 1-6
1.2.3 Enabling Information Output to the Console 1-7
1.2.4 Enabling Information Output to a Monitor Terminal 1-8
1.2.5 Enabling Information Output to the Log Buffer 1-10
1.2.6 Enabling Information Output to the Trap Buffer 1-11
1.2.7 Enabling Information Output to the SNMP 1-12
1.3 Displaying and Debugging Information Center 1-13
1.4 Information Center Configuration Examples 1-13
1.4.1 Log Output to a UNIX Log Host 1-13
1.4.2 Log Output to a Linux Log Host 1-15
1.4.3 Log Output to the Console 1-17

Chapter 1 Information Center

1.1 Information Center Overview

An information center is an indispensable part of Ethernet switches and exists as an information hub of system software modules. The information center manages most information outputs; it sorts information carefully, and hence can screen information in an efficient way. Combined with the debugging program (**debugging** commands), it provides powerful support for network administrators and developers in network operation monitoring and fault diagnosis.

Information items output by S3600 series switches are presented in the following format:

```
<priority>timestamp sysname module/level/digest:content
```

Here, angle brackets “<>”, spaces, slashes “/” and colon are the fixed format of information.

Below is an example of log output to a log host:

```
<188>Apr  9 17:28:50:524 2004 H3C IFNET/5/UPDOWN:Line protocol on the interface
M-Ethernet0/0/0 is UP    (SIP=10.5.1.5 ,SP=1080)
```

The following describes the fields in front of the content field of an information item:

1) Priority

The calculation formula for priority is priority = facility × 8 + severity – 1. For Comware, the default facility value is 23 and severity ranges from 1 to 8. See Table 1-2 for description of severity levels.

Note that no character is permitted between the priority and time stamp. The priority takes effect only when the information is sent to the log host.

2) Time stamp

The time stamp sent to the log host is in the format of Mmm dd hh:mm:ss:ms yyyy, where:

“Mmm” represents the month, and the available values are: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.

“dd” is the date, which shall follow a space if less than 10, for example, “ 7”.

“hh:mm:ss:ms” is the local time, where “hh” is in the 24-hour format, ranging from 00 to 23, both “mm” and ”ss” range from 00 to 59, “ms” ranges from 000 to 999.

“yyyy” is the year.

Note that a space separates the time stamp and the host name.

3) Host name

It refers to the system name of the host, which is “H3C” by default.

You can modify the host name with the **sysname** command. Refer to System Maintaining and Debugging part of the manual for detailed operations.

Note that a space separates the host name and module name.

4) Module name

It indicates the modules that generate the information. The module name is in abbreviation form to indicate different modules. Table 1-1 lists some modules.

Table 1-1 Examples of modules generating the information

Module name	Description
8021X	802.1x module
ACL	Access control list module
ADBM	Address base module
AM	Access management module
ARP	Address resolution protocol module
CMD	Command line module
DEV	Device management module
DHCP	Dynamic host configuration protocol module
DNS	Domain name system module
ETH	Ethernet module
FIB	Forwarding module
FTM	Fabric topology management module
FTMCMD	Fabric topology management command module
FTPS	FTP server module
HA	High availability module
HABP	Huawei authentication bypass protocol module
HTTPD	HTTP server module
HWCM	Huawei Configuration Management private MIB module
HWP	HWPing module
IFNET	Interface management module
IGSP	IGMP snooping module
IP	Internet protocol module
LAGG	Link aggregation module
LINE	Terminal line module

Module name	Description
MSTP	Multiple spanning tree protocol module
MTRACE	Multicast traceroute query module
NAT	Network address translation module
NDP	Neighbor discovery protocol module
NTDP	Network topology discovery protocol module
NTP	Network time protocol module
OSPF	Open shortest path first module
PKI	Public key infrastructure module
RDS	Radius module
RMON	Remote monitor module
RSA	Revest, Shamir and Adleman encryption module
SHELL	User interface module
SNMP	Simple network management protocol module
SOCKET	Socket module
SSH	Secure shell module
SYSMIB	System MIB module
TAC	HWTACACS module
TELNET	Telnet module
TFTPC	TFTP client module
VLAN	Virtual local area network module
VRRP	VRRP (virtual router redundancy protocol) module
VTY	VTY (virtual type terminal) module
XM	Xmodem module
default	Default settings for all the modules

Note that a slash (/) separates the module name and severity level.

5) Severity

Switch information falls into three categories: log information, debugging information and trap information. The information center classifies the information into eight levels by severity or emergency. The higher the information severity is, the lower the corresponding level is. For example, the “debugging” severity corresponds to level 8, and the “emergencies“ severity corresponds to level 1. If filtered by severity, the information of a severity level greater than the defined threshold will be filtered out for

output. Therefore, when the severity threshold is set to “debugging”, all information will be output. See Table 1-2 for description of severities and corresponding levels.

Table 1-2 Severity definitions on the information center

Severity	Value	Description
emergencies	1	The system is unavailable.
alerts	2	Errors that need to be corrected immediately
critical	3	Critical errors
errors	4	Common errors
warnings	5	Warnings
notifications	6	Normal information that needs to be noticed
informational	7	Normal prompt information
debugging	8	Debugging information

Note that a slash (/) separates the level and digest.

6) Digest

It is a phrase within 32 characters, abstracting the information contents.

A colon (:) separates the digest and information contents.

Note:

The above section describes the log information format sent to a log server by a switch. Some log server software will resolve the received information as well as its format, so that you may see the log format displayed on the log server is different from the one described in this manual.

1.2 Information Center Configuration

The switch supports information output to six directions, and the system defaults to assign one information channel for each output direction, as shown in Table 1-3.

Table 1-3 Information channel names and numbers

Output direction	Channel number	Default channel name
Console	0	console
Monitor terminal	1	monitor
Log host	2	loghost

Output direction	Channel number	Default channel name
Trap buffer	3	trapbuffer
Log buffer	4	logbuffer
SNMP	5	snmpagent

Note:

Settings for the six output directions are independent. However, for any output direction, you must first enable the information center to make all other settings effective.

Information center of the Ethernet switch features:

- Supporting six information output directions, namely, console (console), monitor terminal (monitor), log host (loghost), trap buffer (trapbuffer), log buffer (logbuffer) and SNMP (snmp agent).
- Filtering information by severities (information is divided into eight severity levels).
- Filtering information by modules where information is generated.
- Language options (Chinese or English) for information output to a log host.

1.2.1 Enabling Synchronous Terminal Output

To prevent your input from being interrupted by system information output, you can enable the synchronous terminal output function, which echoes your input after each system output. This makes your work with ease, for you no longer worry about losing uncompleted inputs.

Table 1-4 Enable synchronous terminal output

Operation	Command	Description
Enter system view	**system-view**	—
Enable synchronous terminal output	**info-center synchronous**	Optional By default, synchronous terminal output is disabled.

Note:

Running the **info-center synchronous** command during debugging information collection may result in a command prompt echoed after each item of debugging information. To avoid unnecessary output, you are recommended to disable synchronous terminal output in such cases.

1.2.2 Enabling Information Output to a Log Host

Table 1-5 lists the related configurations on the switch.

Table 1-5 Enable information output to a log host

Operation	Command	Description
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional By default, the information center is enabled.
Enable information output for a specified switch in a fabric	**info-center switch-on** { **unit** *unit-id* | **master** | **all** } [**debugging** | **logging** | **trapping**]*	By default, debugging information output is enabled, and log and trap information output are disabled for the master switch in a fabric. Debugging, log and trap information output are all disabled for other switches in the fabric.
Enable information output to a log host	**info-center loghost** *host-ip-addr* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** { **chinese** | **english** }]*	Required By default, the switch does not output information to the log host. After you configure the switch to output information to the log host, the switch uses information channel 2 by default. Be sure to set the correct IP address. A loopback IP address will cause an error message prompting that this address is invalid.
Configure the source interface through which log information is sent to the log host	**info-center loghost source** *interface-type interface-number*	Optional
Define an information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Required
Set the format of the time stamp to be sent to the log host	**info-center timestamp loghost** { **date** | **no-year-date** | **none** }	Optional

Note:

- After the switches form a fabric, you can use the **info-center switch-on** command to enable the information output for the switch to make the log, debugging and trap information of each switch in the fabric synchronous. Each switch sends its own information to other switches in the fabric and receives information sent by other switches at the same time to update the information on itself. In this way, the switch ensures the synchronization of log, debugging and trap information in the whole fabric.
- To view the debugging information of specific modules, you need to set the information type as **debug** in the **info-center source** command, and enable debugging for corresponding modules through the **debugging** command.

1.2.3 Enabling Information Output to the Console

Table 1-6 lists the related configurations on the switch.

Table 1-6 Enable information output to the console

Operation	Command	Description
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional By default, the information center is enabled.
Enable information output to the console	**info-center console channel** { *channel-number* | *channel-name* }	Required By default, the switch uses information channel 0 to output log/debugging/trap information to the console.
Define an information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Required
Set the format of time stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional

To view log/debugging/trap output information on the console, you should also enable the corresponding log/debugging/trap information terminal display on the switch.

For example, to view log information of the switch on the console, you should not only enable log information output to the console, but also enable log information terminal display with the **terminal logging** command.

Perform the following operations in user view.

Table 1-7 Enable debugging/log/trap terminal display

Operation	Command	Description
Enable the debugging/log/trap information terminal display function	**terminal monitor**	Optional By default, this function is enabled for console users.
Enable debugging information terminal display function	**terminal debugging**	Optional By default, the debugging information terminal display is disabled.
Enable log information terminal display function	**terminal logging**	Optional By default, log information terminal display is enabled.
Enable trap information terminal display function	**terminal trapping**	Optional By default, trap information terminal display is enabled

1.2.4 Enabling Information Output to a Monitor Terminal

Table 1-8 lists the related configurations on the switch.

Table 1-8 Enable information output to a monitor terminal

Operation	Command	Description
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional By default, the information center is enabled.
Enable information output to Telnet terminal or dumb terminal	**info-center monitor channel** { *channel-number* | *channel-name* }	Required By default, a switch outputs log/debugging/trap information to user terminal through information channel 1.

Operation	Command	Description
Define an information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Required
Set the format of time stamp	**info-center timestamp** { **log | trap** | **debugging** } { **boot** | **date** | **none** }	Optional This is to set the time stamp format for log/debugging/trap information output. This determines how the time stamp is presented to users.

Note:

- When there are multiple Telnet users or dumb terminal users, they share some configuration parameters including module filter, language and severity level threshold. In this case, change to any such parameter made by one user will also be reflected on all other user terminals.
- To view debugging information of specific modules, you need to set the information type as **debug** when defining the information source, and enable debugging for corresponding modules through the **debugging** command.

To view the log/debugging/trap output information on the monitor terminal, you should enable the corresponding log/debugging/trap display function on the switch.

For example, to view log information of the switch on a monitor terminal, you need to not only enable log information output to the monitor terminal, but also enable log information terminal display function with the **terminal logging** command.

Perform the following configuration in user view.

Table 1-9 Enable debugging/log/trap terminal display

Operation	Command	Description
Enable the debugging/log/trap information terminal display function	**terminal monitor**	Optional By default, this function is enabled for console users.
Enable debugging information terminal display function	**terminal debugging**	Optional By default, debugging information terminal display is disabled.

Operation	Command	Description
Enable log information terminal display function	**terminal logging**	Optional By default, log information terminal display is enabled.
Enable trap information terminal display function	**terminal trapping**	Optional By default, trap information terminal display is enabled.

1.2.5 Enabling Information Output to the Log Buffer

Table 1-10 lists the related configurations on the switch.

Table 1-10 Enable information output to the log buffer

Operation	Command	Description
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional By default, the information center is enabled.
Enable information output to the log buffer	**info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]*	Optional By default, the switch uses information channel 4 to output log information to the log buffer, which can holds up to 512 items by default.
Define an information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Required
Set the format of time stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional This is to set the time stamp format for log/debugging/trap information output. This determines how the time stamp is presented to users.

Note:

To view debugging information of specific modules, you need to configure the information type as **debug** in the **info-center source** command, and enable debugging on corresponding modules with the **debugging** command as well.

1.2.6 Enabling Information Output to the Trap Buffer

Table 1-11 lists the related configurations on the switch.

Table 1-11 Enable information output to the trap buffer

Operation	Command	Description
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional By default, the information center is enabled.
Enable information output to the trap buffer	**info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]*	Optional By default, the switch uses information channel 3 to output trap information to the trap buffer, which can holds up to 256 items by default.
Define an information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Required
Set the format of time stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional This is to set the time stamp format for log/debugging/trap information output. This determines how the time stamp is presented to users.

Note:

To view debugging information of specific modules, you need to set the information type as **debug** in the **info-center source** command, and enable debugging on corresponding modules with the **debugging** command as well.

1.2.7 Enabling Information Output to the SNMP

Table 1-12 lists the related configurations on the switch.

Table 1-12 Enable information output to the SNMP

Operation	Command	Description
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional By default, the information center is enabled.
Enable information output to the SNMP	**info-center snmp channel** { *channel-number* | *channel-name* }	Required By default, the switch outputs trap information to SNMP through channel 5.
Define an information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Required
Set the format of time stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional This is to set the time stamp format for log/debugging/trap information output. This determines how the time stamp is presented to users.

Note:

- To view debug information of specific modules, you need to set the information type as **debug** in the **info-center source** command, and enable debugging on corresponding modules with the **debugging** command as well.
- To send information to a remote SNMP workstation properly, related configurations are required on both the switch and the SNMP workstation.

1.3 Displaying and Debugging Information Center

After the above configurations, you can execute the **display** command in any view to display the running status of the information center, and thus validating your configurations. You can also execute the **reset** command in user view to clear the information in the log buffer and trap buffer.

Table 1-13 Display and debug information center

Operation	Command	Description
Display information on an information channel	**display channel** [*channel-number* | *channel-name*]	The **display** command can be executed in any view
Display the operation status of information center, the configuration of information channels, the format of time stamp and the information output in case of fabric	**display info-center** [**unit** *unit-id*]	
Display the status of log buffer and the information recorded in log buffer	**display logbuffer** [**unit** *unit-id*] [**level** *severity* | **size** *buffersize*]* [| { **begin** | **exclude** | **include** } *regular-expression*]	
Display the summary information recorded in log buffer	**display logbuffer summary** [**level** *severity*]	
Display the status of trap buffer and the information recorded in trap buffer	**display trapbuffer** [**unit** *unit-id*] [**size** *buffersize*]	
Clear information recorded in log buffer	**reset logbuffer** [**unit** *unit-id*]	The **reset** command can be executed in user view
Clear information recorded in trap buffer	**reset trapbuffer** [**unit** *unit-id*]	

1.4 Information Center Configuration Examples

1.4.1 Log Output to a UNIX Log Host

I. Network requirements

The switch sends the following log information in English to the UNIX log host whose IP address is 202.38.1.10: the log information of the two modules ARP and IP, with severity higher than “informational”.

II. Network diagram

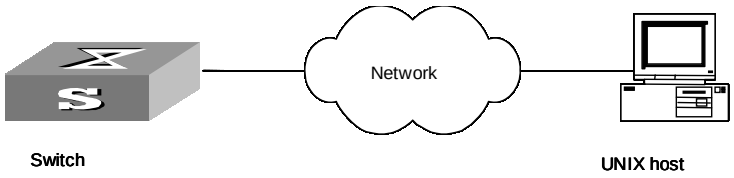


Figure 1-1 Network diagram for log output to a Unix log host

III. Configuration procedure

1) Configure the switch:

Enable the information center.

```
<H3C> system-view
[H3C] info-center enable
```

Disable the function of outputting information to log host channels.

```
[H3C] undo info-center source default channel loghost
```

Configure the host whose IP address is 202.38.1.10 as the log host. Set the output language to English. Permit ARP and IP modules to output information with severity level higher than informational to the log host.

```
[H3C] info-center loghost 202.38.1.10 facility local4 language english
[H3C] info-center source arp channel loghost log level informational debug state off trap state off
[H3C] info-center source ip channel loghost log level informational debug state off trap state off
```

2) Configure the log host:

The operations here are performed on SunOS 4.0. The operations on other manufacturers' UNIX operation systems are similar.

Step 1: Execute the following commands as the super user (root user).

```
# mkdir /var/log/H3C
# touch /var/log/H3C/information
```

Step 2: Edit the file “/etc/syslog.conf” as the super user (root user) to add the following selector/action pairs.

```
# H3C configuration messages
local4.info    /var/log/H3C/information
```

Note:

When you edit the file "/etc/syslog.conf", note that:

- A note must start in a new line, starting with a "#" sign.
- In each pair, a tab should be used as a separator instead of a space.
- No space is allowed at the end of a file name.
- The facility and received log information severity level specified in the file "/etc/syslog.conf" must be the same as those corresponding parameters configured in the commands **info-center loghost** and **info-center source**. Otherwise, log information may not be output to the log host normally.

Step 3: After the log file "information" is created and the file "/etc/syslog.conf" is modified, execute the following command to send a HUP signal to the system daemon "syslogd", so that it can read its new configuration file "/etc/syslog.conf".

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

After all the above operations, the switch can make records in the corresponding log file.

Note:

Through combined configuration of the device name (facility), information severity level threshold (severity), module name (filter) and the file "syslog.conf", you can sort information precisely for filtering.

1.4.2 Log Output to a Linux Log Host

I. Network requirements

The switch sends the following log information in English to the Linux log host whose IP address is 202.38.1.10: All modules' log information, with severity higher than "errors".

II. Network diagram

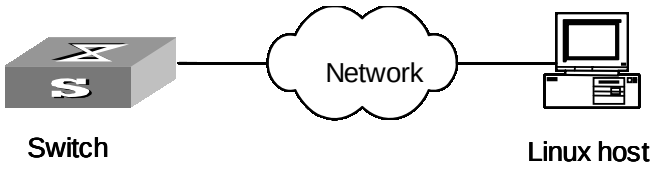


Figure 1-2 Network diagram for log output to a Linux log host

III. Configuration procedure

1) Configure the switch:

Enable the information center.

```
<H3C> system-view
[H3C] info-center enable
```

Configure the host whose IP address is 202.38.1.10 as the log host. Set the output language to English. Permit all modules to output information with severity level higher than error to the log host.

```
[H3C] info-center loghost 202.38.1.10 facility local7 language english
[H3C] info-center source default channel loghost log level errors debug state
off trap state off
```

2) Configure the log host:

Step 1: Execute the following commands as a super user (root user).

```
# mkdir /var/log/H3C
# touch /var/log/H3C/information
```

Step 2: Edit the file “/etc/syslog.conf” as the super user (root user) to add the following selector/action pairs.

```
# H3C configuration messages
local7.info    /var/log/H3C/information
```

Note:

Note the following items when you edit file “/etc/syslog.conf”.

- A note must start in a new line, starting with a “#" sign.
- In each pair, a tab should be used as a separator instead of a space.
- No space is permitted at the end of the file name.
- The facility and received log information severity specified in file “/etc/syslog.conf” must be the same with those corresponding parameters configured in commands **info-center loghost** and **info-center source**. Otherwise, log information may not be output to the log host normally.

Step 3: After the log file “information” is created and the file “/etc/syslog.conf” is modified, execute the following commands to view the process ID of the system daemon “syslogd”, stop the process, and then restart the daemon "syslogd" in the background with the “-r” option.

```
# ps -ae | grep syslogd
147
# kill -9 147
```

```
# syslogd -r &
```

Note:

In case of Linux log host, the daemon “syslogd” must be started with the “-r” option.

After all the above operations, the switch can record information in the corresponding log file.

Note:

Through combined configuration of the device name (facility), information severity level threshold (severity), module name (filter) and the file “syslog.conf”, you can sort information precisely for filtering.

1.4.3 Log Output to the Console

I. Network requirements

The switch sends the following information to the console: the log information of the two modules ARP and IP, with severity higher than “informational”.

II. Network diagram

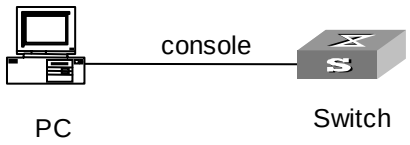


Figure 1-3 Network diagram for log output to the console

III. Configuration procedure

Enable the information center.

```
<H3C> system-view
[H3C] info-center enable
```

Disable the function of outputting information to the console channels.

```
[H3C] undo info-center source default channel console
```

Enable log information output to the console. Permit ARP and IP modules to output information with severity level higher than informational to the console.

```
[H3C] info-center console channel console
[H3C] info-center source arp channel console log level informational debug
state off trap state off
[H3C] info-center source ip channel console log level informational debug state
off trap state off
```

Enable terminal display.

```
<H3C> terminal monitor
<H3C> terminal logging
```

Table of Contents

Chapter 1 BootROM and Host Software Loading 1-1
1.1 Introduction to Loading Approaches 1-1
1.2 Local BootROM and Software Loading 1-1
1.2.1 BOOT Menu 1-2
1.2.2 Loading by XModem through Console Port 1-3
1.2.3 Loading by TFTP through Ethernet Port 1-8
1.2.4 Loading by FTP through Ethernet Port 1-10
1.3 Remote BootROM and Software Loading 1-12
1.3.1 Remote Loading Using FTP 1-12
1.3.2 Remote Loading Using TFTP 1-18

Chapter 2 Basic System Configuration & Debugging 2-1
2.1 Basic System Configuration 2-1
2.1.1 Basic System Configuration Tasks 2-1
2.1.2 Entering System View from User View 2-1
2.1.3 Setting the System Name of the Switch 2-2
2.1.4 Setting the Date and Time of the System 2-2
2.1.5 Setting the Local Time Zone 2-2
2.1.6 Setting the Summer Time 2-2
2.1.7 Setting the CLI Language Mode 2-3
2.1.8 Returning from Current View to Lower Level View 2-3
2.1.9 Returning from Current View to User View 2-3
2.2 Displaying the System Status 2-3
2.3 Debugging the System 2-4
2.3.1 Enabling/Disabling System Debugging 2-4
2.3.2 Displaying Debugging Status 2-6
2.3.3 Displaying Operating Information about Modules in System 2-6

Chapter 3 Network Connectivity Test 3-1
3.1 Network Connectivity Test 3-1
3.1.1 ping 3-1
3.1.2 tracert 3-1

Chapter 4 Device Management 4-1
4.1 Introduction to Device Management 4-1
4.2 Device Management Configuration 4-1
4.2.1 Device Management Configuration Tasks 4-1
4.2.2 Rebooting the Ethernet Switch 4-1
4.2.3 Scheduling a Reboot on the Switch 4-2
4.2.4 Specifying the APP to be Adopted at Reboot 4-2

4.2.5 Upgrading the BootROM 4-3
4.2.6 Upgrading the Host Software in the Fabric 4-3
4.3 Displaying the Device Management Configuration 4-3
4.4 Remote Switch Upgrade Configuration Example 4-4

Chapter 1 BootROM and Host Software Loading

Traditionally, switch software is loaded through a serial port. This approach is slow, time-consuming and cannot be used for remote loading. To resolve these problems, the TFTP and FTP modules are introduced into the switch. With these modules, you can load/download software/files conveniently to the switch through an Ethernet port.

This chapter introduces how to load BootROM and host software to a switch locally and remotely.

1.1 Introduction to Loading Approaches

You can load software locally by using:

- XModem through Console port
- TFTP through Ethernet port
- FTP through Ethernet port

You can load software remotely by using:

- FTP
- TFTP

Note:

The BootROM software version should be compatible with the host software version when you load the BootROM and host software.

1.2 Local BootROM and Software Loading

If your terminal is directly connected to the switch, you can load the BootROM and host software locally.

Before loading the software, make sure that your terminal is correctly connected to the switch.

Note:

The loading process of the BootROM software is the same as that of the host software, except that during the former process, you should press <Ctrl+U> and <Enter> after entering the BOOT menu and the system gives different prompts. The following text mainly describes the BootROM loading process.

1.2.1 BOOT Menu

```
Starting......



          ************************************************************
          *                                                          *
          *          H3C S3600-28P-SI BOOTROM, Version 320           *
          *                                                          *
          ************************************************************

          Copyright(c) 2004-2007 Hangzhou H3C Technologies Co., Ltd.
          Creation date   : Apr  10 2007, 15:30:51
          CPU type        : BCM4704
          CPU Clock Speed : 200MHz
          BUS Clock Speed : 33MHz
          Memory Size     : 64MB
          Mac Address     : 00e0fc123450


Press Ctrl-B to enter Boot Menu...
```

Press <Ctrl+B>. The system displays:

```
Password :
```

Note:

To enter the BOOT menu, you should press <Ctrl+B> within five seconds after the information “Press Ctrl-B to enter BOOT Menu...” displays. Otherwise, the system starts to extract the program; and if you want to enter the BOOT Menu at this time, you will have to restart the switch.

Enter the correct BootROM password (no password is need by default). The system enters the BOOT Menu:

```
              BOOT  MENU


1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Enter your choice(0-9):
```

1.2.2 Loading by XModem through Console Port

I. Introduction to XModem

XModem protocol is a file transfer protocol that is widely used due to its simplicity and good performance. The XModem protocol transfers files through Console port. It supports two types of data packets (128 bytes and 1 KB), two check methods (checksum and CRC), and multiple attempts of error packet retransmission (generally the maximum number of retransmission attempts is ten).

The XModem transmission procedure is completed by a receiving program and a sending program. The receiving program sends negotiation characters to negotiate a packet checking method. After the negotiation, the sending program starts to transmit data packets. When receiving a complete packet, the receiving program checks the packet using the agreed method. If the check succeeds, the receiving program sends acknowledgement characters and the sending program proceeds to send another packet. If the check fails, the receiving program sends negative acknowledgement characters and the sending program retransmits the packet.

II. Loading BootROM

Follow these steps to load the BootROM:

Step 1: At the prompt "Enter your choice(0-9):" in the BOOT Menu, press <6> or <Ctrl+U>, and then press <Enter> to enter the BootROM update menu shown below:

```
Bootrom update menu:
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
```

```
3. Set XMODEM protocol parameter
0. Return to boot menu
Enter your choice(0-3):
```

Step 2: Press 3 in the above menu to download the BootROM using XModem. The system displays the following setting menu for download baudrate:

```
Please select your download baudrate:
1.* 9600
2. 19200
3. 38400
4. 57600
5. 115200
0. Return
Enter your choice (0-5):
```

Step 3: Choose an appropriate download baudrate. For example, if you press 5, the baudrate 115200 bps is chosen and the system displays the following information:

```
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

Note:

If you have chosen 9600 bps as the download baudrate, you need not modify the HyperTerminal's baudrate, and therefore you can skip Step 4 and 5 below and proceed to Step 6 directly. In this case, the system will not display the above information.

Following are configurations on PC. Take the HyperTerminal in Windows operating system as an example.

Step 4: Choose [File/Properties] in HyperTerminal, click <Configure> in the pop-up dialog box, and then select the baudrate of 115200 bps in the Console port configuration dialog box that appears, as shown in Figure 1-1, Figure 1-2.

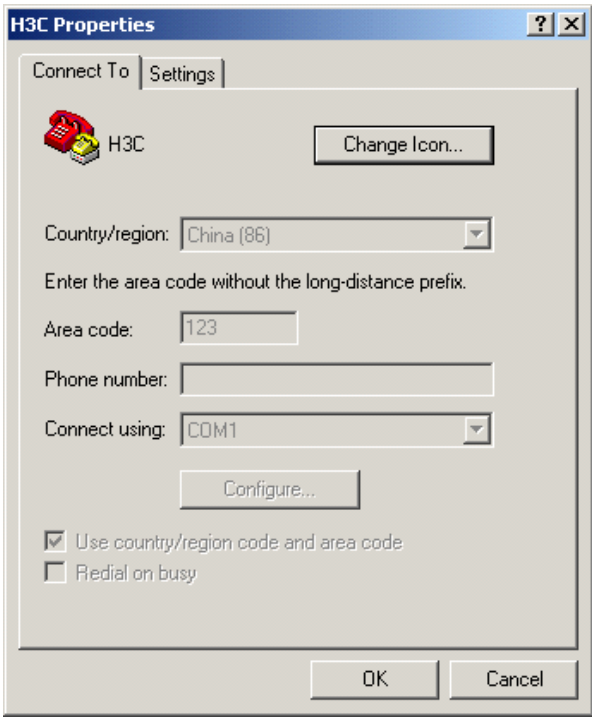


Figure 1-1 Properties dialog box

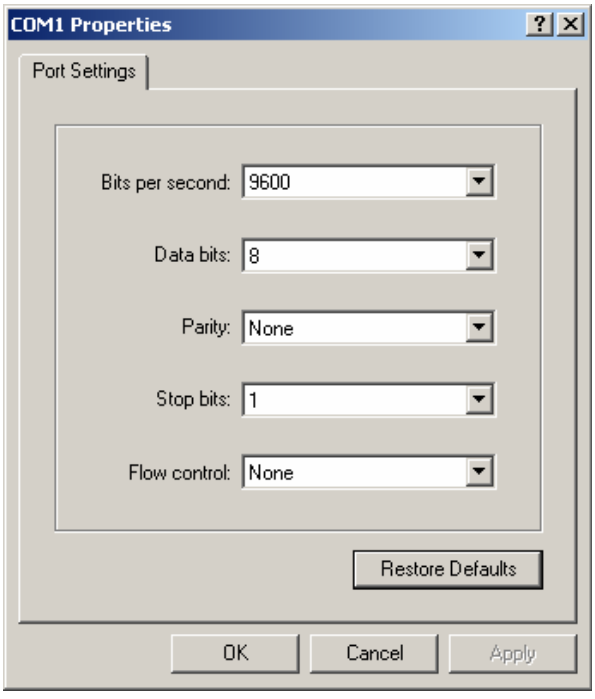


Figure 1-2 Console port configuration dialog box

Step 5: Click the <Disconnect> button to disconnect the HyperTerminal from the switch and then click the <Connect> button to reconnect the HyperTerminal to the switch, as shown in Figure 1-3.

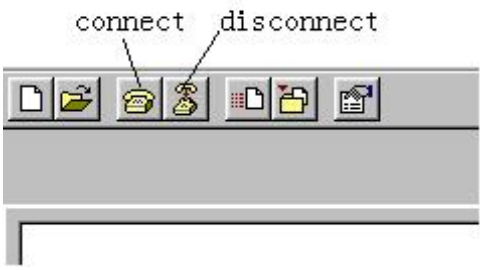


Figure 1-3 Connect and disconnect buttons

Note:

The new baudrate takes effect after you disconnect and reconnect the HyperTerminal program.

Step 6: Press <Enter> to start downloading the program. The system displays the following information:

```
Now please start transfer file with XMODEM protocol.
If you want to exit, Press <Ctrl+X>.
Loading ...CCCCCCCCCC
```

Step 7: Choose [Transfer/Send File] in HyperTerminal, and click <Browse> in pop-up dialog box, as shown in Figure 1-4. Select the software file that you need to load to the switch, and set the protocol to XModem.

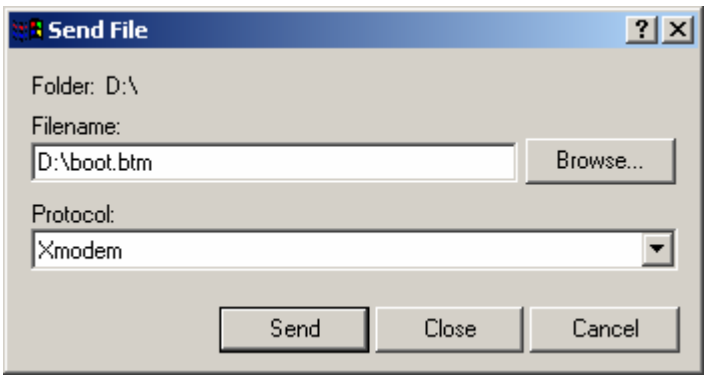


Figure 1-4 Send file dialog box

Step 8: Click <Send>. The system displays the page, as shown in Figure 1-5.

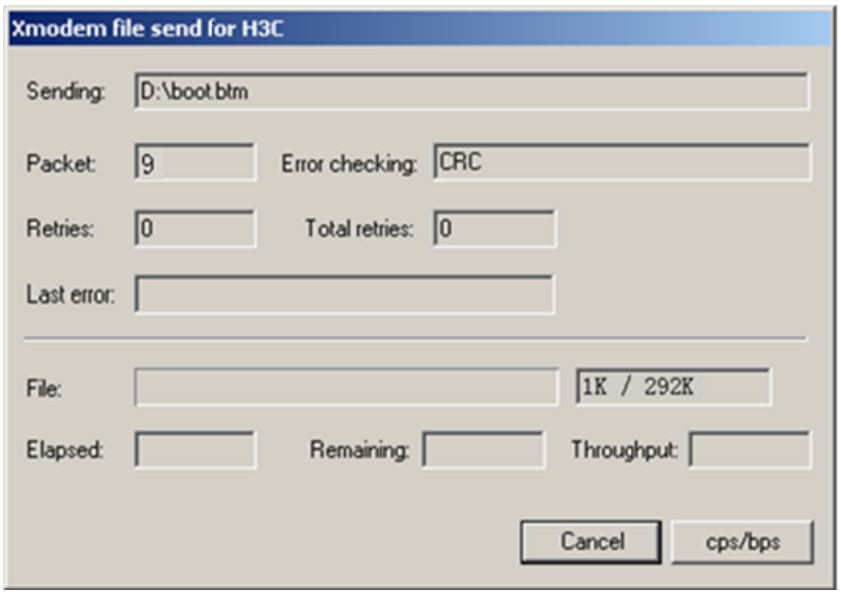


Figure 1-5 Sending file page

Step 9: After the sending process completes, the system displays the following information:

```
Loading ...CCCCCCCCCC done!
```

Step 10: Reset HyperTerminal's baudrate to 9600 bps (refer to Step 4 and 5). Then, press any key as prompted. The system will display the following information when it completes the loading.

```
Bootrom updating.....................................done!
```

Note:

- If the HyperTerminal's baudrate is not reset to 9600 bps, the system prompts "Your baudrate should be set to 9600 bps again! Press enter key when ready".
- You need not reset the HyperTerminal's baudrate and can skip the last step if you have chosen 9600 bps. In this case, the system upgrades BootROM automatically and prompts "Bootrom updating now.....done!".

III. Loading host software

Follow these steps to load the host software:

Step 1: Select <1> in BOOT Menu and press <Enter>. The system displays the following information:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
```

```
3. Set XMODEM protocol parameter
0. Return to boot menu
Enter your choice(0-3):
```

Step 2: Enter 3 in the above menu to load the host software by using XModem.

The subsequent steps are the same as those for loading the BootROM, except that the system gives the prompt for host software loading instead of BootROM loading.

Note:

You can use the **xmodem get** command to upload files locally to the switch through Console ports (AUX ports) as follows (assuming that the PC connects to the switch and logs in to the switch through a Console port):

- Execute the **xmodem get** command in user view on the device. After you execute this command successfully, the switch is ready for receiving data.
- Launch HyperTerminal on the PC, specify XModem as the transmission protocol, and make the transmission settings (that is, baud rate, data bits, parity, etc.) the same as those of the Console port of the switch.
- Select the files to be uploaded to the switch on the super terminal and then send them.

1.2.3 Loading by TFTP through Ethernet Port

I. Introduction to TFTP

TFTP, a protocol in TCP/IP protocol suite, is used for trivial file transfer between client and server. It is over UDP to provide unreliable data stream transfer service.

II. Loading BootROM

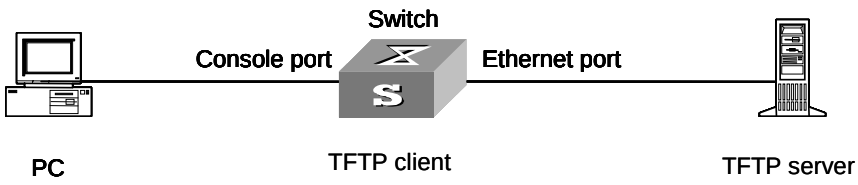


Figure 1-6 Local loading using TFTP

Step 1: As shown in Figure 1-6, connect the switch through an Ethernet port to the TFTP server, and connect the switch through the Console port to the configuration PC.

Note:

You can use one PC as both the configuration device and the TFTP server.

Step2: Run the TFTP server program on the TFTP server, and specify the path of the program to be downloaded.

Caution:

TFTP server program is not provided with the H3C Series Ethernet Switches.

Step 3: Run the HyperTerminal program on the configuration PC. Start the switch. Then enter the BOOT Menu.

At the prompt "Enter your choice(0-9):" in the BOOT Menu, press <6> or <Ctrl+U>, and then press <Enter> to enter the BootROM update menu shown below:

```
Bootrom update menu:
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu
Enter your choice(0-3):
```

Step 4: Enter 1 in the above menu to download the BootROM using TFTP. Then set the following TFTP-related parameters as required:

```
Load File name           :S3600.btm
Switch IP address        :1.1.1.2
Server IP address        :1.1.1.1
```

Step 5: Press <Enter>. The system displays the following information:

```
Are you sure to update your bootrom?Yes or No(Y/N)
```

Step 6: Enter Y to start file downloading or N to return to the Bootrom update menu. If you enter Y, the system begins to download and update the BootROM. Upon completion, the system displays the following information:

```
Loading.....................................done
Bootrom updating.........done!
```

III. Loading host software

Follow these steps to load the host software.

Step 1: Select <1> in BOOT Menu and press <Enter>. The system displays the following information:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu
Enter your choice(0-3):3
```

Step 2: Enter 1 in the above menu to download the host software using TFTP.

The subsequent steps are the same as those for loading the BootROM, except that the system gives the prompt for host software loading instead of BootROM loading.

Caution:

When loading BootROM and host software using TFTP through BOOT menu, you are recommended to use the PC directly connected to the device as TFTP server to promote upgrading reliability.

1.2.4 Loading by FTP through Ethernet Port

I. Introduction to FTP

FTP is an application-layer protocol in the TCP/IP protocol suite. It is used for file transfer between server and client, and is widely used in IP networks.

You can use the switch as an FTP client or a server, and download software to the switch through an Ethernet port. The following is an example.

II. Loading Procedure Using FTP Client

- Loading BootROM

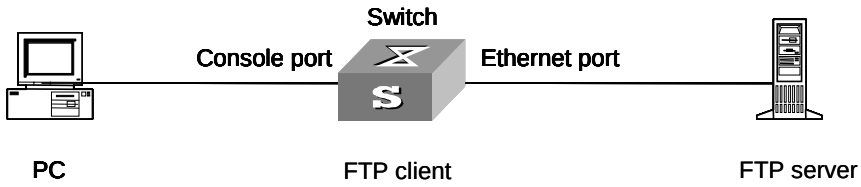


Figure 1-7 Local loading using FTP client

Step 1: As shown in Figure 1-7, connect the switch through an Ethernet port to the FTP server, and connect the switch through the Console port to the configuration PC.

Note:

You can use one computer as both configuration device and FTP server.

Step 2: Run the FTP server program on the FTP server, configure an FTP user name and password, and copy the program file to the specified FTP directory.

Step 3: Run the HyperTerminal program on the configuration PC. Start the switch. Then enter the BOOT Menu.

At the prompt "Enter your choice(0-9):" in the BOOT Menu, press <6> or <Ctrl+U>, and then press <Enter> to enter the BootROM update menu shown below:

```
Bootrom update menu:


1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu
Enter your choice(0-3):
```

Step 4: Enter 2 in the above menu to download the BootROM using FTP. Then set the following FTP-related parameters as required:

```
Load File name           :S3600.btm
Switch IP address        :10.1.1.2
Server IP address        :10.1.1.1
FTP User Name            :3600
FTP User Password        :abc
```

Step 5: Press <Enter>. The system displays the following information:

```
Are you sure to update your bootrom?Yes or No(Y/N)
```

Step 6: Enter Y to start file downloading or N to return to the Bootrom update menu. If you enter Y, the system begins to download and update the program. Upon completion, the system displays the following information:

```
Loading.....................................done
Bootrom updating.........done!
```

- Loading host software

Follow these steps to load the host software:

Step 1: Select <1> in BOOT Menu and press <Enter>. The system displays the following information:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu
```

```
Enter your choice(0-3):
```

Enter 2 in the above menu to download the host software using FTP.

The subsequent steps are the same as those for loading the BootROM, except for that the system gives the prompt for host software loading instead of BootROM loading.

Caution:

When loading BootROM and host software using FTP through BOOT menu, you are recommended to use the PC directly connected to the device as FTP server to promote upgrading reliability.

1.3 Remote BootROM and Software Loading

If your terminal is not directly connected to the switch, you can telnet to the switch, and use FTP or TFTP to load BootROM and host software remotely.

1.3.1 Remote Loading Using FTP

I. Loading Procedure Using FTP Client

1) Loading BootROM

As shown in Figure 1-8, a PC is used as both the configuration device and the FTP server. You can telnet to the switch, and then execute the FTP commands to download the BootROM program S3600.btm from the remote FTP server (whose IP address is 10.1.1.1) to the switch.

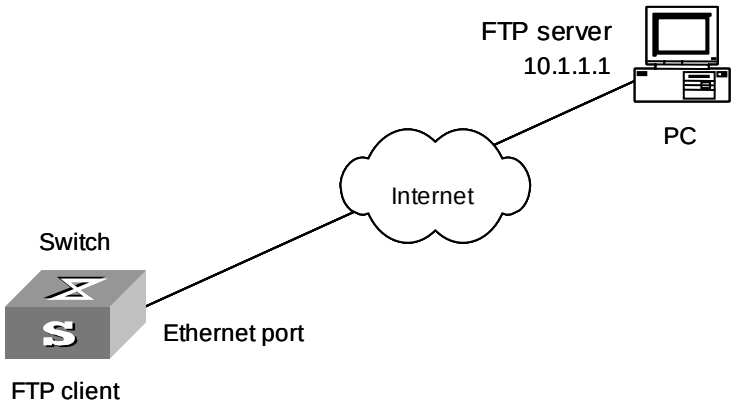


Figure 1-8 Remote loading using FTP Client

Step 1: Download the program to the switch using FTP commands.

```
<H3C> ftp 10.1.1.1
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):abc
331 Give me your password, please
Password:
230 Logged in successfully
[ftp] get S3600.btm
[ftp] bye
```

Note:

When using different FTP server software on PC, different information will be output to the switch.

Step 2: Update the BootROM program on the switch.

```
<H3C> boot bootrom S3600.btm
 This will update BootRom file on unit 1. Continue? [Y/N] y
 Upgrading BOOTROM, please wait...
 Upgrade BOOTROM succeeded!
```

Step 3: Restart the switch.

```
<H3C> reboot
```

Note:

Before restarting the switch, make sure you have saved all other configurations that you want, so as to avoid losing configuration information.

2) Loading host software

Loading the host software is the same as loading the BootROM program, except that the file to be downloaded is the host software file, and that you need to use the **boot boot-loader** command to select the host software used for next startup of the switch.

After the above operations, the BootROM and host software loading is completed.

Pay attention to the following:

- The loading of BootROM and host software takes effect only after you restart the switch with the **reboot** command.

- If the space of the Flash memory is not enough, you can delete the unused files in the Flash memory before software downloading.
- Ensure the power supply during software loading.

II. Loading Procedure Using FTP Server

As shown in Figure 1-9, the switch is used as the FTP server. You can telnet to the switch, and then execute the FTP commands to download the BootROM program S3600.btm from the switch.

1) Loading BootROM

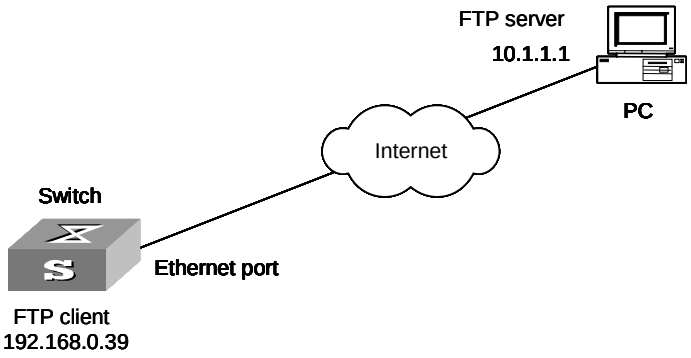


Figure 1-9 Remote loading using FTP server

Step 1: As shown in Figure 1-9, connect the switch through an Ethernet port to the PC (whose IP address is 10.1.1.1)

Step 2: Configure the IP address of VLAN-interface 1 on the switch to 192.168.0.39, and subnet mask to 255.255.255.0.

Note:

You can configure the IP address for any VLAN on the switch for FTP transmission. However, before configuring the IP address for a VLAN interface, you have to make sure whether the IP addresses of this VLAN and PC are routable.

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] interface Vlan-interface 1
[H3C-Vlan-interface1] ip address 192.168.0.39 255.255.255.0
```

Step 3: Enable FTP service on the switch, and configure the FTP user name to test and password to pass.

```
[H3C-Vlan-interface1] quit
[H3C] ftp server enable
```

```
[H3C] local-user test
New local user added.
[H3C-luser-test] password simple pass
[H3C-luser-test] service-type ftp
```

Step 4: Enable FTP client software on the PC. Refer to Figure 1-10 for the command line interface in Windows operating system.



Figure 1-10 Command line interface

Step 5: Use the **cd** command on the interface to enter the path that the BootROM upgrade file is to be stored. Assume the name of the path is D:\Bootrom, as shown in Figure 1-11.

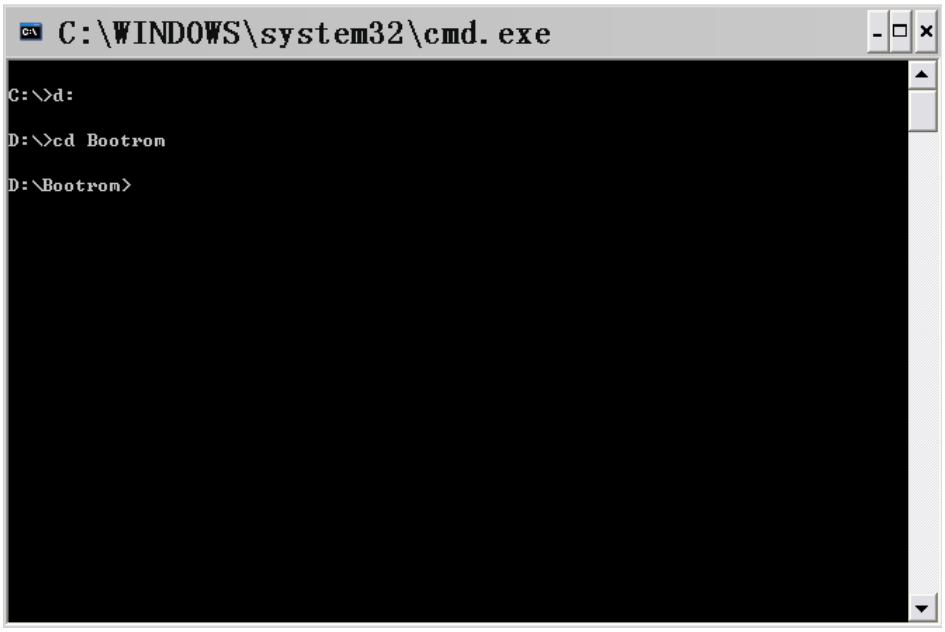


Figure 1-11 Enter BootROM directory

Step 6: Enter **ftp 192.168.0.39** and enter the user name test, password pass, as shown in Figure 1-12, to log on to the FTP server.

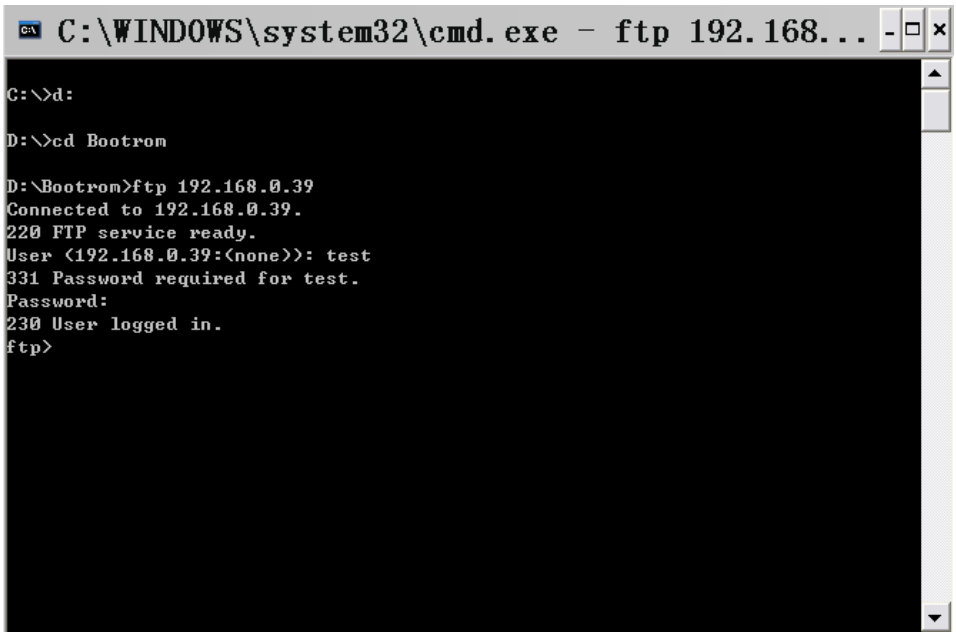


Figure 1-12 Log on to the FTP server

Step 7: Use the **put** command to upload the file S3600.btm to the switch, as shown in Figure 1-13.

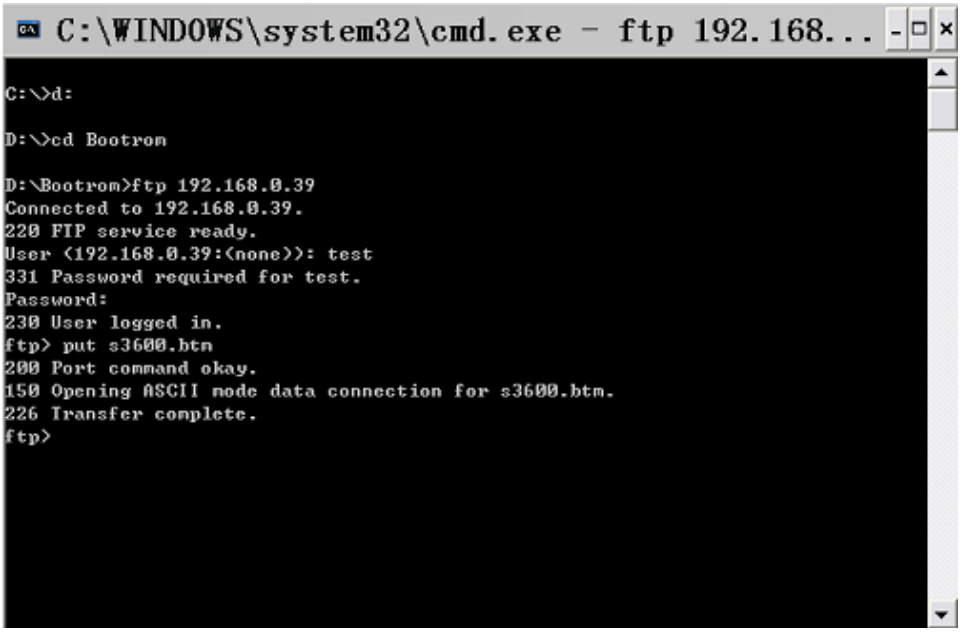


Figure 1-13 Upload file S3600.btm to the switch

Step 8: Configure S3600.btm to be the BootROM at next startup, and then restart the switch.

```
<H3C> boot bootrom S3600.btm
 This will update Bootrom on unit 1.  Continue? [Y/N] y
 Upgrading Bootrom, please wait...
 Upgrade Bootrom succeeded!
<H3C> reboot
```

After the switch restarts, the file S3600.btm is used as the BootROM. It indicates that the BootROM loading is finished.

2) Loading host software

Loading the host software is the same as loading the BootROM program, except that the file to be downloaded is the host software file, and that you need to use the **boot boot-loader** command to select the host software used for the next startup of the switch.

Note:

- The steps listed above are performed in the Windows operating system, if you use other FTP client software, refer to the corresponding user guide before operation.
- Only the configuration steps concerning loading are listed here. For detailed description on the corresponding configuration commands, refer to module “FTP and TFTP” of this manual.

1.3.2 Remote Loading Using TFTP

The remote loading using TFTP is similar to that using FTP. The only difference is that TFTP is used to load software to the switch, and the switch can only act as a TFTP client.

Chapter 2 Basic System Configuration & Debugging

2.1 Basic System Configuration

2.1.1 Basic System Configuration Tasks

Table 2-1 Basic system configuration tasks

Operation	Description	Related section
Enter system view from user view	—	Section 2.1.2 "Entering System View from User View"
Set the system name of the switch	Optional	Section 2.1.3 "Setting the System Name of the Switch"
Set the date and time of the system	Optional	Section 2.1.4 "Setting the Date and Time of the System"
Set the local time zone	Optional	Section 2.1.5 "Setting the Local Time Zone"
Set the summer time	Optional	Section 2.1.6 "Setting the Summer Time"
Set the CLI language mode	Optional	Section 2.1.7 "Setting the CLI Language Mode"
Return from current view to lower level view	—	Section 2.1.8 "Returning from Current View to Lower Level View"
Return from current view to user view	—	Section 2.1.9 "Returning from Current View to User View"

2.1.2 Entering System View from User View

Table 2-2 Enter system view from user view

Operation	Command	Description
Enter system view from user view	**system-view**	—

2.1.3 Setting the System Name of the Switch

Table 2-3 Set the system name of the switch

Operation	Command	Description
Enter system view	**system-view**	—
Set the system name of the switch	**sysname** *sysname*	Optional By default, the name is H3C.

2.1.4 Setting the Date and Time of the System

Table 2-4 Set the date and time of the system

Operation	Command	Description
Set the current date and time of the system	**clock datetime** *HH:MM:SS YYYY/MM/DD*	Optional The initial value is 23:55:00 04/01/2000 when the system starts up.

2.1.5 Setting the Local Time Zone

This configuration task is to configure the name of the local time zone and the difference between the local time zone and the standard universal time coordinated (UTC) time.

Table 2-5 Set the local time zone

Operation	Command	Description
Set the local time zone	**clock timezone** *zone-name* { **add** | **minus** } *HH:MM:SS*	Optional By default, it is the UTC time zone.

2.1.6 Setting the Summer Time

This configuration task is to set the name, time range (start time and end time), and time offset of the summer timer.

- When the system reaches the specified start time, it automatically adds the specified offset to the current time, so as to toggle the system time to the summer time.
- When the system reaches the specified end time, it automatically subtracts the specified offset from the current time, so as to toggle the summer time to normal system time.

Table 2-6 Set the summer time

Operation	Command	Description
Set the name and time range of the summer time	**clock summer-time** *zone_name* { **one-off** | **repeating** } *start-time start-date end-time end-date offset-time*	Optional

2.1.7 Setting the CLI Language Mode

Table 2-7 Set the CLI language mode

Operation	Command	Description
Set the CLI language mode	**language-mode** { **chinese** | **english** }	Optional By default, the CLI language mode is English.

2.1.8 Returning from Current View to Lower Level View

Table 2-8 Return from current view to lower level view

Operation	Command	Description
Return from current view to lower level view	**quit**	This operation will result in exiting the system if current view is user view.

2.1.9 Returning from Current View to User View

Table 2-9 Return from current view to user view

Operation	Command	Description
Return from current view to user view	**return**	The composite key <Ctrl+Z> has the same effect with the **return** command.

2.2 Displaying the System Status

You can use the following **display** commands to check the status and configuration information about the system. For information about protocols and ports, and the associated **display** commands, refer to relevant sections.

Table 2-10 System information **display** commands

Operation	Command	Description
Display the current date and time of the system	**display clock**	You can execute the **display** command in any view
Display the version of the system	**display version**	
Display the information about user accessing the switch	**display users** [**all**]	
Display the debugging status	**display debugging** { **fabric** | **unit** *unit-id* } [**interface** *interface-type interface-number* | *module-name*]	

2.3 Debugging the System

2.3.1 Enabling/Disabling System Debugging

The Ethernet switch provides a variety of debugging functions. Most of the protocols and features supported by the Ethernet switch are provided with corresponding debugging functions. These debugging functions help users diagnose and troubleshoot the system faults.

The output of debugging information is determined by the following two settings:

- Protocol debugging setting, which controls whether the debugging information of a protocol is output.
- Terminal display setting, which controls whether the debugging information is output to the screen of a specific user.

The relationship between the two settings is as follows:

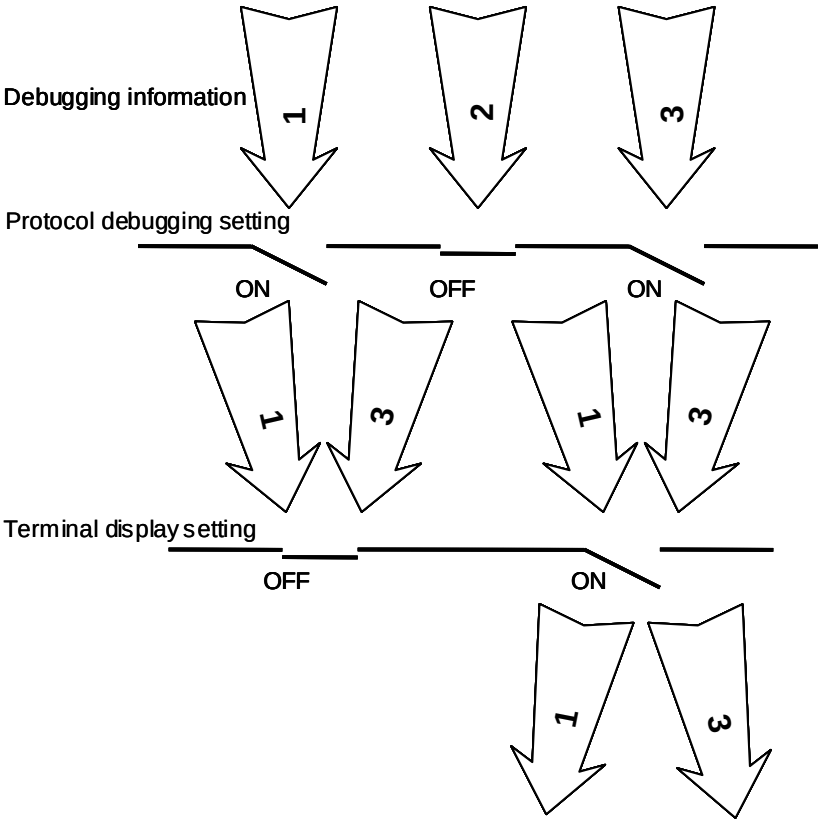


Figure 2-1 Debugging information output

You can use the following commands to perform the settings.

Table 2-11 Enable debugging and terminal display

Operation	Command	Description
Enable system debugging for specific module	**debugging** *module-name* [*debugging-option*]	By default, all debugging is disabled in the system. Because the output of debugging information will affect the efficiency of the system, disable your debugging after you finish it.
Enable terminal display for debugging	**terminal debugging**	By default, terminal display for debugging is disabled.

2.3.2 Displaying Debugging Status

Table 2-12 Display the current debugging status in the system

Operation	Command	Description
Display all enabled debugging on the specified device	**display debugging** { **fabric** | **unit** *unit-id* } [**interface** *interface-type interface-number* | *module-name*]	You can execute the **display** command in any view.
Display all enabled debugging in the Fabric by module	**display debugging fabric by-module**	

2.3.3 Displaying Operating Information about Modules in System

When an Ethernet switch is in trouble, you may need to view a lot of operating information to locate the problem. Each functional module has its corresponding operating information display command(s). You can use the command here to display the current operating information about the modules in the system for troubleshooting your system.

Table 2-13 Display the current operation information about the modules in the system.

Operation	Command	Description
Display the current operation information about the modules in the system.	**display diagnostic-information**	You can use this command in any view. You should execute this command twice to find the difference between the two executing results, thus helping locate the problem.

Chapter 3 Network Connectivity Test

3.1 Network Connectivity Test

3.1.1 ping

You can use the **ping** command to check the network connectivity and the reachability of a host.

Table 3-1 The ping command

Operation	Command	Description
Check the IP network connectivity and the reachability of a host	**ping** [**-a** *ip-address*] [**-c** *count*] [**-d**] [**-f**] [**-h** *ttl*] [**-i** *interface-type interface-number*] [**ip**] [**-n**] [**- p** *pattern*] [**-q**] [**-s** *packetsize*] [**-t** *timeout*] [**-tos** *tos*] [**-v**] *host*	You can use this command in any view.

This command can output the following results:

- Response status for each ping packet. If no response packet is received within the timeout time, the message "Request time out" is displayed. Otherwise, the number of data bytes, packet serial number, TTL (time to live) and response time of the response packet are displayed.
- Final statistics, including the numbers of sent packets and received response packets, the irresponsive packet percentage, and the minimum, average and maximum values of response time.

3.1.2 tracert

You can use the **tracert** command to trace the gateways that a packet passes from the source to the destination. This command is mainly used to check the network connectivity. It can help locate the trouble spot of the network.

The executing procedure of the **tracert** command is as follows: First, the source host sends a data packet with the TTL of 1, and the first hop device returns an ICMP error message indicating that it cannot forward this packet because of TTL timeout. Then, the source host resends the packet with the TTL of 2, and the second hop device also returns an ICMP TTL timeout message. This procedure goes on and on until the packet gets to the destination. During the procedure, the system records the source address of each ICMP TTL timeout message in order to offer the path that the packet passed through to the destination.

Table 3-2 The **tracert** command

Operation	Command	Description
Trace the gateways that a packet passes from the source host to the destination	**tracert** [**-a** *source-ip*] [**-f** *first-ttl*] [**-m** *max-ttl*] [**-p** *port*] [**-q** *num-packet*] [**-w** *timeout*] *string*	You can execute the **tracert** command in any view.

Chapter 4 Device Management

4.1 Introduction to Device Management

The device management function of the Ethernet switch enables the display of current status and event-debugging information of the system. Through this function, you can maintain and manage the status and communication of the physical devices, and restart the system when some functions of the system are exceptional.

4.2 Device Management Configuration

4.2.1 Device Management Configuration Tasks

Table 4-1 Device management configuration tasks

Operation	Description	Related section
Reboot the Ethernet switch	—	Section 4.2.2 “Rebooting the Ethernet Switch”
Schedule a reboot on the switch	Optional	Section 4.2.3 “Scheduling a Reboot on the Switch”
Specify the ARP to be adopted at reboot	Optional	Section 4.2.4 “Specifying the APP to be Adopted at Reboot”
Update the BootROM	Optional	Section 4.2.5 “Upgrading the BootROM”
Update the host software in the Fabric	Optional	Section 4.2.6 “Upgrading the Host Software in the Fabric”

4.2.2 Rebooting the Ethernet Switch

You can perform the following operation in user view when the switch is faulty or needs to be rebooted.

Note:

Before rebooting, the system checks whether there is any configuration change. If yes, it prompts whether or not to proceed. This prevents the system from losing the configurations in case of shutting down the system without saving the configurations

---

Table 4-2 Reboot the Ethernet switch

Operation	Command	Description
Reboot the Ethernet switch	**reboot** [**unit** *unit-id*]	—

4.2.3 Scheduling a Reboot on the Switch

After you schedule a reboot on the switch, the switch will reboot at the specified time.

Table 4-3 Schedule a reboot on the switch

Operation	Command	Description
Schedule a reboot on the switch, and set the reboot date and time	**schedule reboot at** *hh:mm* [*mm/dd/yyyy* | *yyyy/mm/dd*]	Optional
Schedule a reboot on the switch, and set the delay time for reboot	**schedule reboot delay** { *hh:mm* | *mm* }	Optional
Enter system view	**system-view**	—
Schedule a reboot on the switch, and set the reboot period	**schedule reboot regularity at** *hh:mm period*	Optional

Note:

The switch timer can be set to precision of one minute, that is, the switch will reboot within one minute after the specified reboot date and time.

4.2.4 Specifying the APP to be Adopted at Reboot

APP is the host software of the switch. If multiple APPs exist in the Flash memory, you can use the command here to specify the one that will be adopted when the switch reboots.

Table 4-4 Specify the APP to be adopted at reboot

Operation	Command	Description
Specify the APP to be adopted at reboot	**boot boot-loader** [**backup-attribute**] { *file-url* [**fabric**] | *device-name* }	Optional

4.2.5 Upgrading the BootROM

You can use the BootROM program saved in the Flash memory of the switch to upgrade the running BootROM. With this command, a remote user can conveniently upgrade the BootRom by uploading the BootROM to the switch through FTP and running this command. The BootROM can be used when the switch restarts.

Table 4-5 Upgrade the BootROM

Operation	Command	Description
Upgrade the BootROM	**boot bootrom** { *file-url* | *device-name* }	Optional

4.2.6 Upgrading the Host Software in the Fabric

You can execute the following command on any device in a Fabric to use specified host software to upgrade all devices in a Fabric, thus realizing the software version consistency in this Fabric.

Table 4-6 Upgrade the host software in the Fabric

Operation	Command	Description
Upgrade the host software on the devices in the Fabric	**update fabric** { *file-url* | *device-name* }	Optional

4.3 Displaying the Device Management Configuration

After the above configurations, you can execute the **display** command in any view to display the operating status of the device management to verify the configuration effects.

Table 4-7 Display the operating status of the device management

Operation	Command	Description
Display the APP to be adopted at next startup	**display boot-loader** [**unit** *unit-id*]	You can execute the **display** command in any view.
Display the module type and operating status of each board	**display device** [**manuinfo** [**unit** *unit-id*] | **unit** *unit-id*]	
Display CPU usage of a switch	**display cpu** [**unit** *unit-id*]	
Display the operating status of the fan	**display fan** [**unit** *unit-id* [*fan-id*]]	
Display memory usage of a switch	**display memory** [**unit** *unit-id*]	
Display the operating status of the power supply	**display power** [**unit** *unit-id* [*power-id*]]	
Display system diagnostic information or save system diagnostic information to a file with the extension .diag into the Flash memory	**display diagnostic-information**	
Display enabled debugging on a specified switch or all switches in the fabric	**display debugging** { **fabric** | **unit** *unit-id* } [**interface** *interface-type interface-number* | *module-name*]	
Display enabled debugging on all switches in the fabric by modules	**display debugging fabric by-module**	

4.4 Remote Switch Upgrade Configuration Example

I. Network requirements

Telnet to the switch from a PC remotely and download applications from the FTP server to the Flash memory of the switch. Update the switch software by using the device management commands through CLI.

The switch acts as the FTP client, and the remote PC serves as both the configuration PC and the FTP server.

Perform the following configuration on the FTP server.

- Configure an FTP user, whose name is switch and password is hello. Authorize the user with the read-write right on the directory **switch** on the PC.

- Make configuration so that the IP address of a VLAN interface on the switch is 1.1.1.1, the IP address of the PC is 2.2.2.2, and the switch and the PC is reachable to each other.

The host software switch.bin and the BootROM file boot.btm of the switch are stored in the directory **switch** on the PC. Use FTP to download the switch.bin and boot.btm files from the FTP server to the switch.

II. Network diagram

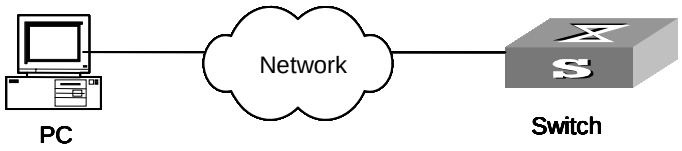


Figure 4-1 Network diagram of FTP configuration

III. Configuration procedure

1) Configure the following FTP server–related parameters on the PC: an FTP user with the username as switch and password as hello, who is authorized with the read-write right on the directory Switch on the PC. The detailed configuration is omitted here.
2) On the switch, configure a level 3 telnet user with the username as user and password as hello. Authentication mode is by user name and password.

Note:

Refer to the part “Login Operation” for configuration commands and steps about telnet user.

---

3) Execute the **telnet** command on the PC to log into the switch. The following prompt appears:

```
<H3C>
```

Caution:

If the Flash memory of the switch is not sufficient, delete the original applications before downloading the new ones.

---

4) Initiate an FTP connection with the following command in user view. Enter the correct user name and password to log into the FTP server.

```
<H3C> 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]
```

5) Enter the authorized path on the FTP server.

```
[ftp] cd switch
```

6) Execute the **get** command to download the switch.bin and boot.btm files on the FTP server to the Flash memory of the switch.

```
[ftp] get switch.bin
[ftp] get boot.btm
```

7) Execute the **quit** command to terminate the FTP connection and return to user view.

```
[ftp] quit
<H3C>
```

8) Upgrade the BootROM.

```
<H3C> boot bootrom boot.btm
 This will update BootRom file on unit 1. Continue? [Y/N] y
 Upgrading BOOTROM, please wait...
 Upgrade BOOTROM succeeded!
```

9) Specify the downloaded program as the host software to be adopted when the switch starts next time. Then restart the switch to upgrade the host software of the switch.

```
<H3C> boot boot-loader switch.bin
 The specified file will be booted next time on unit 1!
<H3C> display boot-loader
 Unit 1:
   The current boot app is: switch.bin
   The main boot app is:    switch.bin
   The backup boot app is:
<H3C> reboot
```

Table of Contents

Chapter 1 VLAN-VPN Configuration 1-1
1.1 VLAN-VPN Overview 1-1
1.1.1 Introduction to VLAN-VPN 1-1
1.1.2 Implementation of VLAN-VPN 1-1
1.1.3 Adjusting the TPID Values of VLAN-VPN Packets 1-2
1.2 VLAN-VPN Configuration 1-3
1.2.1 Configuration Prerequisites 1-3
1.2.2 Configuration Procedure 1-3
1.3 Inner VLAN Tag Priority Replication Configuration 1-4
1.3.1 Configuration Prerequisites 1-4
1.3.2 Configuration Procedure 1-4
1.4 TPID Adjusting Configuration 1-5
1.4.1 Configuration Prerequisites 1-5
1.4.2 Configuration Procedure 1-5
1.5 VLAN-VPN Configuration Example 1-6
Chapter 2 BPDU Tunnel Configuration 2-1
2.1 BPDU Tunnel Overview 2-1
2.1.1 Introduction to the BPDU Tunnel Function 2-1
2.1.2 BPDU Tunnel Fundamental 2-1
2.2 BPDU Tunnel Configuration 2-2
2.2.1 Configuration Prerequisites 2-3
2.2.2 Configuring BPDU Tunnel 2-3
2.3 BPDU Tunnel Configuration Example 2-3

Chapter 1 VLAN-VPN Configuration

1.1 VLAN-VPN Overview

1.1.1 Introduction to VLAN-VPN

The VLAN-VPN function enables packets to be transmitted across the operators' backbone networks with VLAN tags of private networks encapsulated 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 encapsulated in the VLAN tags of public networks are shielded.

Figure 1-1 describes the structure of the packets with single-layer VLAN tags.



Figure 1-1 Structure of packets with single-layer VLAN tags

Figure 1-2 describes the structure of the packets with nested VLAN tags.



Figure 1-2 Structure of packets with double-layer VLAN tags

Compared with MPLS-based Layer 2 VPN, VLAN-VPN has the following features:

- It provides Layer 2 VPN tunnels that are simpler.
- VLAN-VPN can be implemented without the support of signaling protocols. You can enable VLAN-VPN by static configuration.

The VLAN-VPN function provides you with the following benefits:

- Saves public network VLAN ID resource.
- You can have VLAN IDs of your own, which is independent of public network VLAN IDs.
- It allows for simple Layer 2 VPN solutions for small-sized MANs or intranets.

1.1.2 Implementation of VLAN-VPN

VLAN-VPN can be implemented by enabling the VLAN-VPN function on ports.

With the VLAN VPN function enabled, a received packet is tagged with the default VLAN tag of the receiving port no matter whether or not the packet already carries a VLAN tag. If the packet already carries a VLAN tag, the packet becomes a dual-tagged

packet. Otherwise, the packet becomes a packet carrying the default VLAN tag of the port.

1.1.3 Adjusting the TPID Values of VLAN-VPN Packets

Tag protocol identifier (TPID) is a field of the VLAN tag. IEEE 802.1Q specifies the value of TPID to be 0x8100.

Figure 1-3 illustrates the structure of the Tag packet of an Ethernet frame defined by IEEE 802.1Q.

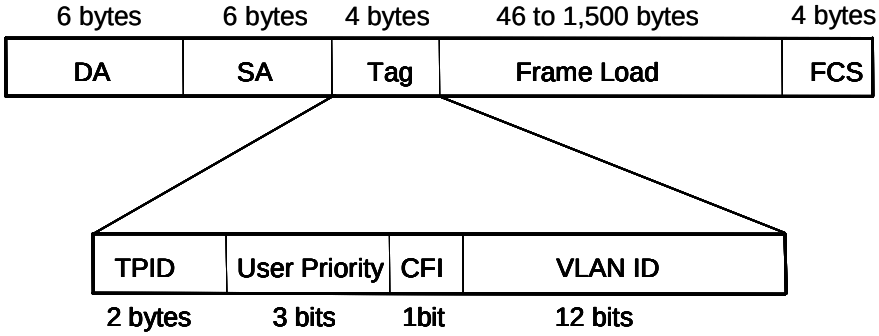


Figure 1-3 The structure of the Tag packet of an Ethernet frame

S3600 series switches adopt the protocol default TPID value (0x8100). Other vendors use other TPID values (such as 0x9100 or 0x9200) in the outer tags of VLAN-VPN packets.

To be compatible with devices coming from other vendors, S3600 series switches can adjust the TPID values of VLAN-VPN packets based on ports. You can configure the TPID value of a port connecting to the public network side by yourself. When a packet is forwarded through the port, the port replaces the TPID value in the outer VLAN tag of this packet with the user-defined value. Thus, the VLAN-VPN packets sent to the public network can be recognized by devices of other vendors.

As the position of the TPID field in an Ethernet packet is the same as that of the protocol type field in a packet without VLAN Tag, to avoid confusion in the process of receiving/forwarding a packet, the TPID value cannot be any of the protocol type value listed in Table 1-1

Table 1-1 Commonly used protocol type values in Ethernet frames

Protocol type	Value
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137

Protocol type	Value
IS-IS	0x8000
LACP	0x8809
802.1x	0x888E

1.2 VLAN-VPN Configuration

1.2.1 Configuration Prerequisites

- GARP VLAN registration protocol (GVRP), GARP multicast registration protocol (GMRP), intelligent resilient framework (IRF), neighbor topology discovery protocol (NTDP), spanning tree protocol (STP), 802.1x and centralized MAC address authentication function are disabled on the port.
- The port is an access port.

⚠ **Caution:**

- The VLAN-VPN function is unavailable to a port if any of the protocols among GVRP, GMRP, IRF, NTDP, STP, 802.1x and centralized MAC address authentication function is enabled on the port.
- By default, STP and NTDP are enabled on a device. You can disable these two protocols using the **stp disable** and **undo ntdp enable** commands.
- The VLAN-VPN function is unavailable to all the ports of a device if the fabric function is enabled on a port of the device.

1.2.2 Configuration Procedure

Table 1-2 Configure the VLAN-VPN function for a port

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the VLAN-VPN function on the port	**vlan-vpn enable**	Required By default, the VLAN-VPN function is disabled on a port.

Operation	Command	Description
Display VLAN VPN configuration information about all the ports	**display port vlan-vpn**	This command can be executed in any view.

Note:

After you enable the VLAN-VPN function for a port, you cannot change the port to be a trunk port or hybrid port, nor can you enable GVRP, GMRP, IRF, NTDP, or STP, 802.1x and centralized MAC address authentication function for the port.

- Error message appears if you try to change the port to be a trunk port or hybrid port or enable GVRP, GMRP, IRF, NTDP, STP, 802.1x or centralized MAC address authentication function for the port by executing corresponding commands.
- If you use the **copy configuration** command to duplicate the configuration of a port to a port enabled with the VLAN-VPN function, the configuration concerning port type (that is, access, trunk, or hybrid), GVRP, GMRP, IRF, NTDP, STP, 802.1x and centralized MAC address authentication function is not duplicated.

1.3 Inner VLAN Tag Priority Replication Configuration

You can configure to replicate the tag priority of the inner VLAN tag of a VLAN-VPN packet to the outer VLAN tag to keep the original tag priority after the packet is inserted an outer VLAN tag.

1.3.1 Configuration Prerequisites

The VLAN-VPN function is enabled.

1.3.2 Configuration Procedure

Table 1-3 Replicate the tag priority of the inner VLAN tag

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Enable the inner VLAN Tag priority replication function	**vlan-vpn inner-cos-trust enable**	Required By default, the inner VLAN tag priority replication function is disabled. And the priority of an outer VLAN tag is that of the default priority of the current port.
Display the VLAN-VPN configuration of about all ports	**display port vlan-vpn**	This command can be executed in any view.

Caution:

If you have configured the port priority, (refer to the QoS&QoS Profile part of *H3C S3600 Series Ethernet Switches Operation Manual* for more), after you configure to replicate the tag priority of the inner VLAN tag of a VLAN-VPN packet, the switch will prompt that the port priority configuration on the current port is invalid.

1.4 TPID Adjusting Configuration

1.4.1 Configuration Prerequisites

The TPID value of the peer end of the public network is available.

1.4.2 Configuration Procedure

Table 1-4 Adjust TPID values for VLAN-VPN packets

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set a TPID value for the port	**vlan-vpn tpid** *value*	Required Do not set the TPID value to any of the protocol type values listed in Table 1-1.
Display VLAN-VPN configuration information about all ports	**display port vlan-vpn**	You can execute the **display** command in any view.

Caution:

You will fail to execute the **vlan-vpn tpid** command on an IRF Fabric port.

1.5 VLAN-VPN Configuration Example

I. Network requirements

- Switch A and Switch C are S3600 series switches. Switch B is a switch coming from another manufacturer, which uses the TPID value of 0x9100.
- Two user networks are connected to the Ethernet1/0/1 ports of Switch A and Switch C respectively.
- Switch B only permits packets of VLAN 10.
- It is required that packets of the VLANs other than VLAN 10 can be exchanged between the user networks connected to Switch A and Switch C.

II. Network diagram

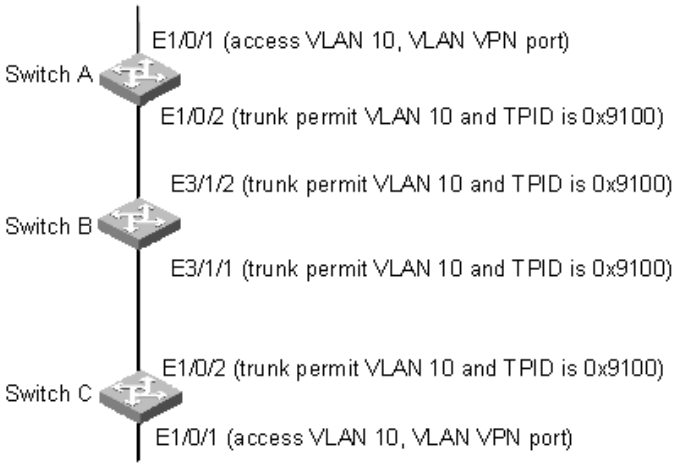


Figure 1-4 Network diagram for VLAN-VPN configuration

III. 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 Ethernet1/0/2 port of Switch A to 0x9100, and add the port to VLAN 10.

```
<SwitchA> system-view
[SwitchA] vlan 10
```

```
[SwitchA-vlan10] quit
[SwitchA] interface Ethernet1/0/2
[SwitchA-Ethernet1/0/2] vlan-vpn tpid 9100
[SwitchA-Ethernet1/0/2] port link-type trunk
[SwitchA-Ethernet1/0/2] port trunk permit vlan 10
```

Add Ethernet1/0/1 port of Switch A to VLAN 10 and enable the VLAN-VPN function for the port.

```
[SwitchA] interface Ethernet1/0/1
[SwitchA-Ethernet1/0/1] port access vlan 10
[SwitchA-Ethernet1/0/1] vlan-vpn enable
[SwitchA-Ethernet1/0/1] quit
```

2) Configure Switch B

Because Switch B comes from another manufacturer, the commands involved may differ from those for S3600 series switches. So only the operations are listed, as shown below:

- Configure Ethernet3/1/1 and Ethernet3/1/2 ports of Switch B to be trunk ports.
- Add the two ports to VLAN 10.

Note:

The following describes how a packet is forwarded from Switch A to Switch C.

- As the Ethernet1/0/1 port of Switch A is a VLAN-VPN port, when a packet from the user's network side reaches Ethernet1/0/1 port of Switch A, it is tagged with the default VLAN tag of the port (VLAN 10) and is then forwarded to Ethernet1/0/2 port.
- Because Ethernet1/0/2 port is configured with VLAN-VPN TPID, 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 Ethernet3/1/2 port of Switch B in the public network. Switch B forwards the packet to Ethernet3/1/1, which belongs to VLAN 10.
- The packet is forwarded from Ethernet3/1/1 port of Switch B to the network on the other side and enters Ethernet1/0/2 port of Switch C. Then Switch C forwards the packet to its Ethernet1/0/1 port, which also belongs to VLAN 10. As Ethernet1/0/1 port is an access port, Switch C strips off the outer VLAN tag of the packet and restores the original packet.
- It is the same case when a packet travels from Switch C to Switch A.

After the configuration, the networks connecting Switch A and Switch C can receive data packets from each other.

Chapter 2 BPDU Tunnel Configuration

2.1 BPDU Tunnel Overview

2.1.1 Introduction to the BPDU Tunnel Function

In MAN networking solutions, the requirements may arise that the branches of an enterprise be interconnected through the operator's network. This can be achieved through VPN (virtual private network), which can integrate geographically dispersed networks to form a logical LAN. The tunnel function is required when you implement VPN. It enables packets of private networks to travel through operator's network and reach another private network securely. To make networks of this kind essentially comparable with an actual LAN, Layer 2 protocol packets used to maintain the network are also required to travel across the tunnels.

2.1.2 BPDU Tunnel Fundamental

I. Layer 2 packet identification

Different from the processing of data packets, a Layer 2 protocol packet is classified first when it reaches a network device. A Layer 2 protocol packet conforming with IEEE standards carries a special destination MAC address and contains a type field. Some proprietary protocols adopt the same packet structure, where a private MAC address is used to identify the corresponding proprietary protocol, and the type field is used to identify the specific protocol type.

II. Transmitting BPDU packets transparently

As shown in Figure 2-1, the network on the top is the operator's network, and the one on the bottom is a user network. The operator's network contains devices that receive/transmit packets. The user network contains Network A and Network B. You can make the BPDU packets to be transmitted in the operator's network transparently by enabling the BPDU Tunnel function on the devices with user networks connected to in the operator's network.

- When a BPDU packet coming from a user network reaches a device in the operator's network, the device changes the destination MAC address carried in the packet from a protocol-specific MAC address to a normal MAC address, which can be identified by both the local device and the peer device. In such a way, the BPDU packet is converted to a normal data packet and is forwarded in the operator's network.
- Before the device in the operator's network forwards the packet to the destination user network, the device restores the original protocol-specific MAC address. This

ensures the data portion of the packet is consistent with that before the packet enters the tunnel. So, a tunnel here acts as a local link for user devices. It enables Layer 2 protocol packets to travel across a logical LAN.

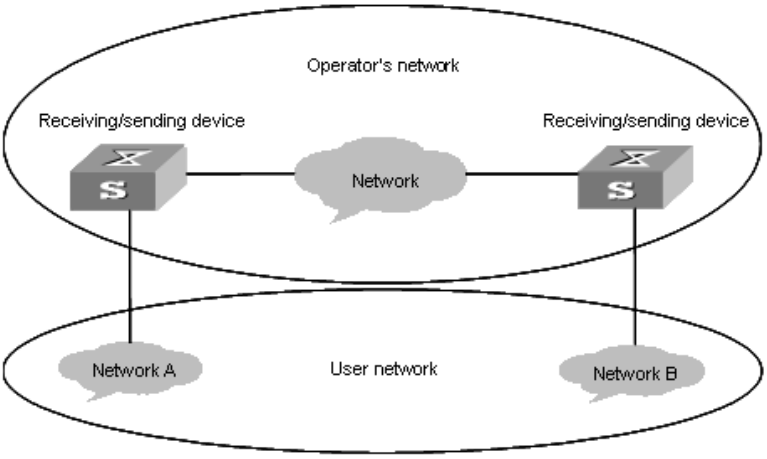


Figure 2-1 BPDU Tunnel network hierarchy

Figure 2-2 and Figure 2-3 show the structure of a BPDU packet before and after it enter a BPDU tunnel.

Destination MAC address (Protocol-specific MAC)	Source MAC address	BPDU Data	FCS

Figure 2-2 The structure of a BPDU packet before it enters a BPDU tunnel

Destination MAC address (Recognizable by user)	Source MAC address	BPDU Data	FCS

Figure 2-3 The structure of a BPDU packet after it enters a BPDU tunnel

2.2 BPDU Tunnel Configuration

You can establish BPDU tunnels between S3600 series Ethernet switches for the packets of the following protocols:

- ALCP (link aggregation control protocol)
- NDP (neighbor discovery protocol)
- Proprietary protocols, including CDP and VTP

2.2.1 Configuration Prerequisites

One or more protocols among LACP, NDP, CDP, and VTP operate properly on the devices.

2.2.2 Configuring BPDU Tunnel

Table 2-1 Configure BPDU Tunnel

<table>
<tr><th colspan="3">Operation</th><th>Command</th><th>Description</th></tr>
<tr><td colspan="3">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td rowspan="4">Set the port to be a BPDU Tunnel uplink port</td><td colspan="2">Enable the function in system view</td><td>bpdu-tunnel uplink interface-list</td><td rowspan="4">You can enable the BPDU Tunnel in system view or in Ethernet view.
By default, NDP is enabled globally.</td></tr>
<tr><td rowspan="3">Enable the function in Ethernet port view</td><td>Enter Ethernet port view</td><td>interface interface-type interface-number</td></tr>
<tr><td>Enable the BPDU Tunnel function</td><td>bpdu-tunnel uplink</td></tr>
<tr><td>Return to system view</td><td>quit</td></tr>
<tr><td colspan="3">Enter Ethernet port view</td><td>interface interface-type interface-number</td><td>-</td></tr>
<tr><td colspan="3">Enable the BPDU Tunnel function for the packets of a specific protocol</td><td>bpdu-tunnel { lacp | ndp | cdp | vtp }</td><td>Required
By default, the BPDU Tunnel function is disabled on a port.</td></tr>
</table>

Note:

The BPDU Tunnel is unavailable to all the ports of a device if the device has the fabric function enabled on one of its ports.

2.3 BPDU Tunnel Configuration Example

I. Network requirements

- Custimer1 and Customer2 are access devices operating in a user network.
- Provider1 and Provider2 are access devices operating in the operator's network. They are interconnected through their trunk ports, as shown in Figure 2-4.

- Enable the BPDU Tunnel function for NDP packets on the Ethernet1/0/1 and Ethernet1/0/4 port shown in the Figure 2-4.Set the port Ethernet1/0/2 and Ethernet1/0/3 to be BPDU Tunnel uplink ports.

II. Network diagram

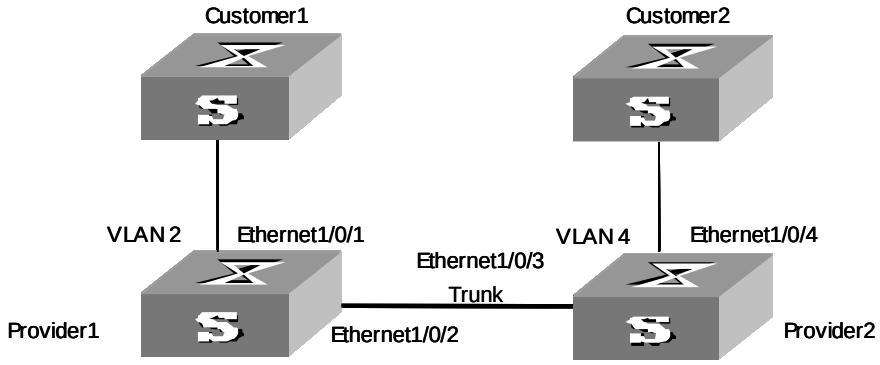


Figure 2-4 Network diagram for BPDU Tunnel configuration

III. Configuration procedure

1) Configure Provide1.

Enable the BPDU Tunnel fuction for NDP packets on port Ethernet1/0/1.

```
<H3C> system-view
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] undo ndp enable
[H3C-Ethernet1/0/1] bpdu-tunnel ndp
```

Set the port Ethernet 1/0/2 to be a BPDU Tunnel uplink port.

```
[H3C-Ethernet1/0/1] quit
[H3C] interface Ethernet 1/0/2
[H3C-Ethernet1/0/2] bpdu-tunnel uplink
```

2) Configure Provider2.

Set the port Ethernet 1/0/3 to be a BPDU Tunnel uplink port.

```
<H3C> system-view
[H3C] interface Ethernet 1/0/3
[H3C-Ethernet1/0/3] bpdu-tunnel uplink
```

Enable the BPDU Tunnel function for NDP packets on port Ethernet1/0/4

```
[H3C-Ethernet1/0/3] quit
[H3C] interface Ethernet 1/0/4
[H3C-Ethernet1/0/4] undo ndp enable
[H3C-Ethernet1/0/4] bpdu-tunnel ndp
```

Table of Contents

Chapter 1 HWPing Configuration 1-1
1.1 Introduction to HWPing 1-1
1.2 HWPing Configuration 1-1
1.2.1 Introduction to HWPing Configuration 1-1
1.2.2 Configuring HWPing 1-2
1.2.3 Displaying HWPing Configuration 1-3
1.2.4 Configuration Example 1-3

Chapter 1 HWPing Configuration

1.1 Introduction to HWPing

HWPing is a network diagnostic tool used to test the performance of protocols (only ICMP by far) running on network. It is an enhanced alternative to the **ping** command.

HWPing test group is a set of HWPing test parameters. A test group contains several test parameters and is uniquely identified by an administrator name plus a test tag.

You can perform an HWPing test after creating a test group and configuring the test parameters.

Different from the **ping** command, HWPing does not display the round trip time (RTT) and timeout status of each packet on the console terminal in real time. You need to execute the **display hwping** command to view the statistic results of your HWPing test operation. HWPing allows setting the parameters of HWPing test groups and starting HWPing test operations through network management system.

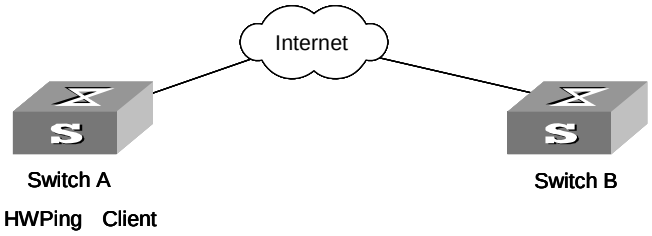


Figure 1-1 Illustration for HWPing

1.2 HWPing Configuration

1.2.1 Introduction to HWPing Configuration

The configuration tasks for HWPing include:

- Enabling HWPing Client
- Creating test group
- Configuring test parameters

The test parameters that you can configure include:

1) Destination IP address

It is equivalent to the destination IP address in the **ping** command.

2) Test type

Currently, HWPing supports only one test type: ICMP.

3) Number of test packets to be sent in a test

If this parameter is set to a number greater than 1, the system sends the second test packet once it receives a response to the first one, or when the test timer times out if it receives no response after sending the first one, and so forth until the last test packet is sent out. This parameter is equivalent to the **–n** keyword in the **ping** command.

4) Automatic test interval

This parameter is used to enable the system to automatically perform the same test at regular intervals.

5) Test timeout time

Test timeout time is the duration while the system waits for an ECHO-RESPONSE packet after it sends out an ECHO-REQUEST packet. If no ECHO-RESPONSE packet is received within this duration, this test is considered a failure. This parameter is similar to the **-t** keyword in the **ping** command, but has a different unit (the **-t** keyword in the **ping** command is in milliseconds, while the timeout time in the **HWPing** command is in seconds).

1.2.2 Configuring HWPing

Table 1-1 Configure HWPing

Operation	Command	Description
Enter system view	**system-view**	—
Enable HWPing Client	**hwping-agent enable**	Required By default, HWPing Client is disabled.
Create an HWPing test group	**hwping** *administrator-name operation- tag*	Required By default, no HWPing test group is configured.
Configure the destination IP address of the test	**destination-ip** *ip-address*	Required By default, no destination IP address is configured.
Configure the test type	**test-type** *type*	Optional By default, the test type is ICMP.
Configure the number of packets to be sent in each test.	**count** *times*	Optional By default, the number of packets to be sent in each test is 1.

Operation	Command	Description
Configure the automatic test interval.	**frequency** *interval*	Optional By default, the automatic test interval is zero, indicating no automatic test will be performed.
Configure the timeout time of the test.	**timeout** *time*	Optional By default, the timeout time is 3 seconds.
Execute the test	**test-enable**	Required

1.2.3 Displaying HWPing Configuration

After the above HWPing configuration, you can execute the **display** command in any view to display the information of HWPing test operation status to you can verify the configuration effect.

Table 1-2 Display HWPing configuration

Operation	Command	Description
Display the information of HWPing test history	**display hwping history** [*administrator-name operation-tag*]	The **display** command can be executed in any view.
Display the latest HWPing test results	**display hwping results** [*administrator-name operation-tag*]	

1.2.4 Configuration Example

I. Network requirement

Perform an HWPing ICMP test between two switches. Like a ping test, this test uses ICMP to test the RTTs of data packets between the source and the destination.

II. Configuration procedure

Enable HWPing Client.

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] hwping-agent enable
```

Create an HWPing test group “administrator icmp”.

```
[H3C] hwping administrator icmp
```

Specify the test type as ICMP.

```
[H3C-hwping-administrator-icmp] test-type icmp
```

Specify the destination IP address as 1.1.1.99.

```
[H3C-hwping-administrator-icmp] destination-ip 1.1.1.99
```

Set the number of test packets sent in a test to 10.

```
[H3C-hwping-administrator-icmp] count 10
```

Set the timeout time of test operations to 5.

```
[H3C-hwping-administrator-icmp] timeout 5
```

Enable the test operation.

```
[H3C-hwping-administrator-icmp] test-enable
```

Display the test results.

```
[H3C-hwping-administrator-icmp] display hwping results administrator icmp
  HWPing entry(admin administrator, tag icmp) test result:
      Destination ip address:1.1.1.99
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 2/5/2
      Square-Sum of Round Trip Time: 66
      Last complete test time: 2000-4-2 7:59:54.7
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      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
[H3C-hwping-administrator-icmp] display hwping history administrator icmp
  HWPing entry(admin administrator, tag icmp) history record:
    Index     Response    Status      LasrRC      Time
       1            1         1           0    2004-11-25 16:28:55.0
       2            1         1           0    2004-11-25 16:28:55.0
       3            1         1           0    2004-11-25 16:28:55.0
       4            1         1           0    2004-11-25 16:28:55.0
       5            1         1           0    2004-11-25 16:28:55.0
       6            2         1           0    2004-11-25 16:28:55.0
       7            1         1           0    2004-11-25 16:28:55.0
       8            1         1           0    2004-11-25 16:28:55.0
       9            1         1           0    2004-11-25 16:28:55.9
      10            1         1           0    2004-11-25 16:28:55.9
```

Refer to the *HWPing Command Manual* for detailed description on displayed information.

Table of Contents

Chapter 1 DNS Configuration 1-1
1.1 DNS Overview 1-1
1.1.1 Static Domain Name Resolution 1-1
1.1.2 Dynamic Domain Name Resolution 1-1
1.2 Configuring Static Domain Name Resolution 1-3
1.3 Configuring Dynamic Domain Name Resolution 1-3
1.3.1 Configuration Procedure 1-3
1.3.2 DNS Configuration Example 1-4
1.4 Displaying and Maintaining DNS 1-5
1.5 Troubleshooting DNS 1-5

Chapter 1 DNS Configuration

1.1 DNS Overview

Domain name system (DNS) is a mechanism used for TCP/IP applications to provide domain name-to-IP address translation. With DNS, you can use memorizable and meaningful domain names in some applications and let the DNS server resolve it into correct IP addresses.

There are two types of DNS services, static and dynamic. Each time the DNS Server receives a name query, it checks its static DNS database before looking up the dynamic DNS database. Reduction of the searching time in the dynamic DNS database would increase efficiency. Some frequently used addresses can be put in the static DNS database.

1.1.1 Static Domain Name Resolution

The static domain name resolution means manually setting up mappings between domain names and IP addresses. IP addresses of the corresponding domain names can be found in the static DNS database for applications.

1.1.2 Dynamic Domain Name Resolution

I. Resolution procedure

Dynamic domain name resolution is implemented by querying the DNS server. The resolution procedure is as follows:

1) A user program sends a name query to the resolver in the DNS Client.
2) The DNS resolver looks up the local domain name cache for a match. If a match is found, it sends the corresponding IP address back. If not, it sends the query to the DNS Server.
3) The DNS Server looks up its DNS database for a match. If no match is found, it sends a query to a higher DNS Server. This process continues until a result, success or failure, is returned.
4) The DNS Client performs the next operation according to the result.

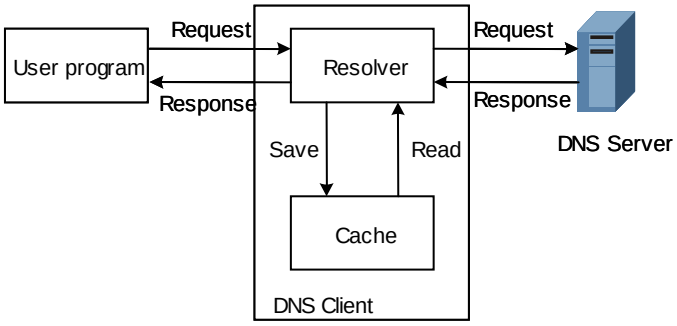


Figure 1-1 Dynamic domain name resolution

Figure 1-1 shows the relationship between user program, NDS Client, and DNS Server.

The resolver and cache comprise the DNS Client. The user program and DNS Client can run on the same machine or different machines, while the DNS Server and the DNS Client usually must run on different machines.

Dynamic domain name resolution allows the DNS Client to store latest mappings between name and IP address in the dynamic domain name cache. There is no need to send a request to the DNS Server for a repeated query request next time. The aged mappings are removed from the cache after some time, and latest entries are required from the DNS Server. The DNS Server decides how long a mapping is valid, and the DNS Client gets the information from DNS messages.

II. DNS suffixes

The DNS Client normally holds a list of suffixes which can be defined by users. It is used when the name to be resolved is not complete. The resolver can supply the missing part. For example, a user can configure com as the suffix for aabbcc.com. The user only needs to type aabbcc to get the IP address of aabbcc.com. The resolver can add the suffix and delimiter before passing the name to the DNS Server.

- If there is no dot in the domain name, such as aabbcc, the resolver will consider this as a host name and add a DNS suffix before processing. The original name such as aabbcc is used if all DNS lookups fail.
- If there is a dot in the domain name, such as www.aabbcc, the resolver will use this domain name to do DNS lookup first. If the lookup fails, the resolver adds a DNS suffix for another lookup.
- If a dot is at the end of the domain name, such as “aabbcc.com.”, the resolver will consider this as a fully qualified domain name and return the result, success or failure. Hence, the dot (.) is called the terminating symbol.

Currently, the device supports static and dynamic DNS services.

1.2 Configuring Static Domain Name Resolution

Table 1-1 Configure static domain name resolution:

Operation	Command	Description
Enter system view	**system-view**	—
Configure a mapping between a host name and an IP address	**ip host** *hostname ip-address*	Required No IP address is assigned to a host name by default.

Note:

The IP address you assign to a host name last time will overwrite the previous one if there is any.

You may create up to 50 static mappings between domain names and IP addresses.

1.3 Configuring Dynamic Domain Name Resolution

1.3.1 Configuration Procedure

Table 1-2 Configure dynamic domain name resolution:

Operation	Command	Description
Enter the system view	**system-view**	—
Enable dynamic domain name resolution	**dns resolve**	Required Disabled by default
Configure an IP address for the DNS Server	**dns server** *ip-address*	Required No IP address is configured for the DNS server by default.
Configure DNS suffixes	**dns domain** *domain-name*	Optional No DNS suffix is configured by default

Note:

You may configure up to six DNS Servers and ten DNS suffixes.

1.3.2 DNS Configuration Example

I. Network requirements

As shown in Figure 1-2, the switch serving as a DNS Client uses the dynamic domain name resolution feature to access the host with the domain name being host1 and the IP address being 3.1.1.1/16. The DNS Server has the IP address 2.1.1.2/16. The DNS suffixes are com and net.

II. Network diagram

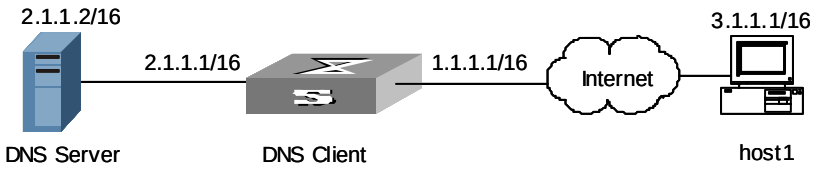


Figure 1-2 Network diagram for dynamic domain name resolution

III. Configuration procedure

Note:

Before doing the following configuration, make sure that:

- The route between the switch and host 1 is reachable.
- Configurations are done on the switch and host1. For the IP addresses of the interfaces, see the figure above.
- There is a mapping between host1 and the IP address 3.1.1.1/16 on the DNS Server.
- The DNS Server works normally.

Enable dynamic domain name resolution.

```
<H3C> system-view
[H3C] dns resolve
```

Configure the IP address 2.1.1.2 for the DNS Server.

```
[H3C] dns server 2.1.1.2
```

Configure net as the DNS suffix.

```
[H3C] dns domain net
```

Configure com as the DNS suffix.

```
[H3C] dns domain com
```

Execute the **ping host1** command on the switch to verify that the communication between the switch and the host is normal and that the corresponding IP address is 3.1.1.1.

1.4 Displaying and Maintaining DNS

After the above configuration, you can execute the **display** command in any view to display the DNS configuration information to verify the configuration effect. You can execute the **reset** command in user view to clear the information stored in the dynamic domain name resolution cache.

Table 1-3 Display and maintain DNS

Operation	Command…	Description
Display static DNS database	**display ip host**	Available in any view
Display the DNS Server information	**display dns server** [**dynamic**]	
Display the DNS suffixes	**display dns domain** [**dynamic**]	
Display the information in the dynamic domain name cache	**display dns dynamic-host**	
Display the DNS resolution result	**nslookup type** { **ptr** *ip-address* | **a** *domain-name* }	Available in any view
Clear the information in the dynamic domain name cache	**reset dns dynamic-host**	Available in user view

1.5 Troubleshooting DNS

I. Symptom

After enabling the dynamic domain name resolution, the user cannot get the correct IP address.

II. Solution

- Use the **display dns dynamic-host** command to check that the specified domain name is in the cache.
- If there is no defined domain name, check that dynamic domain name resolution is enabled and the DNS Client can communicate with the DNS Server.
- If the specified domain name exists in the cache but the IP address is incorrect, check that the DNS Client has the correct IP address of the DNS Server.

- Check that the mapping between the domain name and IP address is correct on the DNS Server.

Table of Contents

Chapter 1 Access Management Configuration 1-1
1.1 Access Management Overview 1-1
1.2 Configure Access Management 1-2
1.2.1 Enable Access Management Function 1-2
1.2.2 Configure the Access IP Address Pool Based on the Physical Port 1-2
1.2.3 Configure Layer 2 Isolation between Ports 1-3
1.2.4 Enable Access Management Trap 1-4
1.3 Display Access Management 1-4
1.4 Access Management Configuration Example 1-5

Chapter 1 Access Management Configuration

1.1 Access Management Overview

One of the typical Ethernet access networking scenario is that the users access external network through the Ethernet switches. In this case, the external network is connected to the Ethernet switch. The Ethernet switch connects to the Hubs, each of which centralizes several PCs. The following figure illustrates the networking scenario.

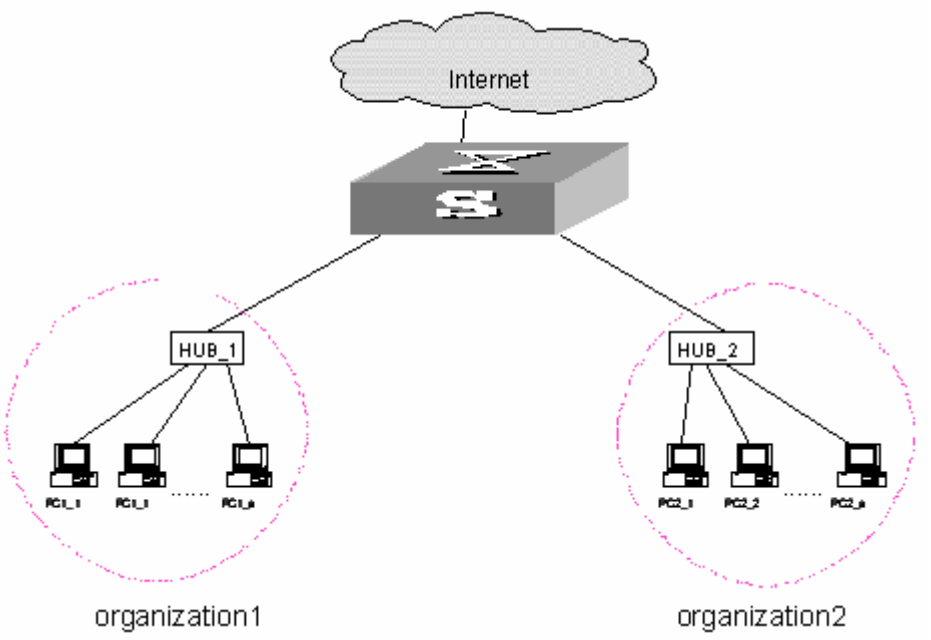


Figure 1-1 Typical Ethernet access networking scenario

If not-so-many users are connected to the switch, the ports allocated to different enterprises need to belong to the same VLAN in the light of cost. Every enterprise is allocated to the fixed IP address range simultaneously. Only those IP addresses in the fixed IP address range can be accessed to external networks from the port. Different organizations should be isolated considering security. All these requirements can be achieved with the access management function by the Ethernet switches, specifically, binding a port with IP addresses and L2 isolation between ports. See Figure 1-1.

In the figure, organization 1 and organization 2 belong to the same VLAN, which are connected to the external networks via an Ethernet switch. The IP addresses 202.10.20.1 ~ 202.10.20.20 are allocated to organization 1, that is, they are bound to the port 1. On the PCs with IP addresses in this range can be connected to external networks. The IP addresses 202.10.20.21 ~ 202.10.20.50 are allocated to organization 2, or bound to the port 2.

Isolation measure is required, because otherwise the PCs in two organizations may interwork with each other. The L2 isolation function at the switch port can ensure two ports do not receive the packets from the other port, so that only those PCs in the same organization can communicate with each other.

1.2 Configure Access Management

Access management configuration includes:

- Enable access management function
- Configure the access IP address pool based on the physical port
- Configure Layer 2 isolation between ports
- Enable access management trap

1.2.1 Enable Access Management Function

You can use the following command to enable access management function. Only after the access management function is enabled globally will the access management features (IP and port binding) take effect.

Table 1-1 Enable access management function

Operation	Command	Description
Enter system view	**system-view**	—
Enable access management function	**am enable**	Required By default, the system disables the access management function.

1.2.2 Configure the Access IP Address Pool Based on the Physical Port

You can use the following command to set the IP address pool for access management on a port. The packet whose source IP address is in the specified pool is allowed to be forwarded on Layer 3 via the port of the switch.

Table 1-2 Configure the access IP address pool based on the physical port

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

Operation	Command	Description
Configure the access management IP address pool based on the physical port	**am ip-pool** *address-list*	Required By default, the IP address pools for access control on the port are null and all the packets are permitted through.

Note:

- Before you configure the access management IP address pool on a port, make sure you configure the IP address of the Layer 3 interface to which the port belongs and these two addresses must be on the same network segment.
- If the IP address pool to be configured contains the IP addresses configured in the static ARP at other ports, then the system prompts you to delete the static ARP to make the later binding effective.

1.2.3 Configure Layer 2 Isolation between Ports

Table 1-3lists the operations to add an Ethernet port to an isolation group to isolate Layer 2 data between each port in the isolation group. See the Port Isolation module for the principles and detailed configurations of port isolation.

Table 1-3 Configure port isolation

Operation	Command	Description
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add the Ethernet port to the isolation group	**port isolate**	Required By default, an isolation group contains no port

Note that:

1) One unit only supports one isolation group. That is, a port in an isolation group on a unit is isolated only from ports within this group, while not isolated from ports in isolation groups on other units.
2) The port isolation feature is synchronous on the same unit within an aggregation group, see the following details:

- When a port in an aggregation group is added in or removed from an isolation group, then all the other ports of this aggregation group on the same unit are automatically added in or removed from this isolation group.
- In the same aggregation group, the port isolation feature on one unit is consistent.
- A port is removed from an aggregation group with its isolation feature not change.
- If a port of an aggregation group is isolated on unit 1, then you can achieve the port-to-port isolation between this aggregation group and all the ports of the isolation group on unit 1.
- If all the ports on unit 1 of this aggregation group are removed from this aggregation group, then the isolation feature of this aggregation group is disabled, that is, the port-to-port isolation mentioned above is unavailable.

1.2.4 Enable Access Management Trap

You can use the following command to enable access management trap.

Table 1-4 Enable access management trap

Operation	Command	Description
Enter system view	**system-view**	—
Enable access management trap	**am trap enable**	Required By default, the access management trap is disabled

1.3 Display Access Management

After the above configuration, execute **display** command in any view to display the current configurations of access management on the ports, and to verify the effect of the configuration.

Table 1-5 Display current configuration of access management

Operation	Command	Description
Display current configuration of access management	**display am** [*interface-list*]	Execute these commands in any view.
Display information about the Ethernet ports added to the isolation group	**display isolate port**	

1.4 Access Management Configuration Example

I. Networking requirements

Organization 1 is connected to the port 1 of the switch, and organization 2 to the port 2. The ports 1 and 2 belong to the same VLAN. The IP addresses ranging 202.10.20.1~202.10.20.20 can be accessed from the port 1 and those ranging 202.10.20.21~202.10.20.50 from the port 2. Organization 1 and organization 2 cannot communicate with each other.

II. Networking diagram

See Figure 1-1.

III. Configuration procedure

Enable access management.

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] am enable
```

Configures the IP address pool for access management on port 1.

```
[H3C] interface ethernet1/0/1
[H3C-Ethernet1/0/1] am ip-pool 202.10.20.1 20
```

Add Ethernet1/0/1 to the isolation group.

```
[H3C-Ethernet1/0/1] port isolate
```

Configures the IP address pool for access management on port 2.

```
[H3C-Ethernet1/0/1] quit
[H3C] interface ethernet1/0/2
[H3C-Ethernet1/0/2] am ip-pool 202.10.20.21 30
```

Add Ethernet1/0/2 to the isolation group.

```
[H3C-Ethernet1/0/2] port isolate
```

Table of Contents

Appendix A Acronyms A-1

Appendix A Acronyms

A	
AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
ACL	Access Control List
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Border Router
B	
BDR	Backup Designated Router
C	
CAR	Committed Access Rate
CLI	Command Line Interface
CoS	Class of Service
D	
DHCP	Dynamic Host Configuration Protocol
DR	Designated Router
D-V	Distance Vector Routing Algorithm
E	
EGP	Exterior Gateway Protocol
F	
FTP	File Transfer Protocol
G	
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GVRP	GARP VLAN Registration Protocol
GMRP	GARP Multicast Registration Protocol
H	
HGMP	Huawei Group Management Protocol
I	
IAB	Internet Architecture Board

ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
L	
LSA	Link State Advertisement
LSDB	Link State DataBase
M	
MAC	Medium Access Control
MIB	Management Information Base
N	
NBMA	Non Broadcast MultiAccess
NIC	Network Information Center
NMS	Network Management System
NVRAM	Nonvolatile RAM
O	
OSPF	Open Shortest Path First
P	
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
Q	
QoS	Quality of Service
R	
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
S	
SNMP	Simple Network Management Protocol
SP	Strict Priority
STP	Spanning Tree Protocol
T	
TCP/IP	Transmission Control Protocol/ Internet Protocol

TFTP	Trivial File Transfer Protocol
ToS	Type of Service
TTL	Time To Live
U	
UDP	User Datagram Protocol
V	
VLAN	Virtual LAN
VOD	Video On Demand
VRRP	Virtual Router Redundancy Protocol
W	
WRR	Weighted Round Robin
X	
XID	eXchange Identification
XRN	eXpandable Resilient Networking