



H3C S3600 Series Ethernet Switches

Operation Manual

Hangzhou H3C Technologies Co., Ltd.
<http://www.h3c.com>

Manual Version: 20100510-C-1.01
Product Version: Release 1702

Copyright © 2007-2010, 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, , H³Care, , TOP G, , IRF, NetPilot, Neoclan, NeoVTL, SecPro, SecPoint, SecEngine, SecPath, Comware, Secware, Storware, NQA, VVG, V²G, VⁿG, 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.

Technical Support

customer_service@h3c.com

<http://www.h3c.com>

Table of Contents

1 About This Document	1-1
Audience	1-1
Part Organization	1-1
New Features	1-4
Conventions	1-6
Command conventions	1-6
GUI conventions	1-6
Symbols	1-6
2 H3C S3600 Series Documentation Guide	2-1
Obtaining the Documentation	2-1
CD-ROM	2-1
H3C Website	2-1
Software Release Notes	2-1
Related Documentation	2-1
Finding Documents at the H3C Website	2-2
Documentation Feedback	2-2
3 Product Overview	3-1
Product Overview	3-1
Network Scenarios	3-2
Broadband Ethernet Access for Residential Communities	3-2
Branch or Small- to Medium-Sized Enterprise Networks	3-2
Large Enterprise and Campus Networks	3-3

1 About This Document

The *H3C S3600 Series Ethernet Switches Operation Manual, Release 1702* describes the software features available in the S3600 series software release 1702, and guides you through the software feature configuration procedures.

Audience

This document is for administrators who are configuring and maintaining the S3600 series switches.

Part Organization

[Table 1-1](#) presents the part organization of this document:

Table 1-1 Part organization

Part	Contents
1 CLI	• Introduction to CLI • CLI Configuration
2 Login	• Logging In Through the Console Port • Logging In Through Telnet or SSH • Logging In Using a Modem • Logging In Through Web or NMS • Configuring Source IP Address for Telnet Service Packets • Controlling Login Users by Using ACL • Switching User Level
3 Configuration File Management	• Introduction to Configuration File • Saving the Current Configuration • Erasing the Startup Configuration File • Specifying a Configuration File for Next Startup
4 VLAN	• Basic VLAN Configuration • Configuring Port-Based VLAN • Configuring Protocol-Based VLAN
5 IP Address and Performance	• Configuring an IP address for a Switch • Configuring the TCP Attributes for a Switch • Enabling Reception of Directed Broadcasts to a Directly Connected Network • Disabling the Switch from Sending ICMP Error Messages • Canceling the System-Defined ACLs for ICMP Attack Guard
6 Voice VLAN	• Voice VLAN Overview • Voice VLAN Configuration
7 GVRP	• Introduction to GVRP • GVRP Configuration
8 Port Basic Configuration	• Configuring Speed Options for Auto Negotiation on a Port • Configuring Flow Control on a Port • Duplicating the Configuration of a Port to Other Ports • Enabling Loopback Test • Enabling Giant-Frame Statistics Function • Limiting Traffic on a Port • Setting Broadcast Storm Suppression Globally • Configuring Loopback Detection on a Port • Enabling Cable Test on a Port

Part	Contents
9 Link Aggregation	- Configuring a Manual Aggregation Group - Configuring a Static LACP Aggregation Group - Configuring a Dynamic LACP Aggregation Group
10 Port Isolation	Configuring Port Isolation Group
11 Port Security-Port Binding	- Setting the Maximum Number of Secure MAC Addresses Allowed on a Port - Setting the Port Security Mode - Configuring Port Security Features - Configuring Guest VLAN for a Port in macAddressOrUserLoginSecure mode - Ignoring the Authorization Information from the RADIUS Server - Configuring Secure MAC Addresses - Configuring MAC-IP-Port Binding
12 DLDP	Device link detection protocol (DLDP)
13 MAC Address Table Management	- Introduction to MAC Address Table - Configuring a MAC Address Entry - Setting the MAC Address Aging Timer - Setting the Maximum Number of MAC Addresses a Port Can Learn - Enabling Destination MAC Address Triggered Update - Assigning MAC Addresses for Ethernet Ports
14 Auto Detect	- Auto Detect Basic Configuration - Auto Detect Implementation in Static Routing - Auto Detect Implementation in VRRP - Auto Detect Implementation in VLAN Interface Backup
15 MSTP	- STP/RSTP/MSTP Overview and Basic Configuration - Performing mCheck Operation - Guard Functions: BPDU Guard, Root Guard, Loop Guard, TC-BPDU Attack Guard, and BPDU Drop - Digest Snooping - Rapid Transition - VLAN-VPN Tunnel - MSTP Maintenance Configuration - Sending Trap Messages Conforming to 802.1d Standard
16 Routing Protocols.	- Static Route - Routing Information Protocol (RIP) v1/v2 - Open Shortest Path First (OSPF) (available only on the S3600-EI series) - Routing Policy - Route Capacity Limiting (available only on the S3600-EI series)
17 Multicast	- Multicast Overview - Configuring the Common Multicast Functions - Internet Group Management Protocol (IGMP) (available only on the S3600-EI series) - Protocol Independent Multicast (PIM) (available only on the S3600-EI series) - Multicast Source Discovery Protocol (MSDP) (available only on the S3600-EI series) - Internet Group Management Protocol Snooping (IGMP Snooping)
18 802.1X and System Guard	802.1X Authentication - Guest VLAN - Quick EAD Deployment - Huawei Authentication Bypass Protocol (HABP) - System Guard
19 AAA	- Authentication, Authorization, and Accounting (AAA) - Remote Authentication Dial-In User Service (RADIUS) - Huawei Terminal Access Controller Access Control System (HWTACACS) - Endpoint Admission Defense (EAD)
20 Web Authentication	- Web Authentication Configuration - Configuring HTTPS Access for Web Authentication - Customizing Web Authentication Pages

Part	Contents
21 MAC Address Authentication	• Basic MAC Address Authentication • Enhanced MAC Address Authentication
22-VRRP	• Virtual Router Redundancy Protocol (VRRP) Basic Configuration • VRRP Tracking
23 ARP	• ARP • Gratuitous ARP • ARP Attack Detection • Proxy ARP • Resilient ARP • MFF
24 DHCP	• DHCP Server (available only on the S3600-EI series) • DHCP Relay Agent • DHCP Snooping • DHCP Packet Rate Limit • DHCP/BOOTP Client
25 ACL	• Basic ACLs • Advanced ACLs • Layer 2 ACLs • User-Defined ACLs • IPv6 ACLs (available only on the S3600-SI series) • Applying ACLs to Ports • Applying ACLs to VLANs
26 QoS-QoS Profile	• Quality of Service (QoS) • QoS Profile
27-Web Cache Redirection	Web Cache Redirection (available only on the S3600-EI series)
28 Mirroring	• Traffic Mirroring • Local Port Mirroring • Remote Port Mirroring (available only on the S3600-EI series)
29-IRF Fabric	• IRF Fabric • Specifying the Fabric Port of a Switch • IRF Fabric Detection • IRF Automatic Fabric
30 Cluster	• Huawei Group Management Protocol (HGMP) v2 • Neighbor Discovery Protocol (NDP) • Neighbor Topology Discovery Protocol (NTDP) • Enhanced Cluster Features • Cluster Synchronization Functions
31-PoE-PoE Profile	• PoE Configuration • PoE Profile Configuration
32-UDP Helper	• Introduction to UDP Helper • Configuring UDP Helper
33 SNMP-RMON	• Simple Network Management Protocol (SNMP) v1, v2, v3 • Configuring Trap-Related Functions • Remote Monitoring (RMON)
34 NTP	• Introduction to NTP • Configuring NTP Implementation Modes • Configuring Access Control Right • Configuring NTP Authentication • Configuring Optional NTP Parameters
35 SSH	• SSH Overview • Configuring the SSH Server • Configuring the SSH Client
36 File System Management	• File System Configuration • File Attribute Configuration

Part	Contents
37 FTP-SFTP-TFTP	- FTP and SFTP Configuration - TFTP Configuration
38 Information Center	- Information Center Overview - Information Center Configuration
39 System Maintenance and Debugging	- Boot ROM and Host Software Loading - Basic System Configuration and Debugging - Network Connectivity Test - Device Management - Scheduled Task Configuration
40 VLAN-VPN	- VLAN VPN (QinQ) - Enabling Transparent IGMP Message Transmission on a VLAN-VPN Port - Configuring the Inner-to-Outer Tag Priority Replication - Configuring TPID Value - Selective QinQ - BPDU Tunnel
41 HWPing	- HWPing Server/HWPing Client Configuration - Nine test types, including ICMP test, DHCP test, FTP test, HTTP test, DNS test, SNMP test, jitter test, TCP test, and UDP test
42 IPv6 Management	- IPv6 Management - Static IPv6 Route - IPv6 DNS - IPv6 Application Configuration
43 DNS	IPv4 Domain Name System (DNS)
44 Smart Link-Monitor Link	- Smart Link - Monitor Link
45 Access Management	- Access Management Overview - Configuring Access Management
46 LLDP	- Basic Link Layer Discovery Protocol (LLDP) configuration - CDP Compatibility - LLDP Trapping
47 PKI	- Submitting a PKI Certificate Request in Auto Mode or in Manual Mode - Verifying, Retrieving, and Deleting a PKI Certificate - Configuring an Access Control Policy
48 SSL	- Configuring an SSL Server Policy - Configuring an SSL Client Policy
49 HTTPS	- HTTPS Service - Associating the HTTPS Service with an SSL Server Policy - Associating the HTTPS Service with a Certificate Attribute Access Control Policy - Associating the HTTPS Service with an ACL

New Features

H3C S3600 Series Ethernet Switches Operation Manual-Release 1702 and *H3C S3600 Series Ethernet Switches Command Manual-Release 1702* are for software release 1702.

See [Table 1-2](#) for new features introduced in release 1702.

Table 1-2 New features in release 1702

New features	Reference
Command alias configuration	01-CLI

Canceling the system-defined ACLs for ICMP attack guard	05-IP Address and Performance
Configuring QoS priority settings for voice traffic on an interface	06-Voice VLAN
Configuring flow control on Ethernet ports	08-Port Basic Configuration
Configuring loopback port auto-shutdown and loopback detection on Ethernet ports in bulk	
Configuring storm suppression thresholds in kbps	
Various types of characters in port descriptions	
Configuring Guest VLAN for port security	11-Port Security-Port Binding
Configuring the aging time for learned secure MAC address entries	
Configuring port-MAC-IP binding	
Configuring PIM prune delay (available only on the S3600-EI series)	17-Multicast Protocol
Configuring the source address to be carried in IGMP group-specific queries	
Disabling a port from becoming a router port	
CPU protection	18-802.1X and System-Guard
Ignoring assigned RADIUS authorization attributes	19-AAA
Auto VLAN	
Setting the maximum online time for Web authentication users	20-Web Authentication
Configuring HTTPS access for Web authentication	
Customizing Web authentication pages	
VRRP (available only on the S3600-SI series Ethernet switches)	22-VRRP
ARP attack defense	23-ARP
Local proxy ARP	
MFF	
The qos-profile keyword, and IP filtering based on authenticated 802.1X clients	24-DHCP
Removing DHCP snooping entries	
Configuring the DHCP relay agent to process DHCP-INFORM messages in an IRF system	
IPv6 ACLs	25-ACL
Port mirroring–STP collaboration	28-Mirroring
Cluster synchronization	30-Cluster
Enabling auto power down on an electrical Ethernet port	39-System Maintenance and Debugging
Scheduled task configuration	
Enabling transparent IGMP message transmission on a VLAN-VPN port	40-VLAN-VPN
New HWPing commands, including: adv-factor , datafill , description , display hwping statistics , filesize , history keep-time , history-record enable , hwping-agent clear , hwping-agent max-requests , sendpacket passroute ,	41-HWPing

statistics, statistics keep-time, test-time begin, and ttl.	
LLDP	46-LLDP
PKI	47-PKI
SSL	48-SSL
HTTPS	49-HTTPS

Conventions

Command conventions

Convention	Description
Boldface	The keywords of a command line are in Boldface .
<i>italic</i>	Command arguments are in <i>italic</i> .
[]	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.
&<1-n>	The argument(s) before the ampersand (&) sign can be entered 1 to n times.
#	A line starting with the # sign contains comments.



Note

Command line interface (CLI) commands of H3C products are case insensitive.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the New User window appears; click OK .
>	Multi-level menus are separated by angle brackets. For example, File > Create > Folder .

Symbols

Convention	Description
 Warning	Means reader be extremely careful. Improper operation may cause bodily injury.

Convention	Description
 Caution	Means reader be careful. Improper operation may cause data loss or damage to equipment.
 Note	Means a complementary description.
 Tip	Means techniques helpful for you to make configuration with ease.

2 H3C S3600 Series Documentation Guide

Obtaining the Documentation

You can obtain the H3C S3600 series documentation in these ways:

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

CD-ROM

H3C delivers a CD-ROM together with each device. The CD-ROM contains a complete set of electronic documents of the product, including operation manuals and command manuals. 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.

H3C Website

To obtain up-to-date documentation and technical support, go to <http://www.h3c.com>.

Go to the following columns for different categories of product documentation:

[Products & Solutions]: Provides information about products and technologies, as well as solutions.

[Technical Support & Document > Technical Documents]: Provides several categories of product documentation, such as installation, configuration, and maintenance.

[Technical Support & Document > Software Download]: Provides the documentation released with the software version.

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.

Related Documentation

Use the documents listed in [Table 2-1](#) together with *H3C S3600 Series Ethernet Switches Operation Manual* to make full use of the benefits delivered by the S3600 series.

Table 2-1 Related documentation

Document title	Description
<i>H3C S3600 Series Ethernet Switches Command Manual-Release 1702</i>	Describes the commands for the <i>S3600 Series Ethernet Switches</i> . A master index of all commands covered by the whole manual is provided for the ease of retrieval.

Document title	Description
<i>H3C S3600 Series Ethernet Switches Installation Manual</i>	Describes the physical views and hardware specifications of the H3C S3600 series switches, and guides you through the installation, power-on and startup, troubleshooting and maintenance procedures.
<i>H3C S3600 Series Ethernet Switches Compliance and Safety Manual</i>	Provides the safety and regulatory compliance statements, and describes the protection actions that you must take when installing and maintaining the H3C S3600 series switches.
<i>H3C Low-End Ethernet Switches Configuration Guide</i>	Describes the typical application scenarios, and provides configuration examples and configuration guidelines.

Finding Documents at the H3C Website

All these documents are available at the H3C website:

- For software feature descriptions and configuration procedures, see [H3C S3600 Series Ethernet Switches Operation Manual](#).
- For command reference, see [H3C S3600 Series Ethernet Switches Command Manual](#).
- For hardware specifications, installation, and troubleshooting, see [H3C S3600 Series Ethernet Switches Installation Manual](#).
- For typical application scenarios, configuration examples, and configuration guidelines, see [H3C Low-End Ethernet Switches Configuration Guides](#).

Documentation Feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

3 Product Overview

Product Overview

The H3C S3600 Series Ethernet Switches are multilayer switching products. They support abundant Layer 3 features and enhanced extended functions, in addition to Layer 2 features. The switches come in two series:

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

See [Table 3-1](#) for all S3600 switch models and their basic hardware specifications.

Table 3-1 S3600 switch hardware summary

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-PW R-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 x 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
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-PW R-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-PW R-EI	AC-/DC-input	52	48 10/100 Mbps ports (electrical)	4 Gigabit (SFP) ports	1
H3C S3600-52P-PW R-SI	AC-/DC-input	52	48 10/100 Mbps ports (electrical)	4 Gigabit (SFP) ports	1

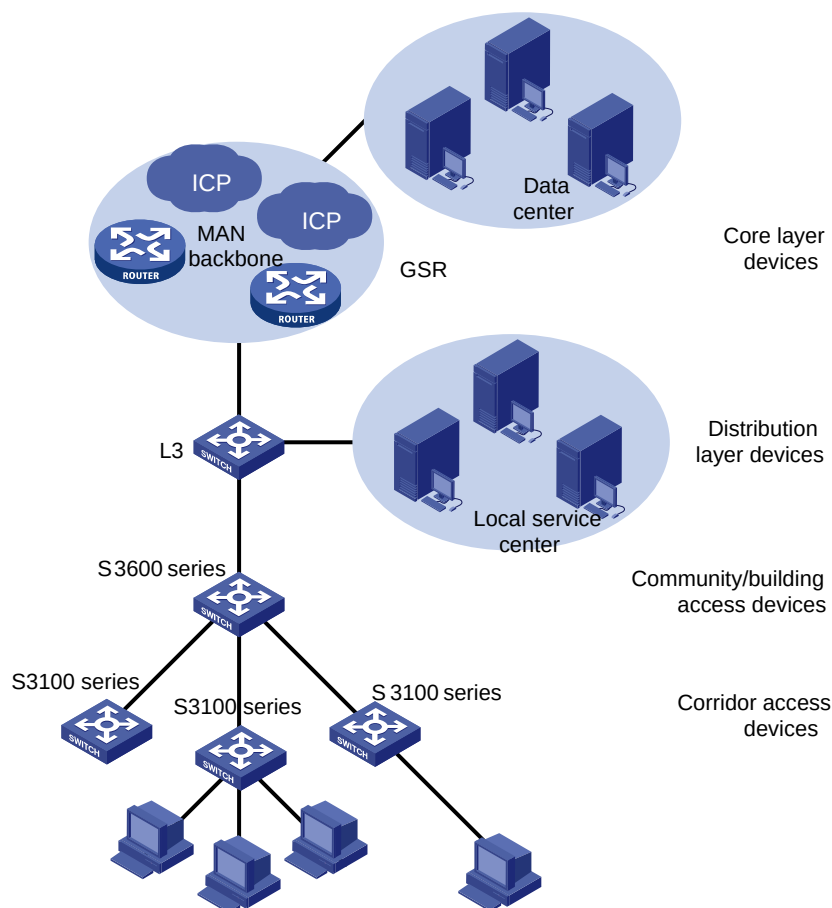
Network Scenarios

You can deploy the S3600 series on many types of networks, such as enterprise and broadband access networks. This section describes several typical application scenarios for the S3600 series.

Broadband Ethernet Access for Residential Communities

Deploy an S3600 series switch at the center of the broadband access network for a residential community. Connect the switch to the access S3100 series switches to reach end users, and to an upstream core Layer 3 switch through a GE port to access the MAN backbone.

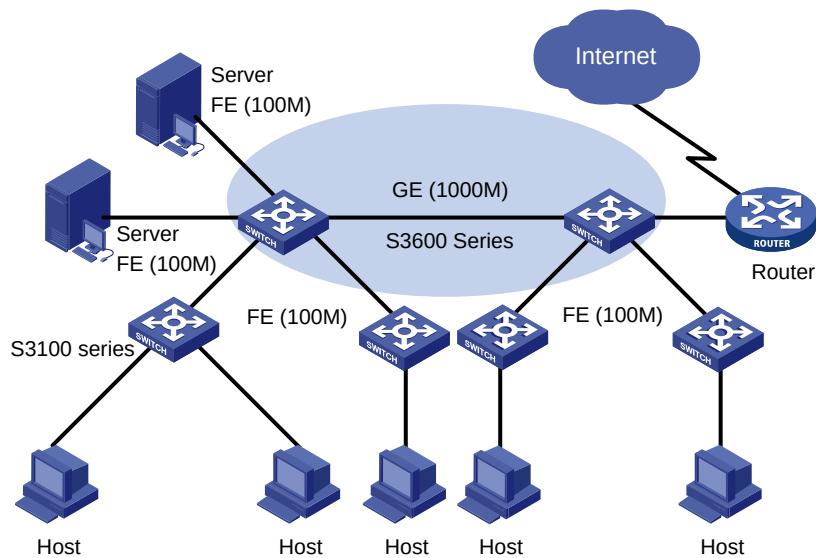
Figure 3-1 Community access network



Branch or Small- to Medium-Sized Enterprise Networks

Deploy the S3600 series switches as backbone switches on a branch or small-to medium-sized enterprise network. Connect the switches to the headquarters or other branches through routers. As the business grows, you can cascade the S3600 series to extend the network.

Figure 3-2 Branch or small-to medium-sized enterprise network



Large Enterprise and Campus Networks

Deploy the S3600 series switches at the distribution layer of a large enterprise or campus network to implement Gigabit-to-backbone and 100 Mbps-to-desktop together with other H3C switches. Connect the S3600 switches to the access Layer 2 switches (for example, the S3100 series), and to the core Layer 3 switches through GE ports.

Figure 3-3 S3600 series application in a large enterprise or campus network

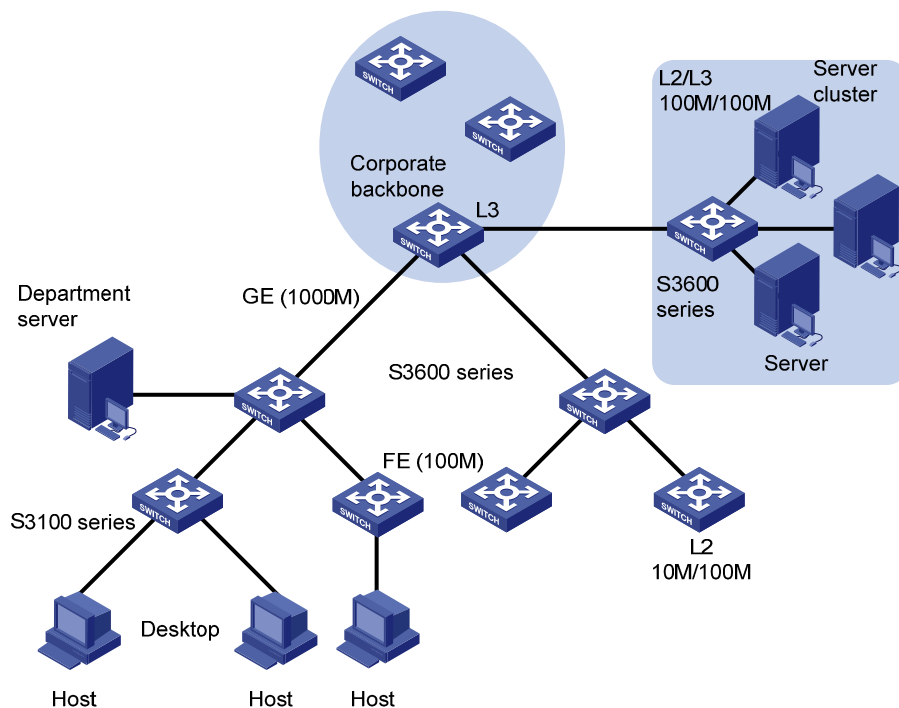


Table of Contents

1 CLI Configuration	1-1
What Is CLI?	1-1
Entering the CLI	1-1
Entering CLI Through the Console Port	1-2
Entering CLI Through Telnet	1-6
H3C Products CLI Descriptions	1-8
Command Conventions	1-8
CLI View Description	1-9
Tips on Using the CLI	1-14
Using the CLI Online Help	1-14
Command Line Error Information	1-15
Typing and Editing Commands	1-16
Displaying and Executing History Commands	1-16
Undo Form of a Command	1-17
Controlling CLI Display	1-17
CLI Configurations	1-18
Configuring Command Aliases	1-18
Synchronous Information Output	1-19
Configuring Command Levels	1-19
Saving Configurations	1-21

1 CLI Configuration

This chapter includes these sections:

- [What Is CLI?](#)
- [Entering the CLI](#)
- [H3C Products CLI Descriptions](#)
- [Tips on Using the CLI](#)
- [CLI Configurations](#)

What Is CLI?

The command line interface (CLI) is an interface where you can interact with your device by typing text commands. At the CLI, you can instruct your device to perform a given task by typing a text command and then pressing **Enter** to submit it to your device. At the CLI, you can enter commands to configure your switch, and verify the configuration based on the output. Thus, the CLI facilitates your switch configuration and management. The CLI of H3C switches is as shown in [Figure 1-1](#).

Figure 1-1 Schematic diagram for the CLI

```
*****
* Copyright (c) 2004-2009 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                  *
*****

User interface aux0 is available.

Please press ENTER.

<H3C>
#Feb 23 10:31:21:665 2010 H3C SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1<hh3cLogIn>: login from Console
%Feb 23 10:31:21:804 2010 H3C SHELL/4/LOGIN: Console login from aux0
<H3C>clock datetime 10:30:20 2/23/2010
<H3C>display clock
10:30:26 UTC Tue 02/23/2010
<H3C>system-view
System View: return to User View with Ctrl+Z.
[H3C]
```

Entering the CLI

The H3C S3600 Series Ethernet switches provide multiple methods of entering the CLI, as follows:

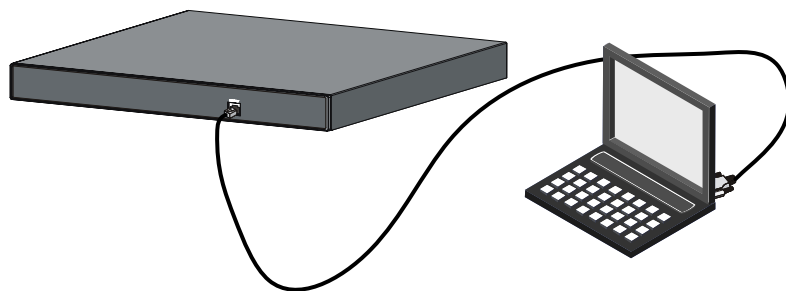
- Through the console port. For more information, see [Entering CLI Through the Console Port](#).
- Through Telnet. For more information, see [Entering CLI Through Telnet](#).
- Through SSH with encryption. For more information, see [SSH Configuration](#).

Entering CLI Through the Console Port

When you use the CLI of an H3C switch for the first time, you can log in to the switch and enter the CLI through the console port only. Follow these steps to log in to your H3C switch and enter the CLI through the console port:

- 1) Use the console cable shipped with your switch to connect your PC to your switch. Plug the DB-9 (female) connector of the console cable into the 9-pin serial port of your PC. Then plug the RJ-45 connector of the console cable into the console port of your switch.

Figure 1-2 Use the console cable to connect your PC to your switch



Warning

Identify the interface to avoid connection errors.

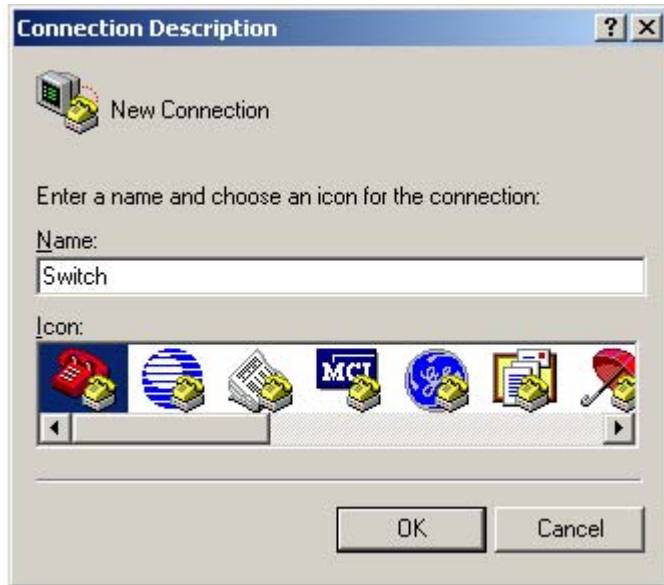


Note

Because the serial port of a PC is not hot swappable, do not plug or unplug the console cable when your switch is powered on. When connecting the PC to your switch, first plug the DB-9 connector of the console cable into the PC, and then plug the RJ-45 connector of the console cable into your switch. When disconnecting the PC from your switch, first unplug the RJ-45 connector and then the DB-9 connector.

- 2) Launch a terminal emulation utility on your PC. In this chapter, the HyperTerminal in Windows XP is used as an example. Click **Start > All Programs > Accessories > Communications > HyperTerminal** to enter the **HyperTerminal** window. The **Connection Description** window as shown in [Figure 1-3](#) appears. Type a connection name (**Switch**, for example) in the **Name** input box, and click **OK**.

Figure 1-3 Connection description



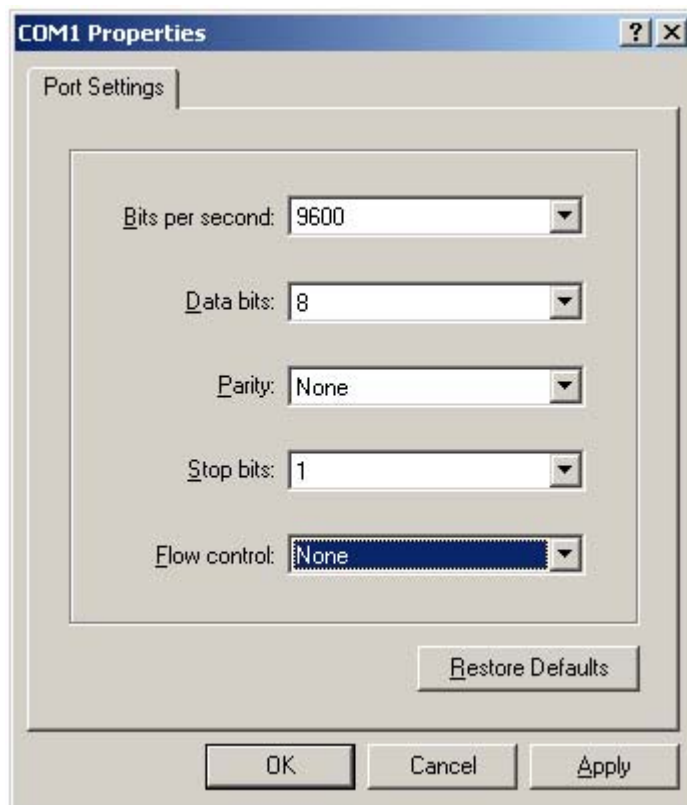
- 3) Then, the **Connect To** window as shown in [Figure 1-4](#) appears. Select the serial port you want to use from the **Connect using** drop-down list, and then click **OK**.

Figure 1-4 Specify the serial port used to establish the connection



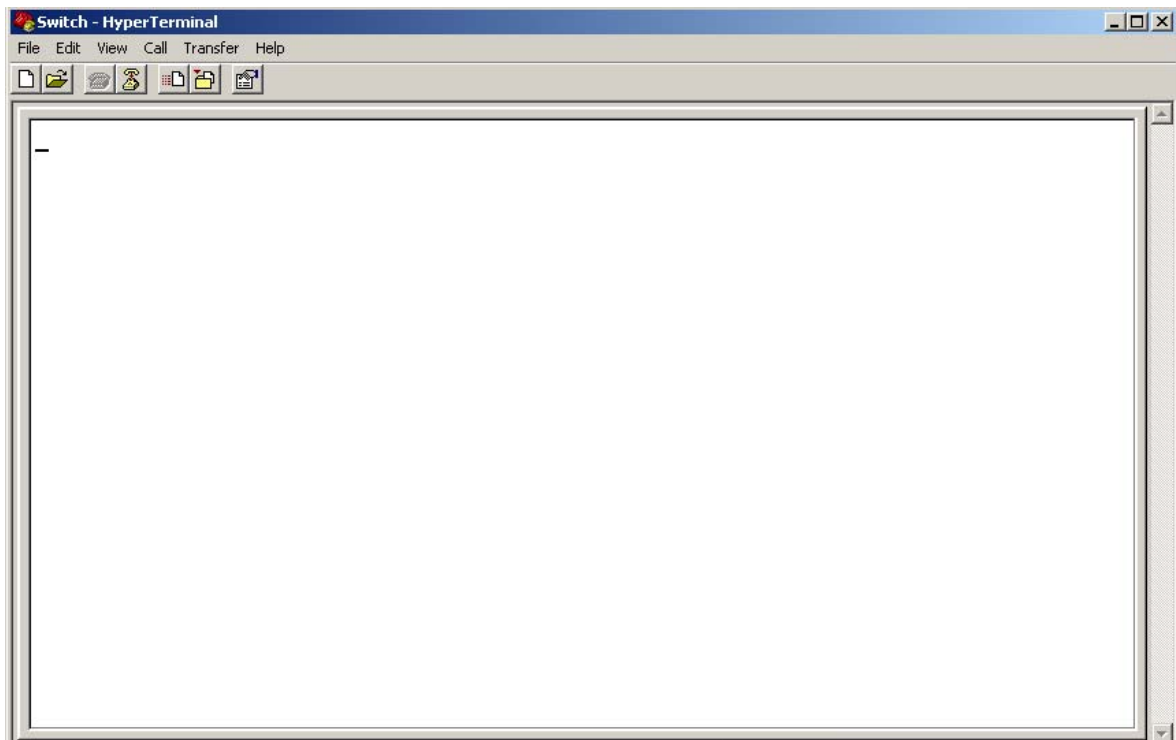
- 4) The **COM1 Properties** window as shown in [Figure 1-5](#) appears. On the window, set **Bits per second** to **9600**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**. Click **OK**.

Figure 1-5 Set the properties of the serial port



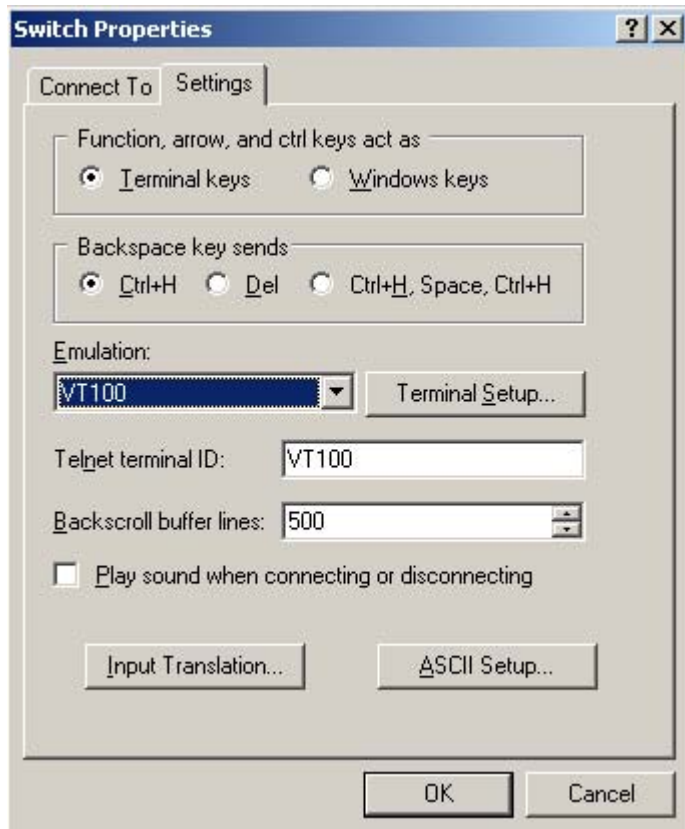
5) The HyperTerminal window as shown in [Figure 1-6](#) appears.

Figure 1-6 The HyperTerminal window



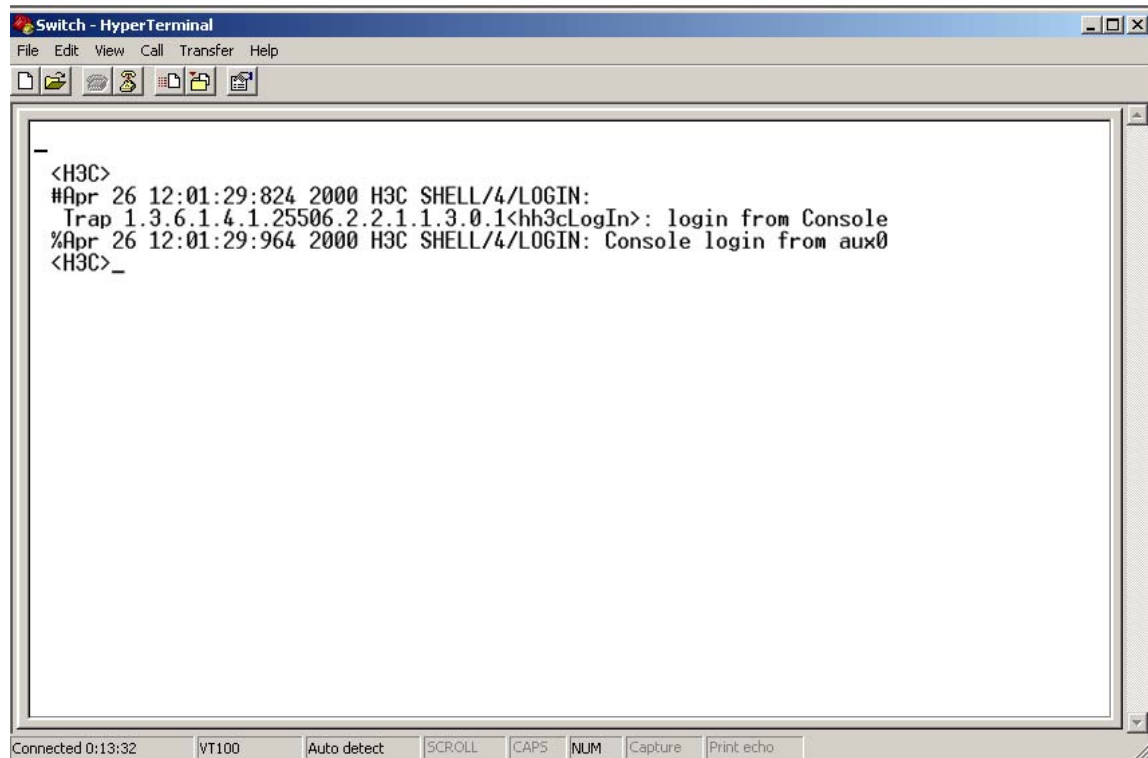
Select **File > Properties** on the HyperTerminal window, and the **Switch Properties** window appears. Select the **Settings** tab as shown in [Figure 1-7](#), select **VT100** from the **Emulation** drop-down list, and then click **OK**.

Figure 1-7 Select the emulation terminal on the **Switch Properties** window



- 6) Press **Enter** on the **HyperTerminal** window. Then the CLI of your switch appears on the window, as shown in [Figure 1-8](#), indicating that you have logged in to your switch successfully.

Figure 1-8 Schematic diagram for successful login through the console port



Entering CLI Through Telnet

After you log in to your switch through the console port for the first time, it is recommended that you configure Telnet login as soon as possible, so that you can use a remote terminal to configure and manage your switch.

Telnet login authentication methods

In order to restrict the login to your switch, H3C provides three Telnet login authentication methods. Select a proper method according to your network conditions.

Table 1-1 Telnet login authentication methods

Authentication method	Description	Application scenarios	Configuration
None	• Easy to configure • Allows any user to telnet to your switch • Least secure	Lab environments and extremely secure network environments	For more information, see <i>Login Configuration</i> .
Password	• Easy to configure • Allows any user knowing the password to telnet to your switch • Secure, but incapable of assigning different privilege levels to different users	Environments that do not need granular privilege management	

Authentication method	Description	Application scenarios	Configuration
Username and password	• Complex to configure • Allows users inputting the correct username and password to telnet to your switch • Most secure, and capable of assigning different privilege levels to different users	Environments where multiple operators cooperate to manage the device	

An H3C switch provides multiple VTY user interfaces. At one time, only one user can telnet to a VTY user interface. Because a remote terminal cannot select the VTY user interface through which it logs in to the switch, it is recommended that you configure all VTY user interfaces with the same authentication method. The following example is configured in this way.



Note

The number of VTY user interfaces provided by a H3C device varies by switch model. In this document, a switch providing five VTY user interfaces is used as an example, which means that the VTY user interface number ranges from 0 to 4. If your switch provides a different number of VTY user interfaces, make sure that the VTY interface number you configure is within the actual range.

Telnet login configuration example

Enter system view.

```
<Sysname> system-view
```

Enable the telnet service.

```
[Sysname] telnet server enable
```

Create VLAN-interface 1.

```
[Sysname] interface vlan-interface 1
```

Assign an IP address to VLAN-interface 1 according to the IP network segment distribution and usage in the current network. 192.168.0.72 is used as an example.

```
[Sysname-Vlan-interface1] ip address 192.168.0.72 24
```

```
[Sysname-Vlan-interface1] quit
```

Enter the view of VTY user interfaces 0 through 4.

```
[Sysname] user-interface vty 0 4
```

```
[Sysname-ui-vty0-4]
```

Configure the authentication method for the VTY user interfaces as needed.

Omitted. For more information, see *Login Configuration*.

Configure the command level available to the users that log in through VTY user interfaces 0 through 4. Command level 3 is used as an example, which means that the users can use all commands.

H3C Products CLI Descriptions

Command Conventions

Before using commands provided in H3C product manuals, learn the command conventions to understand the command meanings.

Commands in H3C product manuals comply with the following conventions, as described in [Table 1-2](#).

Table 1-2 Command conventions

Convention	Description
Boldface	The keywords of a command line are in Boldface . Keep keywords unchanged when typing them in the CLI.
<i>Italic</i>	Command arguments are in <i>italic</i> . Replace arguments with actual values in the CLI.
[]	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.
&<1-n>	The argument(s) before the ampersand (&) sign can be entered 1 to n times.
#	A line starting with the # sign is comments.

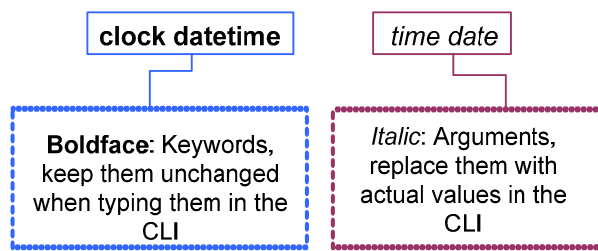


Note

H3C command lines are case insensitive.

Take the **clock datetime** *time date* command as an example to understand the command meaning according to [Table 1-2](#).

Figure 1-9 Read command line parameters



Type the following command line in the CLI of a device and press **Enter**. You set the device system time to 10 o'clock 30 minutes 20 seconds, February 23, 2010.

```
<Sysname> clock datetime 10:30:20 2/23/2010
```

You can read any commands more complicated according to [Table 1-2](#).

CLI View Description

CLI views are designed for different configuration tasks. These are how commands are organized, with groupings of tasks for related operations. For example, once a user logs into a switch successfully, the user enters user view, where the user can perform some simple operations such as checking the operation status and statistics information of the switch. After executing the **system-view** command, the user enters system view, and there are other views below this accessible by entering corresponding commands.

[Table 1-3](#) lists the CLI views provided by S3600 Series Ethernet switches, operations that can be performed in different CLI views and the commands used to enter specific CLI views.

Table 1-3 CLI views

View	Available operation	Prompt example	Enter method	Quit method
User view	Display operation status and statistical information of the switch	<Sysname>	Enter user view once logging into the switch.	Execute the quit command to log out of the switch.
System view	Configure system parameters	[Sysname]	Execute the system-view command in user view.	Execute the quit or return command to return to user view.

View	Available operation	Prompt example	Enter method	Quit method
Ethernet port view	Configure Ethernet port parameters	100 Mbps Ethernet port view: [Sysname-Ethernet1/0/1]	Execute the interface ethernet command in system view.	Execute the quit command to return to system view. Execute the return command to return to user view.
		1000 Mbps Ethernet port view: [Sysname-GigabitEthernet1/1/1]	Execute the interface gigabitethernet command in system view.	
Aux1/0/0 port (the console port) view	The S3600 series do not support configuration on port Aux1/0/0	[Sysname-Aux1/0/0]	Execute the interface aux 1/0/0 command in system view	
VLAN view	Configure VLAN parameters	[Sysname-vlan1]	Execute the vlan command in system view.	
VLAN interface view	Configure VLAN interface parameters, including the management VLAN parameters	[Sysname-Vlan-interface1]	Execute the interface Vlan-interface command in system view.	
Loopback interface view	Configure loopback interface parameters	[Sysname-LoopBack0]	Execute the interface loopback command in system view.	
NULL interface view	Configure NULL interface parameters	[Sysname-NULL0]	Execute the interface null command in system view.	
Local user view	Configure local user parameters	[Sysname-luser-user1]	Execute the local-user command in system view.	
User interface view	Configure user interface parameters	[Sysname-ui-aux0]	Execute the user-interface command in system view.	
FTP client view	Configure FTP client parameters	[ftp]	Execute the ftp command in user view.	
SFTP client view	Configure SFTP client parameters	sftp-client>	Execute the sftp command in system view.	
MST region view	Configure MST region parameters	[Sysname-mst-region]	Execute the stp region-configuration command in system view.	

View	Available operation	Prompt example	Enter method	Quit method
Cluster view	Configure cluster parameters	[Sysname-cluster]	Execute the cluster command in system view.	
Scheduled task view	Configure scheduled task parameters	[Sysname-job-pc1]	Execute the job command in system view.	
Public key view	Configure the RSA public key for SSH users	[Sysname-rsa-public-key]	Execute the rsa peer-public-key command in system view.	Execute the peer-public-key end command to return to system view.
	Configure the RSA or DSA public key for SSH users	[Sysname-peer-public-key]	Execute the public-key peer command in system view.	
Public key editing view	Edit the RSA public key for SSH users	[Sysname-rsa-key-code]	Execute the public-key-code begin command in public key view.	Execute the public-key-code end command to return to public key view.
	Edit the RSA or DSA public key for SSH users	[Sysname-peer-key-code]		
DHCP address pool view	Configure DHCP address pool parameters This configuration is supported by only the S3600-EI series.	[Sysname-dhcp-pool-a123]	Execute the dhcp server ip-pool 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 This configuration is supported by only the S3600-EI series.	[Sysname-pim]	Execute the pim command in system view. If multicast routing is not enabled, you should first execute the multicast routing-enable command.	Execute the return command to return to user view.
RIP view	Configure RIP protocol parameters	[Sysname-rip]	Execute the rip command in system view.	
OSPF view	Configure OSPF protocol parameters Supported by only S3600-EI series switches	[Sysname-ospf-1]	Execute the ospf command in system view.	

View	Available operation	Prompt example	Enter method	Quit method
OSPF area view	Configure OSPF area parameters Supported by only S3600-EI series switches	[Sysname-ospf-1-area-0.0.0.1]	Execute the area 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 policy	[Sysname-route-policy]	Execute the route-policy command in system view.	Execute the quit command to return to system view.
Basic ACL view	Define rules for a basic ACL (with ID ranging from 2000 to 2999)	[Sysname-acl-basic-2000]	Execute the acl number command in system view.	Execute the return command to return to user view.
Advanced ACL view	Define rules for an advanced ACL (with ID ranging from 3000 to 3999)	[Sysname-acl-adv-3000]	Execute the acl number command in system view.	
Layer 2 ACL view	Define rules for an layer 2 ACL (with ID ranging from 4000 to 4999)	[Sysname-acl-ethernetframe-4000]	Execute the acl number command in system view.	
User-defined ACL view	Define rules for a user-defined ACL (with ID ranging from 5000 to 5999)	[Sysname-acl-user-5000]	Execute the acl number command in system view.	
IPv6 ACL view	Define rules for a IPv6 ACL (with ID ranging from 5000 to 5999)	[Sysname-acl-user-5000]	Execute the acl number command in system view.	
QoS profile view	Define QoS profile	[Sysname-qos-profile-a123]	Execute the qos-profile command in system view.	
RADIUS scheme view	Configure RADIUS scheme parameters	[Sysname-radius-1]	Execute the radius scheme command in system view.	
ISP domain view	Configure ISP domain parameters	[Sysname-isp-aa a123.net]	Execute the domain command in system view.	
HWPing test group view	Configure HWPing test group parameters	[Sysname-hwping-a123-a123]	Execute the hwping command in system view.	

View	Available operation	Prompt example	Enter method	Quit method
HWTACACS view	Configure HWTACACS parameters	[Sysname-hwtacacs-a123]	Execute the hwtacacs scheme command in system view.	
MSDP view	Configure MSDP parameters This configuration is supported by only the S3600-EI series.	[Sysname-msdp]	Execute the msdp command in system view.	
PoE profile view	Configure PoE profile parameters	[Sysname-poe-profile-a123]	Execute the poe-profile command in system view.	
Smart link group view	Configure smart link group parameters	[Sysname-smlk-group1]	Execute the smart-link group command in system view.	
Monitor link group view	Configure monitor link group parameters	[Sysname-mtlk-group1]	Execute the monitor-link group command in system view.	
Detected group view	Configure detected group parameters	[Sysname-detect-group-1]	Execute the detect-group command in system view.	
PKI domain view	Configure PKI domain parameters	[Sysname-pki-domain-1]	Execute the pki domain command in system view.	
PKI entity view	Configure PKI entity parameters	[Sysname-pki-entity-en]	Execute the pki entity command in system view.	
PKI certificate attribute group view	Configure PKI certificate attribute group parameters	[Sysname-cert-attribute-group-mygroup]	Execute the pki certificate attribute-group command in system view.	
PKI certificate attribute-based access control policy view	Configure PKI certificate attribute-based access control policy	[Sysname-cert-access-control-policy-mypolicy]	Execute the pki certificate access-control-policy command in system view.	
SSL server policy view	Configure SSL server policy parameters	[Sysname-ssl-server-policy-policy1]	Execute the ssl server-policy command in system view.	

View	Available operation	Prompt example	Enter method	Quit method
SSL client policy view	Configure SSL client policy parameters	[Sysname-ssl-client-policy-policy1]	Execute the ssl client-policy command in system view.	
QinQ view	Configure QinQ parameters	[Sysname-Ethernet1/0/1-vid-20]	Execute the vlan-vpn vid command in Ethernet port view. The vlan-vpn enable command should be first executed.	Execute the quit command to return to Ethernet port view. Execute the return command to return to user view.



Note

The shortcut key <Ctrl+Z> is equivalent to the **return** command.

Tips on Using the CLI

Using the CLI Online Help

In the CLI, you can type a question mark (?) to obtain detailed online help. See the following examples. Type ? in any view to display all commands available in this view and brief descriptions about these commands.

```
<Sysname> ?
```

```
User view commands:
```

```
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.....
```

Type part of a command and a ? separated by a space.

If ? is at the position of a keyword, the CLI displays all possible keywords with a brief description about each of these keywords.

```
<Sysname> terminal ?
```

```
debugging  Send debug information to terminal
logging    Send log information to terminal
monitor    Send information output to current terminal
trapping   Send trap information to terminal
```

If **?** is at the position of an argument, the CLI displays a description about this argument.

```
<Sysname> system-view
[Sysname] interface vlan-interface ?
    <1-4094>  VLAN interface number
[Sysname] interface vlan-interface 1 ?
    <cr>
[Sysname] interface vlan-interface 1
```

The string **<cr>** indicates that the command is already complete, and you can execute the command by pressing **Enter**.

Type a character string followed by a **?**. The CLI displays all commands starting with this string.

```
<Sysname> c?
    cd
    clock
    cluster
    copy
```

Type part of a keyword followed by a **?**. The CLI displays all keywords starting with the character string you typed.

```
<Sysname> display cl?
    clock
    cluster
```

Command Line Error Information

If a command you typed contains syntax errors, the CLI reports error information. [Table 1-4](#) lists some common command line errors.

Table 1-4 Common command line errors

Error information	Cause
% Unrecognized command found at '^' position.	The command was not found.
	The keyword was not found.
% Incomplete command found at '^' position.	Incomplete command
% Ambiguous command found at '^' position.	Ambiguous command
Too many parameters	Too many parameters
% Wrong parameter found at '^' position.	Wrong parameters

Typing and Editing Commands

Fuzzy match

The H3C S3600 series Ethernet switches support fuzzy match for efficient input of commands.

If in the current view, the character string you have typed can already uniquely identify a keyword, you do not need to type the complete keyword.

For example, in user view, commands starting with an **s** include **save**, **startup saved-configuration**, and **system-view**.

- To save the current configuration, type **sa**.
- To set the configuration file for next startup, type **st s**.
- To enter system view, type **sy**.

You can also press **Tab** to have a partial keyword automatically completed, and check that the keyword is the one you intended to use.

Editing command lines

[Table 1-5](#) lists some shortcut keys you can use to edit command lines.

Table 1-5 Editing functions

Key	Function
Common keys	If the edit buffer is not full, insert the character at the position of the cursor and move the cursor to the right.
Backspace	Deletes the character to the left of the cursor and move the cursor back one character.
Left arrow key or Ctrl+B	The cursor moves one character space to the left.
Right arrow key or Ctrl+F	The cursor moves one character space to the right.
Tab	If you press Tab after entering part of a keyword, the system automatically completes the keyword: • If finding a unique match, the system substitutes the complete keyword for the incomplete one and displays it in the next line. • If there is more than one match, you can press Tab repeatedly to display in cycles all the keywords starting with the character string that you typed. • If there is no match, the system does not modify the incomplete keyword and displays it again in the next line.

Displaying and Executing History Commands

The CLI automatically saves the commands recently used in the history command buffer. You can access commands in the history command buffer and execute them again.

Table 1-6 Access history commands

To do...	Use the key/command...	Result
Display history commands	display history-command	Displays valid history commands you used

To do...	Use the key/command...	Result
Access the previous history command	Up arrow key or Ctrl+P	Displays the previous history command, if any
Access the next history command	Down arrow key or Ctrl+N	Displays the next history command, if any



Note

You may use arrow keys to access history commands in Windows 200X and XP Terminal or Telnet. However, the up and down arrow keys are invalid in Windows 9X HyperTerminal, because they are defined differently. You can press **Ctrl+P** or **Ctrl+N** instead.

Note that:

- The commands saved in the history command buffer are in the same format in which you typed the commands. If you typed an incomplete command, the command saved in the history command buffer is also an incomplete one.
- If you execute the same command repeatedly, the device saves only the earliest record. However, if you execute the same command in different formats, the system saves them as different commands. For example, if you execute the **display cu** command repeatedly, the system saves only one command in the history command buffer. If you execute the command in the format of **display cu** and **display current-configuration** respectively, the system saves them as two commands.
- By default, the CLI can save up to ten commands for each user. You can use the **history-command max-size** command to set the capacity of the history command buffer for the current user interface (For more information about the **history-command max-size** command, see *Login Configuration*).

Undo Form of a Command

The **undo** form of a command typically restores the default, disables a function, or removes a configuration.

Most of configuration commands have their own **undo** form.

For example, the **info-center enable** command is used to enable the information center, while the **undo info-center enable** command is used to disable the information center.

Controlling CLI Display

Controlling Multi-Screen Display

If the output information spans multiple screens, each screen pauses after displayed. Then, you can perform one of the following operations to proceed.

Action	Function
Press Space	Displays the next screen.
Press Enter	Displays the next line.
Press Ctrl+C	Stops the display and the command execution.
Press <Ctrl+E>	Moves the cursor to the end of the current line.
Press <PageUp>	Displays the previous page.
Press <PageDown>	Displays the next page.

CLI Configurations

Configuring Command Aliases

You can replace the first keyword of a command supported by the device with your preferred keyword by configuring the command alias function. For example, if you configure **show** as the replacement of the **display** keyword for each **display** command, you can input the command alias **show xx** to execute the **display xx** command.

Note the following when you configure command aliases:

- When you type a command alias, the system displays and saves the command in its original format instead of its alias. That is, you can define and use a command alias but the command is not saved and restored in its alias.
- When you define a command alias, the *cmdkey* and *alias* arguments must be in complete form.
- With the command alias function enabled, when you type an incomplete keyword, which partially matches both a defined alias and the keyword of a command, the alias wins; to execute the command whose keyword partially matches your input, you must type the complete keyword. When you input a character string that matches multiple aliases partially, the system prompts you for various matching information.
- If you press **Tab** after you type the keyword of an alias, the original format of the keyword is displayed.
- You can replace only the first keyword of a non-undo command instead of the complete command; and you can replace only the second keyword of an **undo** command.

Follow these steps to configure command aliases:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the command alias function	command-alias enable	Required Disabled by default, that is, you cannot configure command aliases.
Configure command aliases	command-alias mapping <i>cmdkey alias</i>	Required Not configured by default.

To display the configured command aliases, use the **display command-alias** command.

Synchronous Information Output

Synchronous information output refers to the feature that if your input is interrupted by system output, then after the completion of system output the system displays a command line prompt and your input so far, and you can continue your operations from where you were stopped.

Follow these steps to enable synchronous information output:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable synchronous information output	info-center synchronous	Required Disabled by default



Note

With this feature enabled:

- If you have no input at the command line prompt and the system outputs system information, for example, logs, the system will not display the command line prompt after the outputs.
- If the system outputs system information when you are typing interactive information (not YES/NO for confirmation), the system will not redisplay the prompt information but a line break after the outputs and then what you have typed.

For information about the **info-center synchronous** command, refer to *Information Center Configuration Commands*.

Configuring Command Levels

Introduction

The device restricts different users' usage of the commands by using user privilege levels and command levels to protect the device against unauthorized users. User privilege levels correspond to command levels. When users at different privilege levels log in, they can only use commands at their own, or lower, levels.

All the commands are categorized into four levels, which are visit, monitor, system, and manage from low to high, and identified respectively by 0 through 3. [Table 1-7](#) describes the levels of the commands.

Table 1-7 Default command levels

Level	Privilege	Description
0	Visit	Involves commands for network diagnosis and commands for accessing an external device. Configuration of commands at this level cannot survive a device restart. Upon device restart, the commands at this level will be restored to the default settings. Commands at this level include ping , tracert , telnet and ssh2 .

Level	Privilege	Description
1	Monitor	Involves commands for system maintenance and service fault diagnosis. Commands at this level are not allowed to be saved after being configured. After the device is restarted, the commands at this level will be restored to the default settings. Commands at this level include debugging , terminal , refresh , reset , and send .
2	System	Provides service configuration commands, including routing and commands at each level of the network for providing services. By default, commands at this level include all configuration commands except for those at manage level.
3	Manage	Involves commands that influence the basic operation of the system and the system support modules for service support. By default, commands at this level involve file system, FTP, TFTP, Xmodem command download, user management, level setting, as well as parameter setting within a system (the last case involves those non-protocol or non RFC provisioned commands).

For how to configure the user privilege level, see *Login Configuration*.

Modifying the Command Level

All the commands are defaulted to different levels. The administrator can modify the default command level to improve management flexibility.

Follow these steps to change the command level:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the command level in a specified view	command-privilege level level view view command	Required Refer to Table 1-7 for the default settings.



Caution

- You are recommended to use the default command level or modify the command level under the guidance of professional staff; otherwise, the change of command level may bring inconvenience to your maintenance and operation, or even potential security problem.
- When you change the level of a command with multiple keywords or arguments, you should input the keywords or arguments one by one in the order they appear in the command syntax. Otherwise, your configuration will not take effect. The values of the arguments should be within the specified ranges.
- After you change the level of a command in a certain view to be lower than the default level, change the level of the command used to enter the view accordingly.

Modifying the Command Level Configuration example

The network administrator (a level 3 user) wants to change some TFTP commands (such as **tftp get**) from level 3 to level 0, so that general Telnet users (level 0 users) are able to download files through TFTP.

Change the **tftp get** command in user view (shell) from level 3 to level 0. (Originally, only level 3 users can change the level of a command.)

```
<Sysname> system-view
[Sysname] command-privilege level 0 view shell tftp
[Sysname] command-privilege level 0 view shell tftp 192.168.0.1
[Sysname] command-privilege level 0 view shell tftp 192.168.0.1 get
[Sysname] command-privilege level 0 view shell tftp 192.168.0.1 get bootrom.btm
```

After the above configuration, general Telnet users can use the **tftp get** command to download file bootrom.btm and other files from TFTP server 192.168.0.1 and other TFTP servers.

Saving Configurations

Some commands in the CLI of H3C switches are one-time commands, such as **display** commands, which display specified information, and the **reset** commands, which clear specified information. These commands are executed one-time only and are not saved when the switch reboots.

For other commands, after executing the commands, input the **save** command in any view to save all the submitted and executed commands into the configuration file, and thus all saved configurations are not lost when the switch reboot.

Table of Contents

1 Logging In to an Ethernet Switch	1-1
Logging In to an Ethernet Switch	1-1
Introduction to the User Interface	1-1
Supported User Interfaces	1-1
User Interface Index	1-2
Common User Interface Configuration	1-2
2 Logging In Through the Console Port	2-1
Introduction	2-1
Logging In Through the Console Port	2-1
Console Port Login Configuration	2-4
Common Configuration	2-4
Console Port Login Configurations for Different Authentication Modes	2-5
Console Port Login Configuration with Authentication Mode Being None	2-5
Configuration Procedure	2-5
Configuration Example	2-7
Console Port Login Configuration with Authentication Mode Being Password	2-8
Configuration Procedure	2-8
Configuration Example	2-9
Console Port Login Configuration with Authentication Mode Being Scheme	2-11
Configuration Procedure	2-11
Configuration Example	2-13
3 Logging In Through Telnet	3-1
Introduction	3-1
Common Configuration	3-2
Telnet Configurations for Different Authentication Modes	3-2
Telnet Configuration with Authentication Mode Being None	3-3
Configuration Procedure	3-3
Configuration Example	3-4
Telnet Configuration with Authentication Mode Being Password	3-5
Configuration Procedure	3-5
Configuration Example	3-6
Telnet Configuration with Authentication Mode Being Scheme	3-8
Configuration Procedure	3-8
Configuration Example	3-10
Telnetting to a Switch	3-11
Telnetting to a Switch from a Terminal	3-11
Telnetting to another Switch from the Current Switch	3-14
4 Logging In Using a Modem	4-1
Introduction	4-1
Configuration on the Switch Side	4-1
Modem Configuration	4-1
Switch Configuration	4-2

Modem Connection Establishment	4-2
5 Logging In Through the Web-based Network Management System.....	5-1
Introduction	5-1
Establishing an HTTP Connection	5-1
Configuring the Login Banner	5-2
Configuration Procedure.....	5-2
Configuration Example	5-3
Enabling/Disabling the WEB Server	5-3
6 Logging In Through NMS.....	6-1
Introduction	6-1
Connection Establishment Using NMS	6-1
7 Configuring Source IP Address for Telnet Service Packets	7-1
Overview	7-1
Configuring Source IP Address for Telnet Service Packets	7-1
Displaying Source IP Address Configuration	7-2
8 User Control	8-1
Introduction	8-1
Controlling Telnet Users	8-2
Prerequisites.....	8-2
Controlling Telnet Users by Source IP Addresses	8-2
Controlling Telnet Users by Source and Destination IP Addresses	8-2
Controlling Telnet Users by Source MAC Addresses	8-3
Configuration Example	8-3
Controlling Network Management Users by Source IP Addresses	8-4
Prerequisites.....	8-4
Controlling Network Management Users by Source IP Addresses.....	8-4
Configuration Example	8-5
Controlling Web Users by Source IP Address	8-6
Prerequisites.....	8-6
Controlling Web Users by Source IP Addresses.....	8-6
Disconnecting a Web User by Force.....	8-6
Configuration Example	8-7
9 Switching User Level.....	9-1
Overview	9-1
Specifying the authentication mode for user level switching	9-1
Adopting super password authentication for user level switching.....	9-2
Adopting HWTACACS authentication for user level switching.....	9-3
Switching to a specific user level	9-4
Configuration examples	9-4
Super password authentication configuration example.....	9-4
HWTACACS authentication configuration example	9-5

1 Logging In to an Ethernet Switch

Go to these sections for information you are interested in:

- [Logging In to an Ethernet Switch](#)
- [Introduction to the User Interface](#)
- [User Control](#)
- [Switching User Level](#)



Note

- A new configuration is added which specifies whether the copyright information is to be displayed when a user logs in through Telnet. See [Common User Interface Configuration](#).
 - Another new configuration is added which allows the banner to be displayed when a user logs in through Web. See [Configuring the Login Banner](#).
-

Logging In to an Ethernet Switch

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

- Logging in locally through the console port
- Logging in locally or remotely through an Ethernet port by means of Telnet or SSH
- Telnetting to the console port using a modem
- Logging in to the Web-based network management system
- Logging in through NMS (network management station)

Introduction to the User Interface

Supported User Interfaces



Note

The auxiliary (AUX) port and the console port of an H3C low-end and mid-range Ethernet switch are the same port (referred to as console port in the following part). You will be in the AUX user interface if you log in through this port.

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

- AUX user interface: A view when you log in through the AUX port. AUX port is a line device port.

- Virtual type terminal (VTY) user interface: A view when you log in through VTY. VTY port is a logical terminal line used when you access the device by means of Telnet or SSH.

Table 1-1 Description on user interface

User interface	Applicable user	Port used	Remarks
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.

User Interface Index

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:
 - The absolute AUX user interfaces are numbered 0 through 7.
 - VTY user interface indexes follow AUX user interface indexes. The first absolute VTY user interface is numbered 8, the second is 9, and so on.
- 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 interfaces are numbered from AUX0 to AUX7.
 - VTY user interfaces are numbered VTY0, VTY1, and so on.



Note

S3600 series Ethernet switches support Fabric. A Fabric can contain up to eight devices. Accordingly, the AUX user interfaces in a Fabric can be numbered from AUX0 to AUX7, through which all the console ports of the units in a Fabric can be identified. Refer to the *IRF Fabric* part for information about Fabric.

Common User Interface Configuration

Follow these steps to configure common user interface:

To do...	Use the command...	Remarks
Lock the current user interface	lock	Optional Available 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 Available in user view

To do...	Use the command...	Remarks
Free a user interface	free user-interface [<i>type</i>] <i>number</i>	Optional Available in user view
Enter system view	system-view	—
Set the banner	header [incoming legal login shell] <i>text</i>	Optional By default, no banner is configured
Set a system name for the switch	sysname <i>string</i>	Optional By default, the system name is H3C .
Enable copyright information displaying	copyright-info enable	Optional By default, copyright displaying is enabled. That is, the copy right information is displayed on the terminal after a user logs in successfully.
Enter user interface view	user-interface [<i>type</i>] <i>first-number</i> [<i>last-number</i>]	—
Display the information about the current user interface/all user interfaces	display users [all]	Optional Available in any view.
Display the physical attributes and configuration of the current/a specified user interface	display user-interface [<i>type number</i> <i>number</i>]	
Display the information about the current web users	display web users	

2 Logging In Through the Console Port

Go to these sections for information you are interested in:

- [Introduction](#)
- [Logging In Through the Console Port](#)
- [Console Port Login Configuration](#)
- [Console Port Login Configuration with Authentication Mode Being None](#)
- [Console Port Login Configuration with Authentication Mode Being Password](#)
- [Console Port Login Configuration with Authentication Mode Being Scheme](#)

Introduction

To log in through the console port is the most common way to log in to a switch. It is also the prerequisite to configure other login methods. By default, you can locally log in to an S3600 Ethernet switch through its console port only.

[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

To log in to a switch through the console port, make sure the settings of both the console port and the user terminal are the same.

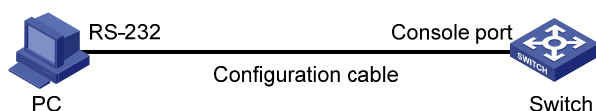
After logging in to a switch, you can perform configuration for AUX users. Refer to [Console Port Login Configuration](#) for more.

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 connecting to the console port of a switch



- 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/Windows 2000/Windows XP. The following assumes that you are running Windows XP) and perform the configuration shown in [Figure 2-2](#) through [Figure 2-4](#) for the connection to be created. Normally, both sides (that is, the serial port of the PC and the console port of the switch) are configured as those listed in [Table 2-1](#).

Figure 2-2 Create a connection

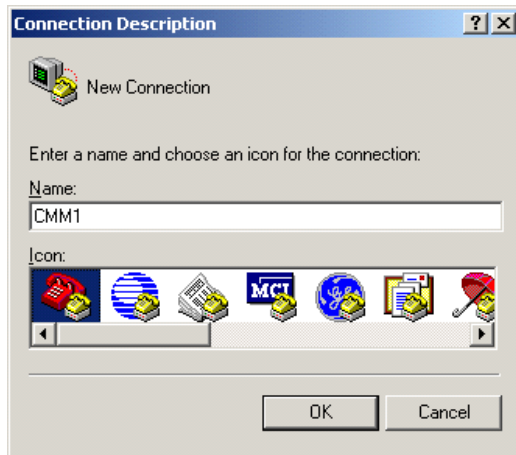
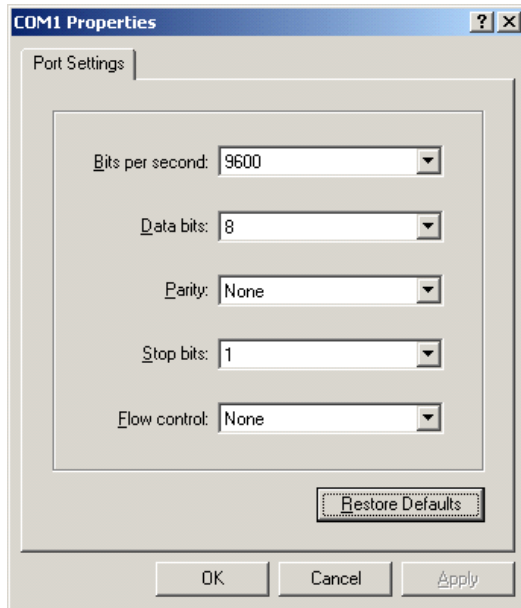


Figure 2-3 Specify the port used to establish the connection

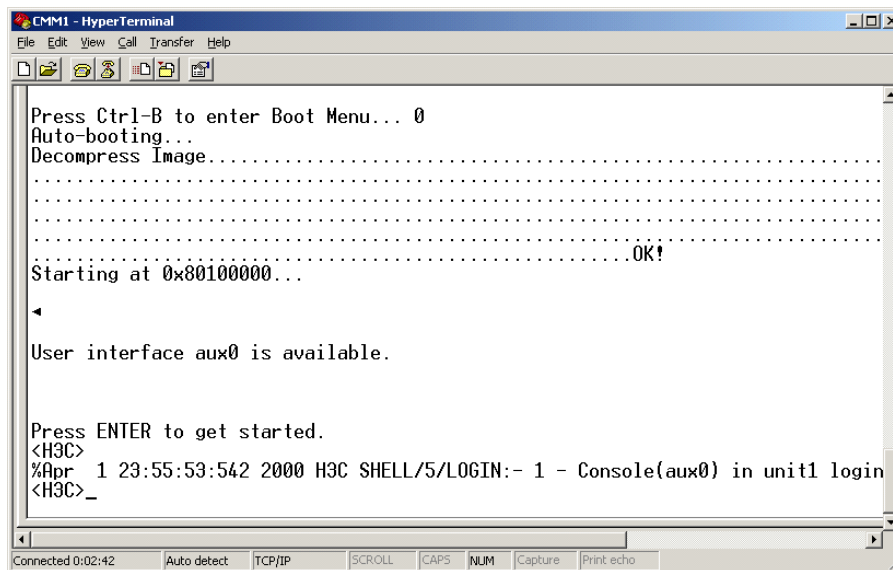


Figure 2-4 Set port parameters



- 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, as shown in [Figure 2-5](#).

Figure 2-5 HyperTerminal CLI



- 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. Refer to related parts in this manual for information about the commands used for configuring the switch.

Console Port Login Configuration

Common Configuration

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 in to the AUX user interface	Optional By default, commands of level 3 are available to the users logging in to 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

The change to console port configuration takes effect immediately, so the connection may be disconnected when you log in through a console port and then configure this console port. To configure a console port, you are recommended to log in to the switch in other ways. To log in to a switch through its console port after you modify the console port settings, you need to modify the corresponding settings of the terminal emulation utility running on your PC accordingly in the dialog box shown in [Figure 2-4](#).

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 Table 2-2 .
Password	Configure the password	Configure the password for local authentication	Required
	Perform common configuration	Perform common configuration for console port login	Optional Refer to Table 2-2 .
Scheme	Specify to perform local authentication or remote RADIUS authentication	AAA configuration specifies whether to perform local authentication or RADIUS authentication	Optional Local authentication is performed by default. Refer to the AAA part 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 Table 2-2 .



Note

Changes made to the authentication mode for console port login takes effect after you quit the command-line interface and then log in again.

Console Port Login Configuration with Authentication Mode Being None

Configuration Procedure

Follow these steps to configure console port login with the authentication mode being none:

To do...		Use the command...	Remarks
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 (AUX user interface) are not authenticated.
Configure the console port	Set the baud rate	speed <i>speed-value</i>	Optional The default baud rate of a 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 none , that is, no check is performed.
	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 in to the user interface		user privilege level <i>level</i>	Optional By default, commands of level 3 are available to users logging in to the AUX user interface, and commands of level 0 are available to users logging in to the VTY user interface.
Enable terminal services		shell	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain		screen-length <i>screen-length</i>	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 <i>value</i>	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.

To do...	Use the command...	Remarks
Set the timeout time for the user interface	idle-timeout <i>minutes</i> [<i>seconds</i>]	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.

Configuration Example

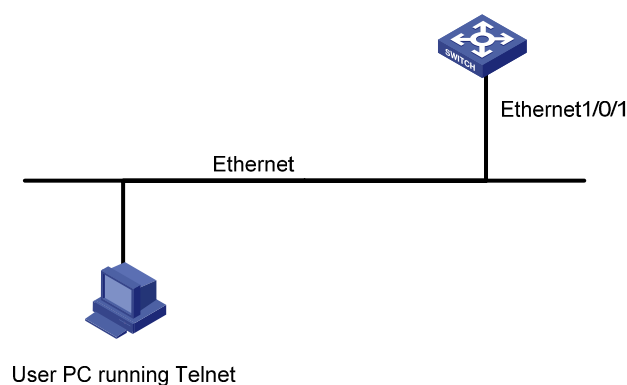
Network requirements

Assume that the switch is configured to allow users to log in through Telnet, and the current user level is set to the administrator level (level 3). Perform the following configurations for users logging in through the console port (AUX user interface).

- Do not authenticate the users.
- Commands of level 2 are available to the users logging in to 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.

Network diagram

Figure 2-6 Network diagram for AUX user interface configuration (with the authentication mode being none)



Configuration procedure

```

# Enter system view.
<Sysname> system-view

# Enter AUX user interface view.
[Sysname] user-interface aux 0
  
```

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

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

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

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

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

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

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

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

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

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

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

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

After the above configuration, you need to modify the configuration of the terminal emulation utility running on the PC accordingly in the dialog box shown in [Figure 2-4](#) to log in to the switch successfully.

Console Port Login Configuration with Authentication Mode Being Password

Configuration Procedure

Follow these steps to configure console port login with the authentication mode being password:

To do...	Use the command...	Remarks
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 in to 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

To do...		Use the command...	Remarks
Configure the console port	Set the baud rate	speed <i>speed-value</i>	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 in to the user interface		user privilege level <i>level</i>	Optional By default, commands of level 3 are available to users logging in to the AUX user interface.
Make terminal services available to the user interface		shell	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain		screen-length <i>screen-length</i>	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 <i>value</i>	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 <i>minutes</i> [<i>seconds</i>]	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.

Configuration Example

Network requirements

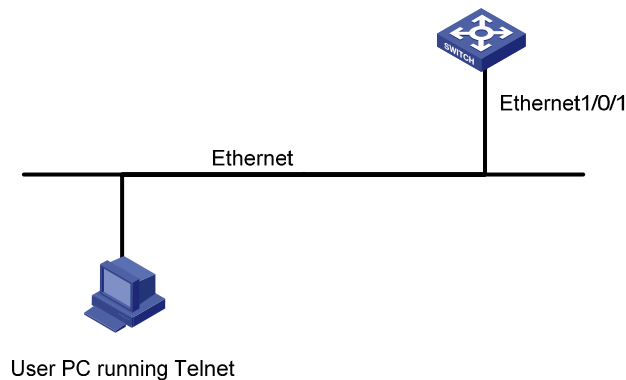
Assume the switch is configured to allow users to log in through Telnet, and the user level is set to the administrator level (level 3). Perform the following configurations for users logging in through the console port (AUX user interface).

- Authenticate the users using passwords.

- Set the local password to 123456 (in plain text).
- The commands of level 2 are available to the users.
- 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.

Network diagram

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



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

Enter AUX user interface view.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

After the above configuration, you need to modify the configuration of the terminal emulation utility running on the PC accordingly in the dialog box shown in [Figure 2-4](#) to log in to the switch successfully.

Console Port Login Configuration with Authentication Mode Being Scheme

Configuration Procedure

Follow these steps to configure console port login with the authentication mode being scheme:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Configure the authentication mode	Enter the default ISP domain view	domain <i>domain-name</i>	Optional By default, the local AAA scheme is applied.
	Specify the AAA scheme to be applied to the domain	scheme { local none radius-scheme <i>radius-scheme-name</i> [local] hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] }	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 <i>radius-scheme-name</i> argument, you need to perform the following configuration as well:
	Quit to system view	quit	Perform AAA&RADIUS configuration on the switch. (Refer to the AAA part for more.) Configure the user name and password accordingly on the AAA server. (Refer to the user manual of AAA server.)
Create a local user (Enter local user view.)		local-user <i>user-name</i>	Required No local user exists by default.
Set the authentication password for the local user		password { simple cipher } <i>password</i>	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. By default, users logging in through the console port (AUX user interface) are not authenticated.

To do...		Use the command...	Remarks
Configure the console port	Set the baud rate	speed <i>speed-value</i>	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 in to the user interface		user privilege level <i>level</i>	Optional By default, commands of level 3 are available to users logging in to the AUX user interface.
Make terminal services available to the user interface		shell	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain		screen-length <i>screen-length</i>	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 <i>value</i>	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 <i>minutes</i> [<i>seconds</i>]	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 in to a switch depends on the command level specified in the **service-type terminal** [**level** *level*] command.

Configuration Example

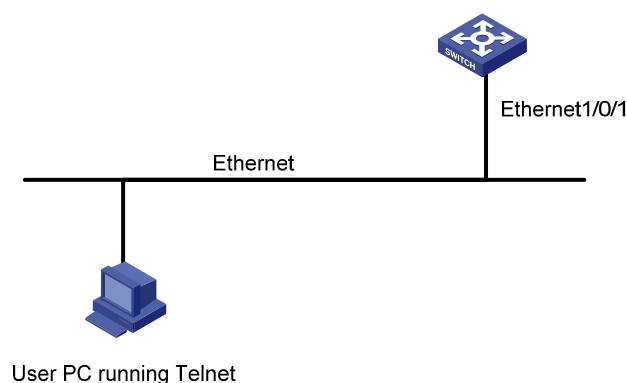
Network requirements

Assume the switch is configured to allow users to log in through Telnet, and the user level is set to the administrator level (level 3). Perform the following configurations for users logging in through the console port (AUX user interface).

- Configure the local user name as **guest**.
- Set the authentication password of the local user to **123456** (in plain text).
- Set the service type of the local user to Terminal and the command level to 2.
- Configure to authenticate the users in the scheme mode.
- 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.

Network diagram

Figure 2-8 Network diagram for AUX user interface configuration (with the authentication mode being scheme)



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

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

```
[Sysname] local-user guest
```

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

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

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

```
[Sysname-luser-guest] service-type terminal level 2
```

```
[Sysname-luser-guest] quit
```

Enter AUX user interface view.

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

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

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

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

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

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

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

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

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

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

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

After the above configuration, you need to modify the configuration of the terminal emulation utility running on the PC accordingly in the dialog box shown in [Figure 2-4](#) to log in to the switch successfully.

3 Logging In Through Telnet

Go to these sections for information you are interested in:

- [Introduction](#)
- [Telnet Configuration with Authentication Mode Being None](#)
- [Telnet Configuration with Authentication Mode Being Password](#)

Introduction

S3600 series Ethernet switches support Telnet. You can manage and maintain a switch remotely by Telnetting to the switch.

To log in to a switch through Telnet, the corresponding configuration is required on both the switch and the Telnet terminal.

You can also log in to a switch through SSH. SSH is a secure shell added to Telnet. Refer to the *SSH Operation* for related information.

Table 3-1 Requirements for Telnetting to a switch

Item	Requirement
Switch	The IP address is configured for the VLAN of the switch, and the route between the switch and the Telnet terminal is reachable. (Refer to the <i>IP Address Configuration – IP Performance Configuration and Routing Protocol</i> parts 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 VLAN interface of the switch is available.



Note

Telnetting to a switch using IPv6 protocols is similar to Telnetting to a switch using IPv4 protocols. Refer to the *IPv6 Management* part for related information.

Common Configuration

Table 3-2 Common Telnet configuration

Configuration		Description
VTY user interface configuration	Configure the command level available to users logging in to the VTY user interface	Optional By default, commands of level 0 are available to users logging in to a VTY user interface.
	Configure the protocols the user interface supports	Optional By default, Telnet and SSH protocol are supported.
	Set the commands to be executed automatically after a user log in to the user interface successfully	Optional By default, no command is executed automatically after a user logs into the VTY user interface.
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.

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 remote RADIUS authentication	AAA configuration specifies whether to perform local authentication or RADIUS authentication	Optional Local authentication is performed by default. Refer to the AAA part 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 RADIUS 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 prevent attacks 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.

Telnet Configuration with Authentication Mode Being None

Configuration Procedure

Follow these steps to configure Telnet with the authentication mode being none:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter one or more VTY user interface views	user-interface vty <i>first-number [last-number]</i>	—
Configure not to authenticate users logging in to VTY user interfaces	authentication-mode none	Required By default, VTY users are authenticated after logging in.

To do...	Use the command...	Remarks
Configure the command level available to users logging in to VTY user interface	user privilege level <i>level</i>	Optional By default, commands of level 0 are available to users logging in to 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.
Set the commands to be executed automatically after a user login to the user interface successfully	auto-execute command <i>text</i>	Optional By default, no command is executed automatically after a user logs into the VTY 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 <i>screen-length</i>	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 <i>value</i>	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 of the VTY user interface	idle-timeout <i>minutes</i> [<i>seconds</i>]	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 in to a switch depends on the **user privilege level** *level* command

Configuration Example

Network requirements

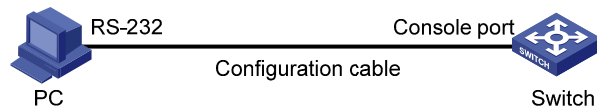
Assume current user logs in through the console port, and the current user level is set to the administrator level (level 3). Perform the following configurations for users logging in through VTY 0 using Telnet.

- Do not authenticate the users.
- Commands of level 2 are available to the users.

- 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.

Network diagram

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



Configuration procedure

```

# Enter system view.
<Sysname> system-view

# Enter VTY 0 user interface view.
[Sysname] user-interface vty 0

# Configure not to authenticate Telnet users logging in to VTY 0.
[Sysname-ui-vty0] authentication-mode none

# Specify commands of level 2 are available to users logging in to VTY 0.
[Sysname-ui-vty0] user privilege level 2

# Configure Telnet protocol is supported.
[Sysname-ui-vty0] protocol inbound telnet

# Set the maximum number of lines the screen can contain to 30.
[Sysname-ui-vty0] screen-length 30

# Set the maximum number of commands the history command buffer can store to 20.
[Sysname-ui-vty0] history-command max-size 20

# Set the timeout time to 6 minutes.
[Sysname-ui-vty0] idle-timeout 6
  
```

Telnet Configuration with Authentication Mode Being Password

Configuration Procedure

Follow these steps to configure Telnet with the authentication mode being password:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter one or more VTY user interface views	user-interface vty <i>first-number [last-number]</i>	—
Configure to authenticate users logging in to VTY user interfaces using the local password	authentication-mode password	Required

To do...	Use the command...	Remarks
Set the local password	set authentication password { cipher simple } <i>password</i>	Required
Configure the command level available to users logging in to the user interface	user privilege level <i>level</i>	Optional By default, commands of level 0 are available to users logging in to 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.
Set the commands to be executed automatically after a user login to the user interface successfully	auto-execute command <i>text</i>	Optional By default, no command is executed automatically after a user logs into the 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 <i>screen-length</i>	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 <i>value</i>	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 of the user interface	idle-timeout <i>minutes</i> [<i>seconds</i>]	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.

When the authentication mode is password, the command level available to users logging in to the user interface is determined by the **user privilege level** command.

Configuration Example

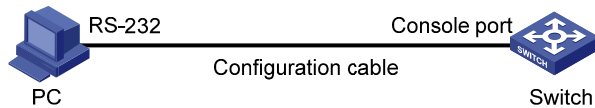
Network requirements

Assume current user logs in through the console port and the current user level is set to the administrator level (level 3). Perform the following configurations for users logging in to VTY 0 using Telnet.

- Authenticate users using the local password.
- Set the local password to 123456 (in plain text).
- Commands of level 2 are available to the users.
- 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.

Network diagram

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



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

Enter VTY 0 user interface view.

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

Configure to authenticate users logging in to VTY 0 using the password.

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

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

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

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

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

Configure Telnet protocol is supported.

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

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

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

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

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

Set the timeout time to 6 minutes.

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

Telnet Configuration with Authentication Mode Being Scheme

Configuration Procedure

Follow these steps to configure Telnet with the authentication mode being scheme:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Configure the authentication scheme	Enter the default ISP domain view	domain <i>domain-name</i>	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 <i>radius-scheme-name</i> argument, you need to perform the following configuration as well: Perform AAA&RADIUS configuration on the switch. (Refer to the AAA part for more.) Configure the user name and password accordingly on the AAA server. (Refer to the user manual of AAA server.)
	Configure the AAA scheme to be applied to the domain	scheme { local none radius-scheme <i>radius-scheme-name</i> [local] hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] }	
	Quit to system view	quit	
Create a local user and enter local user view		local-user <i>user-name</i>	No local user exists by default.
Set the authentication password for the local user		password { simple cipher } <i>password</i>	Required
Specify the service type for VTY users		service-type telnet [level <i>level</i>]	Required
Quit to system view		quit	—
Enter one or more VTY user interface views		user-interface vty <i>first-number</i> [last-number]	—
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 in to the user interface		user privilege level <i>level</i>	Optional By default, commands of level 0 are available to users logging in to 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.

To do...	Use the command...	Remarks
Set the maximum number of lines the screen can contain	screen-length <i>screen-length</i>	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 <i>value</i>	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 <i>minutes</i> [<i>seconds</i>]	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 the users logging in to the switch depends on the **user privilege level** *level* command and the **service-type** { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** }* [**level** *level*] command, as listed in [Table 3-4](#).

Table 3-4 Determine the command level when users logging in to switches are authenticated in the scheme mode

Scenario			Command level
Authentication mode	User type	Command	
authentication-mode scheme [command-auth orization]	VTY users that are AAA&RADIUS authenticated or locally authenticated	The user privilege level <i>level</i> command is not executed, and the service-type command does not specify the available command level.	Level 0
		The user privilege level <i>level</i> command is not executed, and the service-type command specifies the available command level.	Determined by the service-type command
		The user privilege level <i>level</i> command is executed, and the service-type command does not specify the available command level.	Level 0
		The user privilege level <i>level</i> command is executed, and the service-type command specifies the available command level.	Determined by the service-type command

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



Note

Refer to *AAA Operation* and *SSH Operation* of this manual for information about AAA, RADIUS, and SSH.

Configuration Example

Network requirements

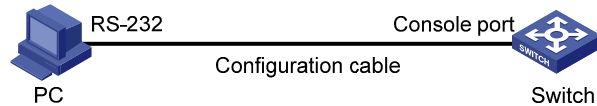
Assume current user logs in through the console port and the user level is set to the administrator level (level 3). Perform the following configurations for users logging in to VTY 0 using Telnet.

- Configure the local user name as **guest**.
- Set the authentication password of the local user to **123456** (in plain text).

- Set the service type of VTY users to Telnet and the command level to 2.
- Configure to authenticate users logging in to VTY 0 in scheme mode.
- 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.

Network diagram

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



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

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

```
[Sysname] local-user guest
```

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

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

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

```
[Sysname-luser-guest] service-type telnet level 2
```

```
[Sysname-luser-guest] quit
```

Enter VTY 0 user interface view.

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

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

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

Configure Telnet protocol is supported.

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

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

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

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

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

Set the timeout time to 6 minutes.

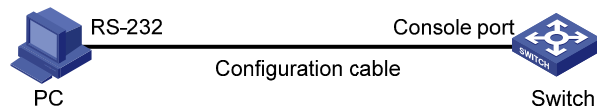
```
[Sysname-ui-vty0] idle-timeout 6
```

Telnetting to a Switch

Telnetting to a Switch from a Terminal

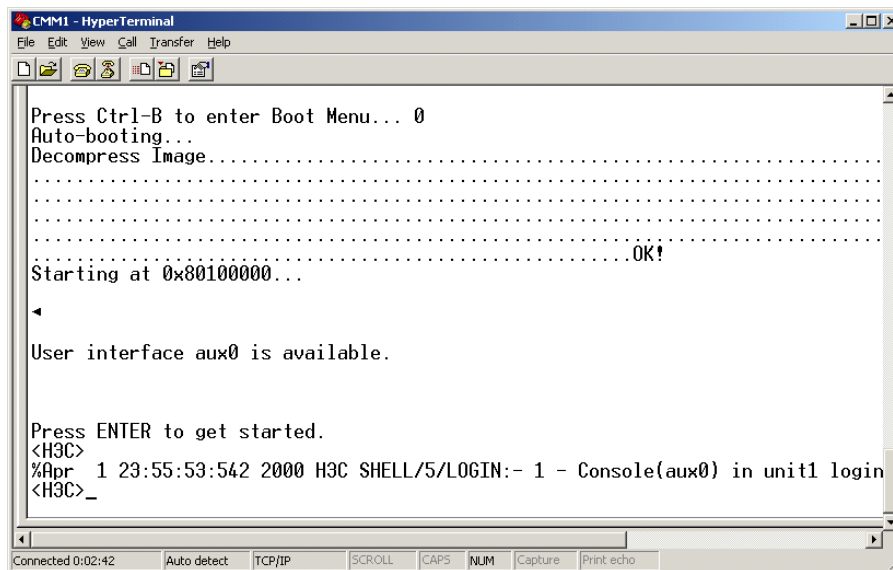
- 1) Assign an IP address to VLAN-interface 1 of the switch (VLAN 1 is the default VLAN of the switch).
- Connect the serial port of your PC/terminal to the console port of the switch, as shown in [Figure 3-4](#)

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



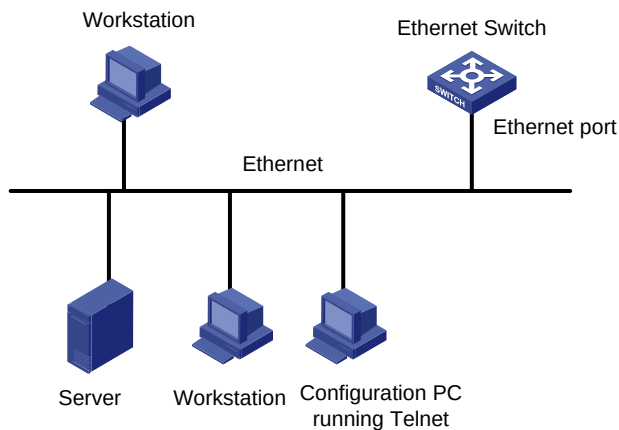
- Launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 95/Windows 98/Windows NT/Windows 2000/Windows XP) on the PC terminal, with the baud rate set to 9,600 bps, data bits set to 8, parity check set to none, and flow control set to none.
- Turn on the switch and press Enter as prompted. The prompt (such as <H3C>) appears, as shown in the following figure.

Figure 3-5 The terminal window



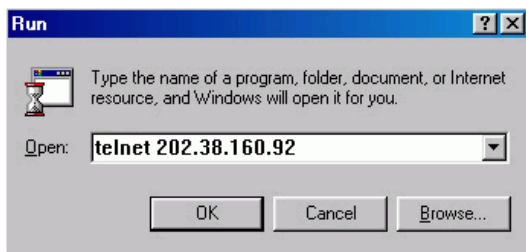
- Perform the following operations in the terminal window to assign IP address 202.38.160.92/24 to VLAN-interface 1 of the switch.
<Sysname> system-view
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ip address 202.38.160.92 255.255.255.0
- 2) Perform Telnet-related configuration on the switch. Refer to [Telnet Configuration with Authentication Mode Being None](#), [Telnet Configuration with Authentication Mode Being Password](#), and [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 VLAN 1 and the route between your PC and VLAN-interface 1 is reachable.

Figure 3-6 Network diagram for Telnet connection establishment



- 4) Launch Telnet on your PC, with the IP address of VLAN-interface 1 of the switch as the parameter, as shown in [Figure 3-7](#).

Figure 3-7 Launch Telnet



- 5) If the password authentication mode is specified, enter the password when the Telnet window displays “Login authentication” and prompts for login password. The CLI prompt (such as <Sysname>) 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 Telnetting 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 relevant parts in this manual 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 the CLI part for information about command hierarchy.

Telnetting 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 Telnetting 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 Telnetting to another switch from the current switch



- 2) Perform Telnet-related configuration on the switch operating as the Telnet server. Refer to [Telnet Configuration with Authentication Mode Being None](#), [Telnet Configuration with Authentication Mode Being Password](#), and [Telnet Configuration with Authentication Mode Being Scheme](#) for more.
- 3) Telnet to the switch operating as the Telnet client.
- 4) Execute the following command on the switch operating as the Telnet client:
`<Sysname> telnet xxxx`

Note that 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.

- 5) After successful login, the CLI prompt (such as <Sysname>) appears. If all the 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!”.
- 6) After successfully Telnetting 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.

4 Logging In Using a Modem

Go to these sections for information you are interested in:

- [Introduction](#)
- [Configuration on the Switch Side](#)
- [Modem Connection Establishment](#)

Introduction

The administrator can log in to the console port of a remote switch using a modem through public switched telephone network (PSTN) 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 manage switches in the network remotely in this way.

To log in to 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 in to 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 .

Configuration on the Switch Side

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 configuration commands and the output of different modems may differ. Refer to the user manual of the modem when performing the above configuration.

Switch Configuration



Note

After logging in to 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 in to 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.

Configuration on switch when the authentication mode is none

Refer to [Console Port Login Configuration with Authentication Mode Being None](#).

Configuration on switch when the authentication mode is password

Refer to [Console Port Login Configuration with Authentication Mode Being Password](#).

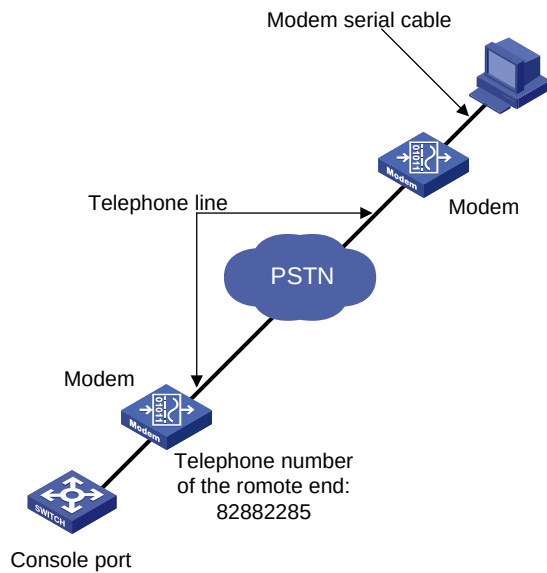
Configuration on switch when the authentication mode is scheme

Refer to [Console Port Login Configuration with Authentication Mode Being Scheme](#).

Modem Connection Establishment

- 1) Before using Modem to log in the switch, perform corresponding configuration for different authentication modes on the switch. Refer to [Console Port Login Configuration with Authentication Mode Being None](#), [Console Port Login Configuration with Authentication Mode Being Password](#), and [Console Port Login Configuration with Authentication Mode Being Scheme](#) for more.
- 2) Perform the following configuration to the modem directly connected to the switch. Refer to [Modem Configuration](#) for related configuration.
- 3) Connect your PC, the modems, and the switch, as shown in [Figure 4-1](#). Make sure the modems are properly connected to telephone lines.

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](#) through [Figure 4-4](#). Note that you need to set the telephone number to that of the modem directly connected to the switch.

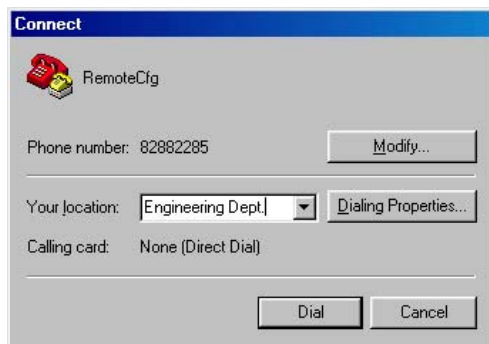
Figure 4-2 Create a connection



Figure 4-3 Set the telephone number



Figure 4-4 Call the modem



- 5) If the password authentication mode is specified, enter the password when prompted. If the password is correct, the prompt (such as <Sysname>) appears. You can then configure or manage the switch. You can also enter the character ? at anytime for help. Refer to the related parts in this manual 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 part for information about command level.

5 Logging In Through the Web-based Network Management System

Go to these sections for information you are interested in:

- [Introduction](#)
- [Establishing an HTTP Connection](#)
- [Configuring the Login Banner](#)
- [Enabling/Disabling the WEB Server](#)

Introduction

An S3600 Ethernet switch has a Web server built in. It enables you to log in to an S3600 Ethernet switch through a Web browser and then manage and maintain the switch intuitively by interacting with the built-in Web server.

To log in to 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 in to a switch through the Web-based network management system

Item	Requirement
Switch	The VLAN interface of the switch is assigned an IP address, and the route between the switch and the Web network management terminal is reachable. (Refer to the <i>IP Address Configuration – IP Performance Configuration and Routing Protocol</i> parts for related information.)
	The user name and password for logging in to the Web-based network management system are configured.
PC operating as the network management terminal	IE is available.
	The IP address of the VLAN interface of the switch, the user name, and the password are available.

Establishing an HTTP Connection

- 1) Assign an IP address to VLAN-interface 1 of the switch (VLAN 1 is the default VLAN of the switch). See [Telnetting to a Switch from a Terminal](#) for related information.
- 2) Configure the user name and the password on the switch for the Web network management user to log in.

Create a Web user account, setting both the user name and the password to **admin** and the user level to 3.

```
<Sysname> system-view
[Sysname] local-user admin
```

```
[Sysname-luser-admin] service-type telnet level 3
[Sysname-luser-admin] password simple admin
```

- 3) Establish an HTTP connection between your PC and the switch, as shown in [Figure 5-1](#).

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



- 4) Log in to 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 in the address bar. (Make sure the route between the Web-based network management terminal and the switch is available.)
- 5) When the login authentication 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

The screenshot shows a web browser window with the title 'Web user login'. It contains three input fields: 'User Name', 'Password', and 'Language' (a dropdown menu with 'English' selected). Below these fields is a 'Login' button.

Configuring the Login Banner

Configuration Procedure

If a login banner is configured with the **header** command, when a user logs in through Web, the banner page is displayed before the user login authentication page. The contents of the banner page are the login banner information configured with the **header** command. Then, by clicking <Continue> on the banner page, the user can enter the user login authentication page, and enter the main page of the Web-based network management system after passing the authentication. If no login banner is configured by the **header** command, a user logging in through Web directly enters the user login authentication page.

Follow these steps to configure the login banner:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the banner to be displayed when a user logs in through Web	header login text	Required By default, no login banner is configured.

Configuration Example

Network requirements

- A user logs in to the switch through Web.
- The banner page is desired when a user logs into the switch.

Network diagram

Figure 5-3 Network diagram for login banner configuration



Configuration Procedure

Enter system view.

```
<Sysname> system-view
```

Configure the banner **Welcome** to be displayed when a user logs into the switch through Web.

```
[Sysname] header login %Welcome%
```

Assume that a route is available between the user terminal (the PC) and the switch. After the above-mentioned configuration, if you enter the IP address of the switch in the address bar of the browser running on the user terminal and press <Enter>, the browser will display the banner page, as shown in [Figure 5-4](#).

Figure 5-4 Banner page displayed when a user logs in to the switch through Web



Click <Continue> to enter user login authentication page. You will enter the main page of the Web-based network management system if the authentication succeeds.

Enabling/Disabling the WEB Server

Follow these steps to enable/Disable the WEB Server:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the Web server	ip http shutdown	Required By default, the Web server is enabled.
Disable the Web server	undo ip http shutdown	Required



Note

To improve security and prevent attack to the unused Sockets, TCP 80 port (which is for HTTP service) is enabled/disabled after the corresponding configuration.

- Enabling the Web server (by using the **undo ip http shutdown** command) opens TCP 80 port.
- Disabling the Web server (by using the **ip http shutdown** command) closes TCP 80 port.

6 Logging In Through NMS

Go to these sections for information you are interested in:

- [Introduction](#)
- [Connection Establishment Using NMS](#)

Introduction

You can also log in to a switch through a network management station (NMS), and then configure and manage the switch through the agent module on the switch. Simple network management protocol (SNMP) is applied between the NMS and the agent. Refer to the *SNMP-RMON* part for related information.

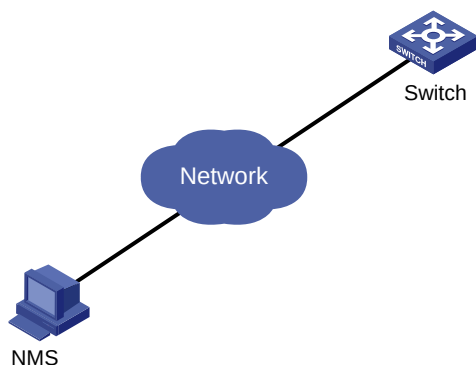
To log in to a switch through an NMS, you need to perform related configuration on both the NMS and the switch.

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

Item	Requirement
Switch	The IP address of the VLAN interface of the switch is configured. The route between the NMS and the switch is reachable. (Refer to the <i>IP Address Configuration – IP Performance Configuration and Routing Protocol</i> parts for related information.)
	The basic SNMP functions are configured. (Refer to the <i>SNMP-RMON</i> part for related information.)
NMS	The NMS is properly configured. (Refer to the user manual of your NMS for related information.)

Connection Establishment Using NMS

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



7 Configuring Source IP Address for Telnet Service Packets

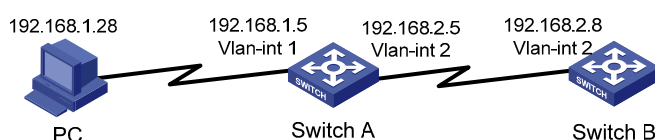
Go to these sections for information you are interested in:

- [Overview](#)
- [Configuring Source IP Address for Telnet Service Packets](#)
- [Displaying Source IP Address Configuration](#)

Overview

You can configure the source IP address for Telnet service packets for an S3600 switch operating as a Telnet client. The IP address can only be the IP address of a Layer 3 interface on the switch.

Figure 7-1 Specify source IP address for Telnet service packets



As shown in [Figure 7-1](#), suppose you are going to telnet to Switch B from PC. If devices in the segment 192.168.1.0/24 are not allowed to telnet to Switch B, you can log in to Switch A (an S3600 Ethernet switch) first, configure the source IP address of the Telnet service packets on Switch A as 192.168.2.5, and then log in to Switch B through Switch A.

Configuring Source IP Address for Telnet Service Packets

The feature of configuring source IP address for Telnet service packets can be configured in either user view or system view.

The configuration performed in user view takes effect for only the current session

The configuration performed in system view takes effect for all the following sessions. That is, when a switch telnets to a remote device, it automatically uses the configured source IP address or source interface to encapsulate Telnet service packets.

Use the following commands to configure a source IP address or source interface for Telnet service packets:

To do...	Use the command...	Remarks
Specify a source IP address or source interface for Telnet service packets for an S3600 switch serving as a Telnet client	telnet { <i>hostname</i> <i>ip-address</i> } [<i>service-port</i>] { source-ip <i>ip-address</i> source-interface <i>interface-type interface-number</i> }	Required Use either approach
	system-view	
	telnet { source-ip <i>ip-address</i> source-interface <i>interface-type interface-number</i> }	



Note

- The IP address specified is that of a Layer 3 interface of the local device. Otherwise, the system prompts configuration failure.
- The source interface specified must exist. Otherwise, the system prompts configuration failure.
- Configuring the source interface of Telnet service packets equals configuring the IP address of this interface as the source IP address of the Telnet service packets.
- If a source IP address (or source interface) is specified, you need to make sure that the route between the IP addresses (or interface) and the Telnet server is reachable.

Displaying Source IP Address Configuration

To do...	Use the command...	Remarks
Display the source IP address configured for the Telnet service packets	display telnet source-ip	Available in any view

8 User Control

Go to these sections for information you are interested in:

- [Introduction](#)
- [Controlling Telnet Users](#)
- [Controlling Network Management Users by Source IP Addresses](#)
- [Controlling Web Users by Source IP Address](#)



Note

Refer to the *ACL* part for information about ACL.

Introduction

You can control users logging in through Telnet, SNMP and WEB by defining Access Control List (ACL), 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	Controlling Telnet Users by Source IP Addresses
	By source and destination IP address	Through advanced ACL	Controlling Telnet Users by Source and Destination IP Addresses
	By source MAC address	Through Layer 2 ACL	Controlling Telnet Users by Source MAC Addresses
SNMP	By source IP addresses	Through basic ACL	Controlling Network Management Users by Source IP Addresses
WEB	By source IP addresses	Through basic ACL	Controlling Web Users by Source IP Address
	Disconnect Web users by force	By executing commands in CLI	Disconnecting a Web User by Force

Controlling Telnet Users

Prerequisites

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

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.

Follow these steps to control Telnet users by source IP addresses:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a basic ACL or enter basic ACL view	acl number <i>acl-number</i> [match-order { auto config }]	As for the acl number command, the config keyword is specified by default.
Define rules for the ACL	rule [<i>rule-id</i>] { deny permit } [<i>rule-string</i>]	Required
Quit to system view	quit	—
Enter user interface view	user-interface [<i>type</i>] <i>first-number</i> [<i>last-number</i>]	—
Apply the ACL to control Telnet users by source IP addresses	acl <i>acl-number</i> { 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.

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.

Follow these steps to control Telnet users by source and destination IP addresses:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create an advanced ACL or enter advanced ACL view	acl number <i>acl-number</i> [match-order { auto config }]	As for the acl number command, the config keyword is specified by default.
Define rules for the ACL	rule [<i>rule-id</i>] { deny permit } <i>protocol</i> [<i>rule-string</i>]	Required You can define rules as needed to filter by specific source and destination IP addresses.
Quit to system view	quit	—

To do...	Use the command...	Remarks
Enter user interface view	user-interface [<i>type</i>] <i>first-number</i> [<i>last-number</i>]	—
Apply the ACL to control Telnet users by specified source and destination IP addresses	acl <i>acl-number</i> { 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.

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.

Follow these steps to control Telnet users by source MAC addresses:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create or enter Layer 2 ACL view	acl number <i>acl-number</i>	—
Define rules for the ACL	rule [<i>rule-id</i>] { deny permit } [<i>rule-string</i>]	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 [<i>type</i>] <i>first-number</i> [<i>last-number</i>]	—
Apply the ACL to control Telnet users by specified source MAC addresses	acl <i>acl-number</i> inbound	Required By default, no ACL is applied for Telnet users.

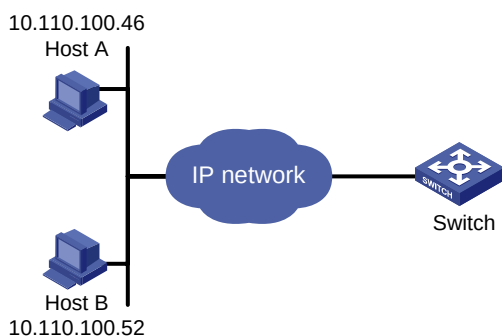
Configuration Example

Network requirements

Only the Telnet users sourced from the IP address of 10.110.100.52 are permitted to access the switch.

Network diagram

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



Configuration procedure

Define a basic ACL.

```
<Sysname> system-view
```

```
[Sysname] acl number 2000
```

```
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
```

```
[Sysname-acl-basic-2000] quit
```

Apply the ACL.

```
[Sysname] user-interface vty 0 4
```

```
[Sysname-ui-vty0-4] acl 2000 inbound
```

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

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).

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.

Follow these steps to control network management users by source IP addresses:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a basic ACL or enter basic ACL view	acl number <i>acl-number</i> [match-order { auto config }]	As for the acl number command, the config keyword is specified by default.
Define rules for the ACL	rule [<i>rule-id</i>] { deny permit } [<i>rule-string</i>]	Required
Quit to system view	quit	—
Apply the ACL while configuring the SNMP community name	snmp-agent community { read write } <i>community-name</i> [acl <i>acl-number</i> mib-view <i>view-name</i>]*	Required According to the SNMP version and configuration customs of NMS users, you can reference an ACL when configuring community name, group name or username. For the detailed configuration, refer to <i>SNMP-RMON</i> for more.
Apply the ACL while configuring the SNMP group name	snmp-agent group { v1 v2c } <i>group-name</i> [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-number</i>] snmp-agent group v3 <i>group-name</i> [authentication privacy] [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-number</i>]	
Apply the ACL while configuring the SNMP user name	snmp-agent usm-user { v1 v2c } <i>user-name</i> <i>group-name</i> [acl <i>acl-number</i>] snmp-agent usm-user v3 <i>user-name</i> <i>group-name</i> [[cipher] authentication-mode { md5 sha } <i>auth-password</i> [privacy-mode { des56 aes128 } <i>priv-password</i>]] [acl <i>acl-number</i>]	

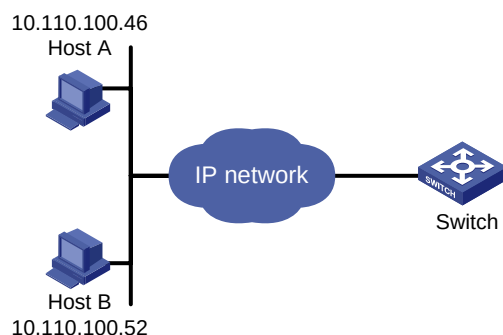
Configuration Example

Network requirements

Only SNMP users sourced from the IP addresses of 10.110.100.52 are permitted to log in to the switch.

Network diagram

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



Configuration procedure

Define a basic ACL.

```
<Sysname> system-view
```

```
[Sysname] acl number 2000
```

```
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
```

```
[Sysname-acl-basic-2000] quit
```

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

```
[Sysname] snmp-agent community read aaa acl 2000
```

```
[Sysname] snmp-agent group v2c groupa acl 2000
```

```
[Sysname] snmp-agent usm-user v2c usera groupa acl 2000
```

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

Prerequisites

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

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.

Follow these steps to control Web users by source IP addresses:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a basic ACL or enter basic ACL view	acl number <i>acl-number</i> [match-order { config auto }]	As for the acl number command, the config keyword is specified by default.
Define rules for the ACL	rule [<i>rule-id</i>] { deny permit } [<i>rule-string</i>]	Required
Quit to system view	quit	—
Apply the ACL to control Web users	ip http acl <i>acl-number</i>	Optional By default, no ACL is applied for Web users.

Disconnecting a Web User by Force

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

Follow these steps to disconnect a Web user by force:

To do...	Use the command...	Remarks
Disconnect a Web user by force	free web-users { all user-id <i>user-id</i> user-name <i>user-name</i> }	Required Available in user view

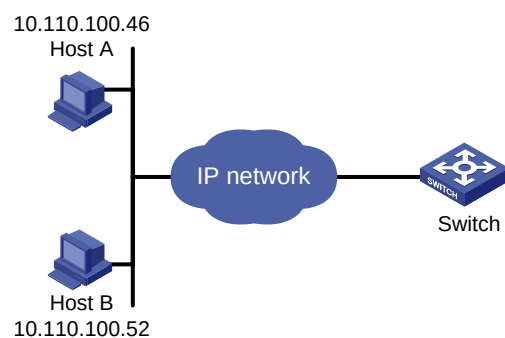
Configuration Example

Network requirements

Only the Web users sourced from the IP address of 10.110.100.52 are permitted to access the switch.

Network diagram

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



Configuration procedure

Define a basic ACL.

```
<Sysname> system-view
```

```
[Sysname] acl number 2030
```

```
[Sysname-acl-basic-2030] rule 1 permit source 10.110.100.52 0
```

```
[Sysname-acl-basic-2030] quit
```

Apply ACL 2030 to only permit the Web users sourced from the IP address of 10.110.100.52 to access the switch.

```
[Sysname] ip http acl 2030
```

9 Switching User Level

Overview

Users can switch their user privilege level temporarily without logging out and disconnecting the current connection; after the switch, users can continue to configure the device without the need of relogin and reauthentication, but the commands that they can execute have changed.

For example, if the current user privilege level is 3, the user can configure system parameters; after switching the user privilege level to 0, the user can only execute some simple commands, like **ping** and **tracert**, and only a few **display** commands.

The switching of user privilege level is temporary, and effective for the current login; after the user relogs in, the user privilege restores to the original level.

To avoid misoperations, the administrators are recommended to log in to the device by using a lower privilege level and view device operating parameters, and when they have to maintain the device, they can switch to a higher level temporarily; when the administrators need to leave for a while or ask someone else to manage the device temporarily, they can switch to a lower privilege level before they leave to restrict the operation by others.

The high-to-low user level switching is unlimited. However, the low-to-high user level switching requires the corresponding authentication. Generally, two authentication modes are available: the super password authentication mode and HWTACACS authentication mode.

Complete the following tasks to configure user level switching:

Task		Remarks
The administrator configures the user level switching authentication policies	Specifying the authentication mode for user level switching	Optional
	Adopting super password authentication for user level switching	Required
	Adopting HWTACACS authentication for user level switching	Required
The user switches user level after logging in	Switching to a specific user level	Required

Specifying the authentication mode for user level switching

The low-to-high user level switching requires the corresponding authentication. The super password authentication mode and HWTACACS authentication mode are available at the same time to provide authentication redundancy.

The configuration of authentication mode for user level switching is performed by Level-3 users (administrators).

Follow these steps to specify the authentication mode for user level switching:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enter user interface view		user-interface [<i>type</i>] <i>first-number</i> [<i>last-number</i>]	—
Specify the authentication mode for user level switching	Super password authentication	super authentication-mode super-password	Optional These configurations will take effect on the current user interface only. By default, super password authentication is adopted for user level switching.
	HWTACACS authentication	super authentication-mode scheme	
	Super password authentication preferred (with the HWTACACS authentication as the backup authentication mode)	super authentication-mode super-password scheme	
	HWTACACS authentication preferred (with the super password authentication as the backup authentication mode)	super authentication-mode scheme super-password	



Note

When both the super password authentication and the HWTACACS authentication are specified, the device adopts the preferred authentication mode first. If the preferred authentication mode cannot be implemented (for example, the super password is not configured or the HWTACACS authentication server is unreachable), the backup authentication mode is adopted.

Adopting super password authentication for user level switching

With the super password set, you can pass the super password authentication successfully only when you provide the super password as prompted. If no super password is set, the system prompts “%Password is not set” when you attempt to switch to a higher user level. In this case, you cannot pass the super password authentication.

For example, after the administrator configures the **super password level 3 simple 123** command, when users of level 0 through level 2 want to switch to user level 3, they need to input super password 123.

The following table lists the operations to configure super password authentication for user level switching, which can only be performed by level-3 users (administrators).

Follow these steps to set a password for use level switching:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the super password for user level switching	super password [<i>level level</i>] { cipher simple } <i>password</i>	Required The configuration will take effect on all user interfaces. By default, the super password is not set.



Note

The super password is for level switching only and is different from the login password..

Adopting HWTACACS authentication for user level switching

To implement HWTACACS authentication for user level switching, a level-3 user must perform the commands listed in the following table to configure the HWTACACS authentication scheme used for low-to-high user level switching. With HWTACACS authentication enabled, you can pass the HWTACACS authentication successfully only after you provide the right user name and the corresponding password as prompted. Note that if you have passed the HWTACACS authentication when logging in to the switch, only the password is required.

The following table lists the operations to configure HWTACACS authentication for user level switching, which can only be performed by Level-3 users.

Follow these steps to set the HWTACACS authentication scheme for user level switching:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter ISP domain view	domain <i>domain-name</i>	—
Set the HWTACACS authentication scheme for user level switching	authentication super hwtacacs-scheme <i>hwtacacs-scheme-name</i>	Required By default, the HWTACACS authentication scheme for user level switching is not set.



Note

When setting the HWTACACS authentication scheme for user level switching using the **authentication super hwtacacs-scheme** command, make sure the HWTACACS authentication scheme identified by the *hwtacacs-scheme-name* argument already exists. Refer to *AAA Operation* for information about HWTACACS authentication scheme.

Switching to a specific user level

Follow these steps to switch to a specific user level:

To do...	Use the command...	Remarks
Switch to a specified user level	super [/level/]	Required Execute this command in user view.



Note

- If no user level is specified in the **super password** command or the **super** command, level 3 is used by default.
- For security purpose, the password entered is not displayed when you switch to another user level. You will remain at the original user level if you have tried three times but failed to enter the correct authentication information.

Configuration examples

After a general user telnets to the switch, his/her user level is 0. Now, the network administrator wants to allow general users to switch to level 3, so that they are able to configure the switch.

Super password authentication configuration example

- The administrator configures the user level switching authentication policies.

Set the user level switching authentication mode for VTY 0 users to super password authentication.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] super authentication-mode super-password
[Sysname-ui-vty0] quit
```

Set the password used by the current user to switch to level 3.

```
[Sysname] super password level 3 simple 123
```

- A VTY 0 user switches its level to level 3 after logging in.

A VTY 0 user telnets to the switch, and then uses the set password to switch to user level 3.

```
<Sysname> super 3
Password:
User privilege level is 3, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

After configuring the switch, the general user switches back to user level 0.

```
<Sysname> super 0
User privilege level is 0, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```


HWTACACS authentication configuration example

- The administrator configures the user level switching authentication policies.

Configure a HWTACACS authentication scheme named **acs**, and specify the user name and password used for user level switching on the HWTACACS server defined in the scheme. Refer to *AAA Operation* for detailed configuration procedures.

Enable HWTACACS authentication for VTY 0 user level switching.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] super authentication-mode scheme
[Sysname-ui-vty0] quit
```

Specify to adopt the HWTACACS authentication scheme named **acs** for user level switching in the ISP domain named system.

```
[Sysname] domain system
[Sysname-isp-system] authentication super hwtacacs-scheme acs
```

- A VTY 0 user switches its level to level 3 after logging in.

Switch to user level 3 (assuming that you log into the switch as a VTY 0 user by Telnet).

```
<Sysname> super 3
Username: user@system
Password:

User privilege level is 3, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

Table of Contents

1 Configuration File Management	1-1
Introduction to Configuration File	1-1
Configuration Task List	1-2
Saving the Current Configuration	1-2
Erasing the Startup Configuration File	1-4
Specifying a Configuration File for Next Startup	1-4
Displaying Switch Configuration	1-5

1 Configuration File Management

When configuring configuration file management, go to these sections for information you are interested in:

- [Introduction to Configuration File](#)
- [Configuration Task List](#)

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.

Types of configuration

The configuration of a switch falls into two types:

- Saved configuration, a configuration file used for initialization. If this file does not exist, the switch starts up without loading any configuration file.
- Current configuration, which refers to the user's configuration during the operation of a switch. This configuration is stored in Dynamic Random-Access Memory (DRAM). It is removed when rebooting.

Format of configuration file

Configuration files are saved as text files for ease of reading. They:

- Save configuration in the form of commands.
- Save only non-default configuration settings.
- 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 comment lines. (A line is a comment line if it starts with the character #.)
- The sections are listed in this order: system configuration section, logical interface configuration section, physical port configuration section, routing protocol configuration section, user interface configuration, and so on.
- End with a return.

The operating interface provided by the configuration file management function is user-friendly. With it, you can easily manage your configuration files.

Main/backup attribute of the configuration file

Main and backup indicate the main and backup attribute of the configuration file respectively. A main configuration file and a backup configuration file can coexist on the switch. As such, when the main configuration file is missing or damaged, the backup file can be used instead. This increases the safety and reliability of the file system compared with the switch that only support one configuration file. You can configure a file to have both main and backup attribute, but only one file of either main or backup attribute is allowed on a switch.

The following three situations are concerned with the main/backup attributes:

- When saving the current configuration, you can specify the file to be a main or backup or normal configuration file.
- When removing a configuration file from a switch, you can specify to remove the main or backup configuration file. Or, if it is a file having both main and backup attribute, you can specify to erase the main or backup attribute of the file.
- When setting the configuration file for next startup, you can specify to use the main or backup configuration file.

Startup with the configuration file

When booting, the system chooses the configuration files following the rules below:

- 1) If the main configuration file exists, the switch initializes with this configuration.
- 2) If the main configuration file does not exist but the backup configuration file exists, the switch initializes with the backup configuration.
- 3) If neither the main nor the backup configuration file exists, but the default configuration file **config.def** exists, the switch initializes with the default configuration file; if the default configuration file does not exist, the switch starts up without loading the configuration file.



Note

At present, only a PoE-supported switch is shipped with a default configuration file.

Configuration Task List

Complete these tasks to configure configuration file management:

Task	Remarks
Saving the Current Configuration	Optional
Erasing the Startup Configuration File	Optional
Specifying a Configuration File for Next Startup	Optional

Saving the Current Configuration

You can modify the configuration on your switch at the command line interface (CLI). To use the modified configuration for your subsequent startups, you must save it (using the **save** command) as a configuration file.

Use the following command to save current configuration:

To do...	Use the command...	Remarks
Save current configuration	save [<i>cfgfile</i> [safely] [backup main]]	Required Available in any view

Modes in saving the configuration

- Fast saving mode. This is the mode when you use the **save** command without the **safely** keyword. The mode saves the file quicker but is likely to lose the original configuration file if the switch reboots or the power fails during the process.
- Safe mode. This is the mode when you use the **save** command with the **safely** keyword. The mode saves the file slower but can retain the original configuration file in the switch even if the switch reboots or the power fails during the process.

When you use the **save safely** command to save the configuration file, if the switch reboots or the power fails during the saving process, the switch initializes itself in the following two conditions when it starts up next time:

- If a configuration file with the extension **.cfg** exists in the Flash, the switch uses the configuration file to initialize itself when it starts up next time.
- If there is no **.cfg** configuration file in the Flash, but there is a configuration file with the extension **.cfgbak** (backup configuration file containing the original configuration information) or/and a configuration file with the extension **.cfgtmp** (temporary configuration file containing the current configuration information) in the Flash, you can change the extension **.cfgbak** or **.cfgtmp** to **.cfg** using the **rename** command. The switch will use the renamed configuration file to initialize itself when it starts up next time.

For details of the **rename** command, refer to the *File System Management* part of the manual.

Three attributes of the configuration file

- Main attribute. When you use the **save [[safely] [main]]** command to save the current configuration, the configuration file you get has main attribute. If this configuration file already exists and has backup attribute, the file will have both main and backup attributes after execution of this command. If the filename you entered is different from that existing in the system, this command will erase its main attribute to allow only one main attribute configuration file in the switch.
- Backup attribute. When you use the **save [safely] backup** command to save the current configuration, the configuration file you get has backup attribute. If this configuration file already exists and has main attribute, the file will have both main and backup attributes after execution of this command. If the filename you entered is different from that existing in the system, this command will erase its backup attribute to allow only one backup attribute configuration file in the switch.
- Normal attribute. When you use the **save cfgfile** command to save the current configuration, the configuration file you get has normal attribute if it is not an existing file. Otherwise, the attribute is dependent on the original attribute of the file.



Note

- It is 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.
- 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.
- The extension name of the configuration file must be .cfg.

Erasing the Startup Configuration File

You can clear the configuration files saved on the switch through commands.

Use the following command to erase the configuration file:

To do...	Use the command...	Remarks
Erase the startup configuration file from the storage switch	reset saved-configuration [backup main]	Required Available in user view

You may need to erase the configuration file for one of these reasons:

- After you upgrade software, the old configuration file does not match the new software.
- The startup configuration file is corrupted or not the one you needed.

The following two situations exist:

- While the **reset saved-configuration** [**main**] command erases the configuration file with main attribute, it only erases the main attribute of a configuration file having both main and backup attribute.
- While the **reset saved-configuration backup** command erases the configuration file with backup attribute, it only erases the backup attribute of a configuration file having both main and backup attribute.



Caution

This command will permanently delete the configuration file from the switch.

Specifying a Configuration File for Next Startup

Use the following command to specify a configuration file for next startup:

To do...	Use the command...	Remarks
Specify a configuration file for next startup	startup saved-configuration <i>cfgfile</i> [backup main]	Required Available in user view

You can specify a configuration file to be used for the next startup and configure the main/backup attribute for the configuration file.

Assigning main attribute to the startup configuration file

- If you save the current configuration to the main configuration file, the system will automatically set the file as the main startup configuration file.
- You can also use the **startup saved-configuration *cfgfile* [main]** command to set the file as main startup configuration file.

Assigning backup attribute to the startup configuration file

- If you save the current configuration to the backup configuration file, the system will automatically set the file as the backup startup configuration file.
- You can also use the **startup saved-configuration *cfgfile* backup** command to set the file as backup startup configuration file.



Caution

The configuration file must use .cfg as its extension name and the startup configuration file must be saved at the root directory of the switch.

Displaying Switch Configuration

To do...	Use the command...	Remarks
Display the initial configuration file saved in the Flash of a switch	display saved-configuration [unit <i>unit-id</i>] [by-linenum]	Available in any view.
Display the configuration file used for this and next startup	display startup [unit <i>unit-id</i>]	
Display the current VLAN configuration of the switch	display current-configuration vlan [<i>vlan-id</i>] [by-linenum]	
Display the validated configuration in current view	display this [by-linenum]	
Display current configuration	display current-configuration [configuration [<i>configuration-type</i>] interface [<i>interface-type</i>] [<i>interface-number</i>] [by-linenum] [{ begin exclude include } <i>regular-expression</i>]	

Table of Contents

1 VLAN Overview	1-1
VLAN Overview	1-1
Introduction to VLAN	1-1
Advantages of VLANs	1-2
VLAN Fundamentals	1-2
VLAN Interface	1-4
VLAN Classification	1-4
Port-Based VLAN	1-4
Link Types of Ethernet Ports	1-4
Assigning an Ethernet Port to Specified VLANs	1-5
Configuring the Default VLAN ID for a Port	1-5
Protocol-Based VLAN	1-6
Introduction to Protocol-Based VLAN	1-6
Encapsulation Format of Ethernet Data	1-6
Procedure for the Switch to Judge Packet Protocol	1-9
Encapsulation Formats	1-9
Implementation of Protocol-Based VLAN	1-10
2 VLAN Configuration	2-1
VLAN Configuration	2-1
VLAN Configuration Task List	2-1
Basic VLAN Configuration	2-1
Basic VLAN Interface Configuration	2-2
Displaying VLAN Configuration	2-3
Configuring a Port-Based VLAN	2-3
Port-Based VLAN Configuration Task List	2-3
Configuring the Link Type of an Ethernet Port	2-3
Assigning an Ethernet Port to a VLAN	2-4
Configuring the Default VLAN for a Port	2-4
Displaying and Maintaining Port-Based VLAN	2-5
Port-Based VLAN Configuration Example	2-5
Configuring a Protocol-Based VLAN	2-7
Protocol-Based VLAN Configuration Task List	2-7
Configuring a Protocol Template for a Protocol-Based VLAN	2-7
Associating a Port with a Protocol-Based VLAN	2-8
Displaying Protocol-Based VLAN Configuration	2-9
Protocol-Based VLAN Configuration Example	2-9

1 VLAN Overview

This chapter covers these topics:

- [VLAN Overview](#)
- [Port-Based VLAN](#)
- [Protocol-Based VLAN](#)

VLAN Overview

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. Hubs and switches, which are the basic network connection devices, have limited forwarding functions.

- A hub is a physical layer device without the switching function, so it forwards the received packet to all ports except the inbound port of the packet.
- A switch is a link layer device which can forward a 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.

The above scenarios could result in the following network problems.

- Large quantity of broadcast packets or unknown unicast packets may exist in a network, wasting network resources.
- A host in the network receives a lot of packets whose destination is not the host itself, causing potential serious security problems.

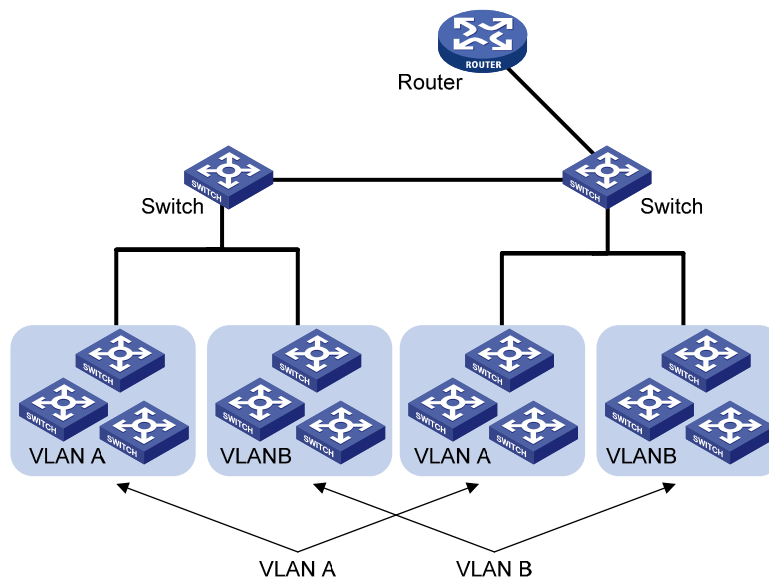
Isolating broadcast domains is the solution for the above problems. The traditional way is to use routers, which forward packets according to the destination IP address and does not forward broadcast packets in the link layer. However, routers are expensive and provide few ports, so they cannot split the network efficiently. Therefore, using routers to isolate broadcast domains has many limitations.

The Virtual Local Area Network (VLAN) technology is developed for switches to control broadcasts in LANs.

A VLAN can span multiple physical spaces. This enables hosts in a VLAN to be located in different physical locations.

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 in the traditional Ethernet way. However, hosts in different VLANs cannot communicate with each other directly but need the help of network layer devices, such as routers and Layer 3 switches. [Figure 1-1](#) illustrates a VLAN implementation.

Figure 1-1 A VLAN implementation



Advantages of VLANs

Compared with traditional Ethernet technology, VLAN technology delivers the following benefits:

- Confining broadcast traffic within individual VLANs. This saves bandwidth and improves network performance.
- Improving LAN security. By assigning user groups to different VLANs, you can isolate them at Layer 2. To enable communication between VLANs, routers or Layer 3 switches are required.
- Flexible virtual workgroup creation. As users from the same workgroup can be assigned to the same VLAN regardless of their physical locations, network construction and maintenance is much easier and more flexible.

VLAN Fundamentals

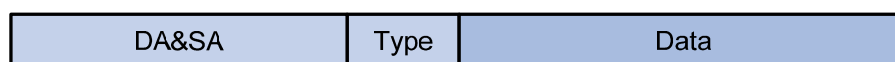
VLAN tag

To enable a Layer-2 switch to identify frames of different VLANs, a VLAN tag field is inserted into the data link layer encapsulation.

The format of VLAN-tagged frames is defined in IEEE 802.1Q issued by IEEE in 1999.

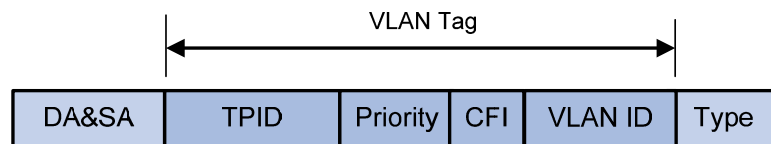
In the header of a traditional Ethernet data frame, the field after the destination MAC address and the source MAC address (DA&SA) is the Type field indicating the upper layer protocol type, as shown in [Figure 1-2](#).

Figure 1-2 Encapsulation format of traditional Ethernet frames



IEEE 802.1Q inserts a four-byte VLAN tag after the DA&SA field, as shown in [Figure 1-3](#).

Figure 1-3 Format of VLAN tag



A VLAN tag comprises four fields: tag protocol identifier (TPID), priority, canonical format indicator (CFI), and VLAN ID.

- The 16-bit TPID field with a value of 0x8100 indicates that the frame is VLAN tagged. On the H3C series Ethernet switches, the default TPID is 0x8100.
- The 3-bit priority field indicates the 802.1p priority of the frame. Refer to the “QoS-QoS profile” part of this manual for details.
- The 1-bit CFI field specifies whether the MAC addresses are encapsulated in the canonical format for the receiving device to correctly interpret the MAC addresses. Value 0 indicates that the MAC addresses are encapsulated in canonical format; value 1 indicates that the MAC addresses are encapsulated in non-canonical format. The field is set to 0 by default.
- The 12-bit VLAN ID field identifies the VLAN the frame belongs to. The VLAN ID range is 0 to 4095. As 0 and 4095 are reserved by the protocol, a VLAN ID actually ranges from 1 to 4094.



The Ethernet II encapsulation format is used here. Besides the Ethernet II encapsulation format, other encapsulation formats such as 802.2 LLC and 802.2 SNAP are also supported by Ethernet. The VLAN tag fields are also added to frames encapsulated in these formats for VLAN identification. Refer to section [Encapsulation Format of Ethernet Data](#) for 802.2/802.3 encapsulation format.

VLAN ID identifies the VLAN to which a packet belongs. When a switch receives a packet carrying no VLAN tag, the switch encapsulates a VLAN tag with the default VLAN ID of the inbound port for the packet, and sends the packet to the default VLAN of the inbound port for transmission. For the details about setting the default VLAN of a port, refer to [Configuring the Default VLAN ID for a Port](#).

MAC address learning mechanism of VLANs

Switches forward packets according to the destination MAC addresses of the packets. So that switches maintain a table called MAC address forwarding table to record the source MAC addresses of the received packets and the corresponding ports receiving the packets for consequent packet forwarding. The process of recording is called MAC address learning.

After VLANs are configured on a switch, the MAC address learning of the switch has the following two modes.

- Shared VLAN Learning (SVL): the switch records all the MAC address entries learnt by ports in all VLANs to a shared MAC address forwarding table. Packets received on any port of any VLAN are forwarded according to this table.
- Independent VLAN Learning (IVL): the switch maintains an independent MAC address forwarding table for each VLAN. The source MAC address of a packet received on a port of a VLAN is

recorded to the MAC address forwarding table of this VLAN only, and packets received on a port of a VLAN are forwarded according to the VLAN's own MAC address forwarding table.

Currently, the H3C S3600 series Ethernet switches adopt the IVL mode only. For more information about the MAC address forwarding table, refer to the “MAC Address Forwarding Table Management” part of the manual.

VLAN Interface

Hosts in different VLANs cannot communicate with each other directly unless routers or Layer 3 switches are used to do Layer 3 forwarding. The S3600 series Ethernet switches support VLAN interfaces configuration to forward packets in Layer 3.

VLAN interface is a virtual interface in Layer 3 mode, used to realize the layer 3 communication between different VLANs, and does not exist on a switch as a physical entity. Each VLAN has a VLAN interface, which can forward packets of the local VLAN to the destination IP addresses at the network layer. Normally, since VLANs can isolate broadcast domains, each VLAN corresponds to an IP network segment. And a VLAN interface serves as the gateway of the segment to forward packets in Layer 3 based on IP addresses.

VLAN Classification

Depending on how VLANs are established, VLANs fall into the following six categories.

- Port-based VLANs
- MAC address-based VLANs
- Protocol-based VLANs
- IP-subnet-based VLANs
- Policy-based VLANs
- Other types

At present, the S3600 series switches support the port-based and protocol-based VLANs.

Port-Based VLAN

Port-based VLAN technology introduces the simplest way to classify VLANs. You can assign the ports on the device to different VLANs. Thus packets received on a port will be transmitted through the corresponding VLAN only, so as to isolate hosts to different broadcast domains and divide them into different virtual workgroups.

Ports on Ethernet switches have the three link types: access, trunk, and hybrid. For the three types of ports, the process of being added into a VLAN and the way of forwarding packets are different.

Port-based VLANs are easy to implement and manage and applicable to hosts with relatively fixed positions.

Link Types of Ethernet Ports

The link type of an Ethernet port on the S3600 series can be one of the following:

- Access: An access port can belong to only one VLAN, and is generally connected to a user PC.
- Trunk: A trunk port can belong to more than one VLAN. It can forward packets for multiple VLANs, and is generally connected to another switch.

- Hybrid: A hybrid port can belong to more than one VLAN to forward packets for multiple VLANs. It can be connected to either a switch or a user PC.



Note

A hybrid port allows the packets of multiple VLANs to be sent untagged, but a trunk port only allows the packets of the default VLAN to be sent untagged.

The three types of ports can coexist on the same device.

Assigning an Ethernet Port to Specified VLANs

You can assign an Ethernet port to a VLAN to forward packets for the VLAN, thus allowing the VLAN on the current switch to communicate with the same VLAN on the peer switch.

An access port can be assigned to only one VLAN, while a hybrid or trunk port can be assigned to multiple VLANs.



Note

Before assigning an access or hybrid port to a VLAN, create the VLAN first.

Configuring the Default VLAN ID for a 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 multiple VLANs, so you should configure a default VLAN ID for the port.

After a port is added to a VLAN and configured with a default VLAN, the port receives and sends packets in a way related to its link type. For detailed description, refer to the following tables:

Table 1-1 Packet processing of an access port

Processing of an incoming packet		Processing of an outgoing packet
For an untagged packet	For a tagged packet	
Receive the packet and tag the packet with the default VLAN tag.	• 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.	Strip the tag from the packet and send the packet.

Table 1-2 Packet processing of a trunk port

Processing of an incoming packet		Processing of an outgoing packet
For an untagged packet	For a tagged packet	
- If the port has already been added to its default VLAN, tag the packet with the default VLAN tag and then forward the packet. - If the port has not been added to its default VLAN, discard the packet.	- If the VLAN ID is one of the VLAN IDs allowed to pass through the port, receive the packet. - If the VLAN ID is not one of the VLAN IDs allowed to pass through the port, discard the packet.	- If the VLAN ID is just the default VLAN ID, strip off 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.

Table 1-3 Packet processing of a hybrid port

Processing of an incoming packet		Processing of an outgoing packet
For an untagged packet	For a tagged packet	
- If the port has already been added to its default VLAN, tag the packet with the default VLAN tag and then forward the packet. - If the port has not been added to its default VLAN, discard the packet.	- If the VLAN ID is one of the VLAN IDs allowed to pass through the port, receive the packet. - If the VLAN ID is not one of the VLAN IDs allowed to pass through the port, discard the packet.	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 keeps or strips off the tags when sending packets of a VLAN (including the default VLAN).

Protocol-Based VLAN

Introduction to Protocol-Based VLAN

Protocol-based VLAN is also known as protocol VLAN, which is another way to classify VLANs. 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 specific fields. If a packet is matched, the switch will add a corresponding VLAN tag to it automatically. Thus, data of 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.

Encapsulation Format of Ethernet Data

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

Ethernet II and 802.2/802.3 encapsulation

There are two encapsulation types of Ethernet packets: Ethernet II defined by RFC 894 and 802.2/802.3 defined by RFC 1042. The two encapsulation formats are described in the following figures.

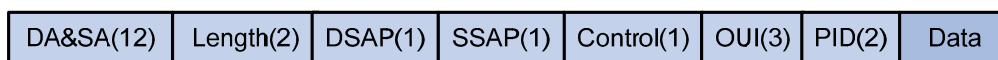
Ethernet II packet:

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 bytes.

The maximum length of an Ethernet packet is 1500 bytes, that is, 0x05DC 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.

Packets with the value of the type or length field being in the range 0x05DD to 0x05FF are regarded as illegal packets and thus discarded directly.

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.



Note

The 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.

Extended encapsulation formats of 802.2/802.3 packets

802.2/802.3 packets have the following three extended encapsulation formats:

- 802.3 raw encapsulation: only the length field is encapsulated after the source and destination address field, followed by the upper layer data. No other fields are included.

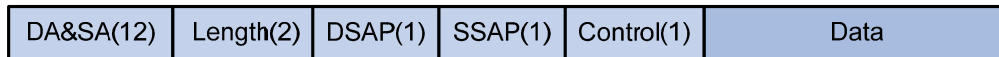
Figure 1-6 802.3 raw encapsulation format



Currently, only IPX supports 802.3 raw encapsulation, featuring with the value of the two bytes after the length field being 0xFFFF.

- 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. The value of the control field is always 3.

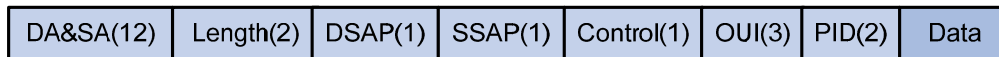
Figure 1-7 802.2 LLC encapsulation format



The DSAP field and the SSAP field in the 802.2 LLC encapsulation are used to identify the upper layer protocol. For example, if the two fields are both 0xE0, the upper layer protocol is IPX protocol.

- 802.2 Sub-Network Access Protocol (SNAP) encapsulation: encapsulates packets according to the 802.3 standard packet format, including the length, DSAP, SSAP, control, organizationally unique identifier (OUI), and protocol-ID (PID) fields.

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 0xAA, 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.

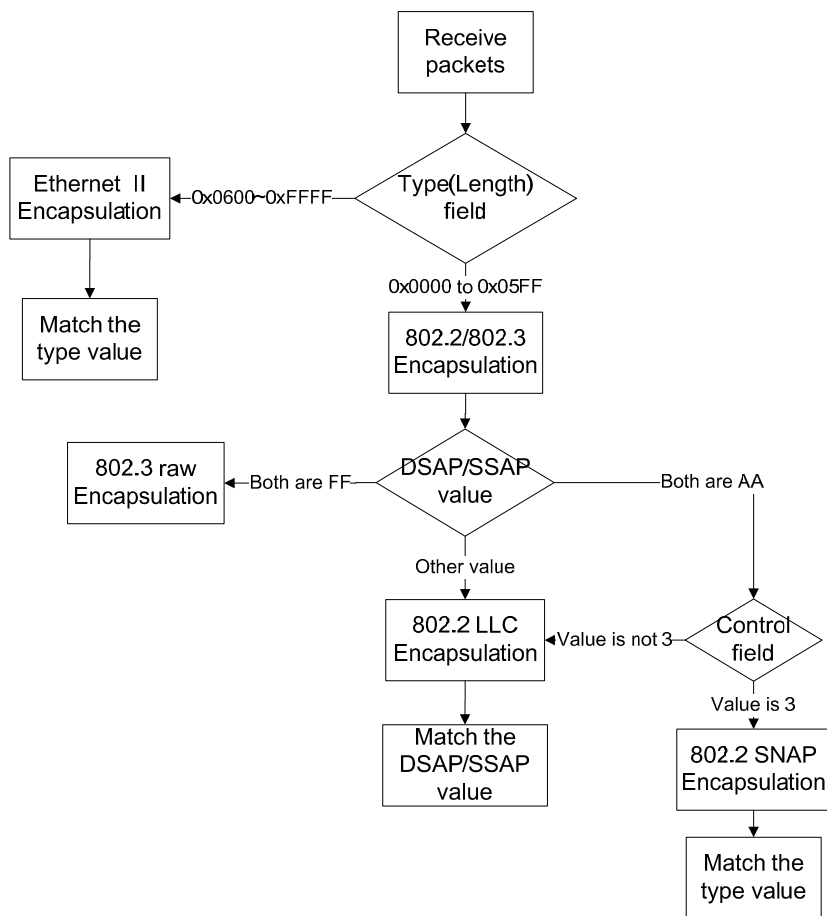


Note

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 RFC 1042 encapsulation, which is standard SNAP encapsulation. The SNAP encapsulation mentioned in this chapter refers to SNAP RFC 1042 encapsulation.

Procedure for the Switch to Judge Packet Protocol

Figure 1-9 Protocol identification procedure



Encapsulation Formats

[Table 1-4](#) lists the encapsulation formats supported by some protocols. In brackets are type values of these protocols.

Table 1-4 Encapsulation formats

Encapsulation (left)	Ethernet II	802.3 raw	802.2 LLC	802.2 SNAP
Protocol (down)				
IP (0x0800)	Supported	Not supported	Not supported	Supported
IPX (0x8137)	Supported	Supported	Supported	Supported
AppleTalk (0x809B)	Supported	Not supported	Not supported	Supported

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.

2 VLAN Configuration

When configuring a VLAN, go to these sections for information you are interested in:

- [VLAN Configuration](#)
- [Configuring a Port-Based VLAN](#)
- [Configuring a Protocol-Based VLAN](#)

VLAN Configuration

VLAN Configuration Task List

Complete the following tasks to configure VLAN:

Task	Remarks
Basic VLAN Configuration	Required
Basic VLAN Interface Configuration	Optional
Displaying VLAN Configuration	Optional

Basic VLAN Configuration

Follow these steps to perform basic VLAN configuration:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create multiple VLANs in batch	vlan { <i>vlan-id1</i> to <i>vlan-id2</i> all }	Optional
Create a VLAN and enter VLAN view	vlan <i>vlan-id</i>	Required By default, there is only one VLAN, that is, the default VLAN (VLAN 1).
Assign a name for the current VLAN	name <i>text</i>	Optional By default, the name of a VLAN is its VLAN ID. VLAN 0001 for example.
Specify the description string of the current VLAN	description <i>text</i>	Optional By default, the description string of a VLAN is its VLAN ID. VLAN 0001 for example.



Caution

- VLAN 1 is the system default VLAN, which needs not to be created and cannot be removed, either.
- The VLAN you created in the way described above is a static VLAN. On the switch, there are dynamic VLANs which are registered through GVRP. For details, refer to “GVRP” part of this manual.
- 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.

Basic VLAN Interface Configuration

Configuration prerequisites

Before configuring a VLAN interface, create the corresponding VLAN.

Configuration procedure

Follow these steps to perform basic VLAN interface configuration:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a VLAN interface and enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	Required By default, there is no VLAN interface on a switch.
Specify the description string for the current VLAN interface	description <i>text</i>	Optional By default, the description string of a VLAN interface is the name of this VLAN interface. Vlan-interface1 Interface for example.
Disable the VLAN interface	shutdown	Optional By default, the VLAN interface is enabled. In this case, the VLAN interface's status is determined by the status of the ports in the VLAN, that is, if all ports of the VLAN are down, the VLAN interface is down (disabled); if one or more ports of the VLAN are up, the VLAN interface is up (enabled).
Enable the VLAN Interface	undo shutdown	If you disable the VLAN interface, the VLAN interface will always be down, regardless of the status of the ports in the VLAN.



Note

The operation of enabling/disabling a VLAN's VLAN interface does not influence the physical status of the Ethernet ports belonging to this VLAN.

Displaying VLAN Configuration

To do...	Use the command...	Remarks
Display the VLAN interface information	display interface Vlan-interface [<i>vlan-id</i>]	Available in any view.
Display the VLAN information	display vlan [<i>vlan-id</i> [<i>to vlan-id</i>] all dynamic static]	

Configuring a Port-Based VLAN

Port-Based VLAN Configuration Task List

Complete these tasks to configure a port-based VLAN:

Task	Remarks
Configuring the Link Type of an Ethernet Port	Optional
Assigning an Ethernet Port to a VLAN	Required
Configuring the Default VLAN for a Port	Optional

Configuring the Link Type of an Ethernet Port

Follow these steps to configure the link type of an Ethernet port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the port link type	port link-type { access hybrid trunk }	Required The link type of an Ethernet port is access by default.



Note

- To change the link type of a port from trunk to hybrid or vice versa, you need to set the link type to access first.
- You can use the **port link-type irf-fabric** command to configure fabric ports. For information about this command, refer to the *IRF Fabric* module in this manual.

Assigning an Ethernet Port to a VLAN

You can assign an Ethernet port to a VLAN in Ethernet port view or VLAN view.

1) In Ethernet port view

Follow these steps to assign an Ethernet port to one or multiple VLANs:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enter Ethernet port view		interface <i>interface-type interface-number</i>	—
Assign the port to one or multiple VLANs	Access port	port access vlan <i>vlan-id</i>	Optional By default, all Ethernet ports belong to VLAN 1.
	Trunk port	port trunk permit vlan { <i>vlan-id-list</i> all }	
	Hybrid port	port hybrid vlan <i>vlan-id-list</i> { tagged untagged }	



Note

When assigning an access or hybrid port to a VLAN, make sure the VLAN already exists.

2) In VLAN view

Follow these steps to assign one or multiple access ports to a VLAN in VLAN view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN view	vlan <i>vlan-id</i>	Required If the specified VLAN does not exist, this command creates the VLAN first.
Assign the specified access port or ports to the current VLAN	port <i>interface-list</i>	Required By default, all ports belong to VLAN 1.

Configuring the Default VLAN for a Port

Because an access port can belong to its default VLAN only, there is no need for you to configure the default VLAN for an access port.

This section describes how to configure a default VLAN for a trunk or hybrid port.

Follow these steps to configure the default VLAN for a port:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enter Ethernet port view		interface <i>interface-type</i> <i>interface-number</i>	—
Configure the default VLAN for the port	Trunk port	port trunk pvid vlan <i>vlan-id</i>	Optional VLAN 1 is the default VLAN by default.
	Hybrid port	port hybrid pvid vlan <i>vlan-id</i>	

Caution

- After configuring the default VLAN for a trunk or hybrid port, you need to use the **port trunk permit** command or the **port hybrid vlan** command to configure the port to allow traffic of the default VLAN to pass through. Otherwise, the port cannot forward traffic of the default VLAN, nor can it receive VLAN untagged packets.
- The local and remote trunk (or hybrid) ports must use the same default VLAN ID for the traffic of the default VLAN to be transmitted properly.

Displaying and Maintaining Port-Based VLAN

To do...	Use the command...	Remarks
Display the hybrid or trunk ports	display port { hybrid trunk }	Available in any view.

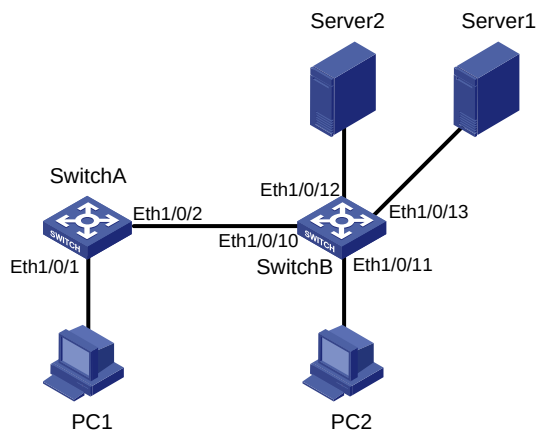
Port-Based VLAN Configuration Example

Network requirements

- As shown in [Figure 2-1](#), Switch A and Switch B connect to PC 1/PC 2 and Server 1/Server 2 used by different departments.
- To isolate data between different departments, PC 1 and Server 1 are assigned to VLAN 100 with the descriptive string being Dept1; PC 2 and Server 2 are assigned to VLAN 200 with the descriptive string being Dept2.
- Configure VLAN interfaces for the two VLANs on Switch A for forwarding data from PC 1 to Server 2 at Layer 3.

Network diagram

Figure 2-1 Network diagram for VLAN configuration



Configuration procedure

- Configure Switch A.

Create VLAN 100, specify its descriptive string as **Dept1**, and add Ethernet 1/0/1 to VLAN 100.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] description Dept1
[SwitchA-vlan100] port Ethernet 1/0/1
[SwitchA-vlan100] quit
```

Create VLAN 200, and specify its descriptive string as **Dept2**.

```
[SwitchA] vlan 200
[SwitchA-vlan200] description Dept2
[SwitchA-vlan200] quit
```

Create VLAN-interface 100 and VLAN-interface 200, and assign IP addresses 192.168.1.1 and 192.168.2.1 to them respectively. The two VLAN-interfaces are used for forwarding packets from Host 1 to Server 2 at Layer 3.

```
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 192.168.1.1 24
[SwitchA-Vlan-interface100] quit
[SwitchA] interface Vlan-interface 200
[SwitchA-Vlan-interface200] ip address 192.168.2.1 24
```

- Configure Switch B.

Create VLAN 100, specify its descriptive string as **Dept1**, and add Ethernet 1/0/13 to VLAN 100.

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] description Dept1
[SwitchB-vlan100] port Ethernet 1/0/13
[SwitchB-vlan100] quit
```

Create VLAN 200, specify its descriptive string as **Dept2** and add Ethernet 1/0/11 and Ethernet 1/0/12 to VLAN 200.


```
[SwitchB] vlan 200
[SwitchB-vlan200] description Dept2
[SwitchB-vlan200] port Ethernet1/0/11 Ethernet 1/0/12
[SwitchB-vlan200] quit
```

- Configure the link between Switch A and Switch B.

Because the link between Switch A and Switch B needs to transmit data of both VLAN 100 and VLAN 200, you can configure the ports at both ends of the link as trunk ports and permit packets of the two VLANs to pass through the two ports.

Configure Ethernet 1/0/2 of Switch A.

```
[SwitchA] interface Ethernet 1/0/2
[SwitchA-Ethernet1/0/2] port link-type trunk
[SwitchA-Ethernet1/0/2] port trunk permit vlan 100
[SwitchA-Ethernet1/0/2] port trunk permit vlan 200
```

Configure Ethernet 1/0/10 of Switch B.

```
[SwitchB] interface Ethernet 1/0/10
[SwitchB-Ethernet1/0/10] port link-type trunk
[SwitchB-Ethernet1/0/10] port trunk permit vlan 100
[SwitchB-Ethernet1/0/10] port trunk permit vlan 200
```

Configuring a Protocol-Based VLAN

Protocol-Based VLAN Configuration Task List

Complete these tasks to configure protocol-based VLAN:

Task	Remarks
Configuring a Protocol Template for a Protocol-Based VLAN	Required
Associating a Port with a Protocol-Based VLAN	Required
Displaying Protocol-Based VLAN Configuration	Optional

Configuring a Protocol Template for a Protocol-Based VLAN

Configuration prerequisites

Create a VLAN before configuring the VLAN as a protocol-based VLAN.

Configuration procedure

Follow these steps to configure the protocol template for a VLAN:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN view	vlan <i>vlan-id</i>	—

To do...	Use the command...	Remarks
Configure the protocol template for the VLAN	protocol-vlan [<i>protocol-index</i>] { at ip ipx { ethernetii llc raw snap } mode { ethernetii etype <i>etype-id</i> llc dsap <i>dsap-id</i> ssap <i>ssap-id</i> snap etype <i>etype-id</i> } }	Required By default, no protocol template is configured for the VLAN.

When configuring a protocol template for a protocol-based VLAN, use the **at**, **ip** or **ipx** keyword to configure a standard template to match AppleTalk, IP, and IPX packets respectively, and use the **mode** keyword to configure a user-defined template.



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 to avoid that ARP packets and IP packets are not assigned to the same VLAN, which will cause IP address resolution failure.
- If you specify some special values for both the *dsap-id* and *ssap-id* arguments when configuring the user-defined template for **llc** encapsulation, the matching packets will take the same encapsulation format as some standard type of packets. For example, when both *dsap-id* and *ssap-id* have a value of 0xFF, the encapsulation format will be the same as that of **ipx raw** packets; if they both have a value of 0xE0, the packet encapsulation format will be the same as that of **ipx llc** packets; if they both have a value of 0xAA, the packet encapsulation format will be the same as that of **snap** packets. To prevent two commands from processing packets of the same protocol type in different ways, the system does not allow you to set both the *dsap-id* and *ssap-id* arguments to 0xFF, 0xE0, or 0xAA.
- When you use the **mode** keyword to configure a user-defined protocol template, if you set the *etype-id* argument for **ethernetii** or **snap** packets to 0x0800, 0x8137, or 0x809B, the matching packets will take the same format as that of the IP, IPX, and AppleTalk packets respectively. To prevent two commands from processing packets of the same protocol type in different ways, the switch will prompt that you cannot set the *etype-id* argument for **Ethernet II** or **snap** packets to 0x0800, 0x8137, or 0x809B.

Associating a Port with a Protocol-Based VLAN

Configuration prerequisites

- The protocol template for the protocol-based VLAN is configured.
- 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.

Configuration procedure

Follow these steps to associate a port with the protocol-based VLAN:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter port view	interface <i>interface-type</i> <i>interface-number</i>	—
Associate the port with the specified protocol-based VLAN	port hybrid protocol-vlan vlan <i>vlan-id</i> { <i>protocol-index</i> [to <i>protocol-index-end</i>] all }	Required By default, a port is not associated with any protocol-based VLAN.

Displaying Protocol-Based VLAN Configuration

To do...	Use the command...	Remarks
Display the information about the protocol-based VLAN	display vlan [<i>vlan-id</i> [to <i>vlan-id</i>] all dynamic static]	Available in any view
Display the protocol information and protocol indexes configured on the specified VLAN	display protocol-vlan vlan { <i>vlan-id</i> [to <i>vlan-id</i>] all }	
Display the protocol information and protocol indexes configured on the specified port	display protocol-vlan interface { <i>interface-type</i> <i>interface-number</i> [to <i>interface-type</i> <i>interface-number</i>] all }	

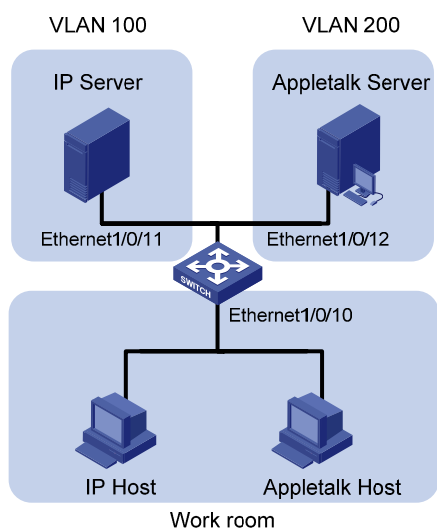
Protocol-Based VLAN Configuration Example

Network requirements

- As shown in [Figure 2-2](#), Workroom connects to the LAN through port Ethernet 1/0/10 on the S3600 switch.
- IP network and AppleTalk network workstations (hosts) coexist in the Workroom.
- The S3600 switch connects to VLAN 100 (using IP network) through Ethernet 1/0/11 and to VLAN 200 (using AppleTalk network) through Ethernet 1/0/12.
- Configure the switch to automatically assign the IP and AppleTalk packets to proper VLANs for transmission, so as to ensure the normal communication between the workstations and servers.

Network diagram

Figure 2-2 Network diagram for protocol-based VLAN configuration



Configuration procedure

Create VLAN 100 and VLAN 200, and add Ethernet 1/0/11 and Ethernet 1/0/12 to VLAN 100 and VLAN 200 respectively.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] port Ethernet 1/0/11
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] port Ethernet 1/0/12
```

Configure protocol templates for VLAN 200 and VLAN 100, matching AppleTalk protocol and IP protocol respectively.

```
[Switch-vlan200] protocol-vlan at
[Switch-vlan200] quit
[Switch] vlan 100
[Switch-vlan100] protocol-vlan ip
```

To ensure the normal operation of IP network, you need to configure a user-defined protocol template for VLAN 100 to match the ARP protocol (assume Ethernet II encapsulation is adopted here).

```
[Switch-vlan100] protocol-vlan mode ethernetii etype 0806
```

Display the created protocol-based VLANs and the protocol templates.

```
[Switch-vlan100] display protocol-vlan vlan all
VLAN ID: 100
VLAN Type: Protocol-based VLAN
  Protocol Index      Protocol Type
      0                ip
      1                ethernetii etype 0x0806
```

```
VLAN ID: 200
```

VLAN Type: Protocol-based VLAN

Protocol Index	Protocol Type
0	at

Configure Ethernet 1/0/10 as a hybrid port, which removes the VLAN tag of the packets of VLAN 100 and VLAN 200 before forwarding the packets.

```
[Switch-vlan100] quit
```

```
[Switch] interface Ethernet 1/0/10
```

```
[Switch-Ethernet1/0/10] port link-type hybrid
```

```
[Switch-Ethernet1/0/10] port hybrid vlan 100 200 untagged
```

Associate Ethernet 1/0/10 with protocol template 0 and 1 of VLAN 100, and protocol template 0 of VLAN 200.

```
[Switch-Ethernet1/0/10] port hybrid protocol-vlan vlan 100 0 to 1
```

```
[Switch-Ethernet1/0/10] port hybrid protocol-vlan vlan 200 0
```

Display the associations between Ethernet 1/0/10 and the VLAN protocol templates to verify your configuration.

```
[Switch-Ethernet1/0/10] display protocol-vlan interface Ethernet 1/0/10
```

Interface:Ethernet1/0/10

VLAN ID	Protocol-Index	Protocol-Type
100	0	ip
100	1	ethernetii etype 0x0806
200	0	at

The above output information indicates that Ethernet 1/0/10 has already been associated with the corresponding protocol templates of VLAN 100 and VLAN 200. Thus, packets from the IP and AppleTalk workstations can be automatically assigned to VLAN 100 and VLAN 200 respectively for transmission by matching the corresponding protocol templates, so as to realize the normal communication between workstations and servers.

Table of Contents

1 IP Addressing Configuration	1-1
IP Addressing Overview	1-1
IP Address Classes	1-1
Special Case IP Addresses	1-2
Subnetting and Masking	1-2
Configuring IP Addresses	1-3
Displaying IP Addressing Configuration	1-4
IP Address Configuration Examples	1-4
IP Address Configuration Example I	1-4
IP Address Configuration Example II	1-5
2 IP Performance Configuration	2-1
IP Performance Overview	2-1
Introduction to IP Performance Configuration	2-1
Introduction to FIB	2-1
Configuring IP Performance	2-1
IP Performance Configuration Task List	2-1
Configuring TCP Attributes	2-2
Enabling Reception of Directed Broadcasts to a Directly Connected Network	2-2
Disabling ICMP to Send Error Packets	2-3
Canceling the System-Defined ACLs for ICMP Attack Guard	2-3
Displaying and Maintaining IP Performance Configuration	2-4
IP Performance Configuration Example	2-5
Enabling the Reception of Directed Broadcasts to a Directly Connected Network	2-5

1 IP Addressing Configuration

When configuring IP addressing, go to these sections for information you are interested in:

- [IP Addressing Overview](#)
- [Configuring IP Addresses](#)
- [Displaying IP Addressing Configuration](#)
- [IP Address Configuration Examples](#)

IP Addressing Overview

IP Address Classes

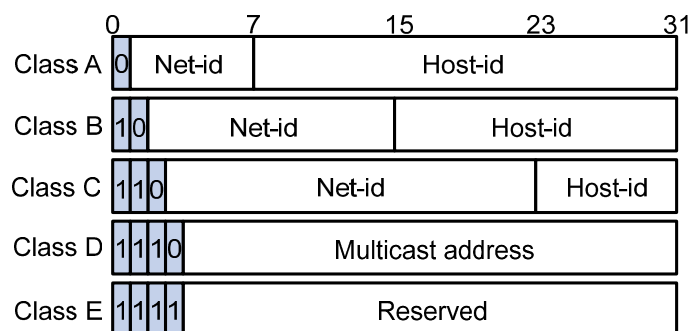
IP addressing uses a 32-bit address to identify each host on a network. An example is 01010000100000001000000010000000 in binary. To make IP addresses in 32-bit form easier to read, they are written in dotted decimal notation, each being four octets in length, for example, 10.1.1.1 for the address just mentioned.

Each IP address breaks down into two parts:

- Net ID: The first several bits of the IP address defining a network, also known as class bits.
- Host ID: Identifies a host on a network.

For administration sake, IP addresses are divided into five classes, as shown in the following figure (in which the blue parts represent the address class).

Figure 1-1 IP address classes



[Table 1-1](#) describes the address ranges of these five classes. Currently, the first three classes of IP addresses are used in quantity.

Table 1-1 IP address classes and ranges

Class	Address range	Description
A	0.0.0.0 to 127.255.255.255	Address 0.0.0.0 means this host on this network. This address is used by a host at bootstrap when it does not know its IP address. This address is never a valid destination address. Addresses starting with 127 are reserved for loopback test. Packets destined to these addresses are processed locally as input packets rather than sent to the link.
B	128.0.0.0 to 191.255.255.255	—
C	192.0.0.0 to 223.255.255.255	—
D	224.0.0.0 to 239.255.255.255	Multicast address.
E	240.0.0.0 to 255.255.255.255	Reserved for future use except for the broadcast address 255.255.255.255.

Special Case IP Addresses

The following IP addresses are for special use, and they cannot be used as host IP addresses:

- IP address with an all-zeros net ID: Identifies a host on the local network. For example, IP address 0.0.0.16 indicates the host with a host ID of 16 on the local network.
- IP address with an all-zeros host ID: Identifies a network.
- IP address with an all-ones host ID: Identifies a directed broadcast address. For example, a packet with the destination address of 192.168.1.255 will be broadcasted to all the hosts on the network 192.168.1.0.

Subnetting and Masking

Subnetting was developed to address the risk of IP address exhaustion resulting from fast expansion of the Internet. The idea is to break a network down into smaller networks called subnets by using some bits of the host ID to create a subnet ID. To identify the boundary between the host ID and the combination of net ID and subnet ID, masking is used.

Each subnet mask comprises 32 bits related to the corresponding bits in an IP address. In a subnet mask, the part containing consecutive ones identifies the combination of net ID and subnet ID whereas the part containing consecutive zeros identifies the host ID.

[Figure 1-2](#) shows how a Class B network is subnetted.

Figure 1-2 Subnet a Class B network



While allowing you to create multiple logical networks within a single Class A, B, or C network, subnetting is transparent to the rest of the Internet. All these networks still appear as one. As subnetting adds an additional level, subnet ID, to the two-level hierarchy with IP addressing, IP routing now involves three steps: delivery to the site, delivery to the subnet, and delivery to the host.

In the absence of subnetting, some special addresses such as the addresses with the net ID of all zeros and the addresses with the host ID of all ones, are not assignable to hosts. The same is true of subnetting. When designing your network, you should note that subnetting is somewhat a tradeoff between subnets and accommodated hosts. For example, a Class B network can accommodate 65,534 ($2^{16} - 2$. Of the two deducted Class B addresses, one with an all-ones host ID is the broadcast address and the other with an all-zeros host ID is the network address) hosts before being subnetted. After you break it down into 512 (2^9) subnets by using the first 9 bits of the host ID for the subnet, you have only 7 bits for the host ID and thus have only 126 ($2^7 - 2$) hosts in each subnet. The maximum number of hosts is thus 64,512 (512×126), 1022 less after the network is subnetted.

Class A, B, and C networks, before being subnetted, use these default masks (also called natural masks): 255.0.0.0, 255.255.0.0, and 255.255.255.0 respectively.

Configuring IP Addresses

S3600 Series Ethernet Switches support assigning IP addresses to VLAN interfaces and loopback interfaces. Besides directly assigning an IP address to a VLAN interface, you may configure a VLAN interface to obtain an IP address through BOOTP or DHCP as alternatives. If you change the way an interface obtains an IP address, from manual assignment to BOOTP for example, the IP address obtained from BOOTP will overwrite the old one manually assigned.



Note

This chapter only covers how to assign an IP address manually. For the other two approaches to IP address assignment, refer to the part discussing DHCP in this manual.

Follow these steps to configure an IP address to an interface:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—

To do...	Use the command...	Remarks
Assign an IP address to the Interface	ip address <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } [sub]	Required No IP address is assigned by default.



Note

- You can assign at most five IP address to an interface, among which one is the primary IP address and the others are secondary IP addresses. A newly specified primary IP address overwrites the previous one if there is any.
- The primary and secondary IP addresses of an interface cannot reside on the same network segment; the IP address of a VLAN interface must not be on the same network segment as that of a loopback interface on a device.
- A VLAN interface cannot be configured with a secondary IP address if the interface has been configured to obtain an IP address through BOOTP or DHCP.

Displaying IP Addressing Configuration

To do...	Use the command...	Remarks
Display information about a specified or all Layer 3 interfaces	display ip interface [<i>interface-type</i> <i>interface-number</i>]	Available in any view
Display brief configuration information about a specified or all Layer 3 interfaces	display ip interface brief [<i>interface-type</i> [<i>interface-number</i>]]	

IP Address Configuration Examples

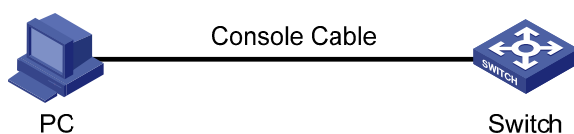
IP Address Configuration Example I

Network requirement

Assign IP address 129.2.2.1 with mask 255.255.255.0 to VLAN-interface 1 of the switch.

Network diagram

Figure 1-3 Network diagram for IP address configuration



Configuration procedure

Configure an IP address for VLAN-interface 1.

```

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

```

IP Address Configuration Example II

Network requirements

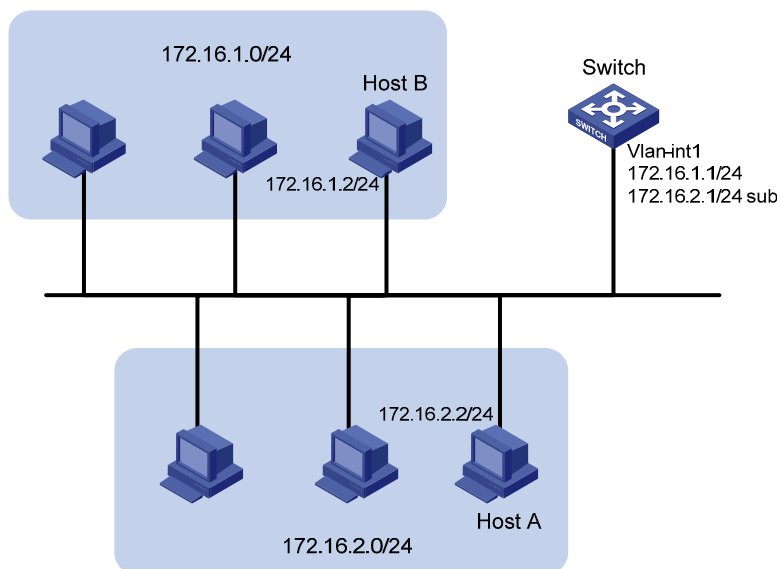
As shown in [Figure 1-4](#) VLAN-interface 1 on a switch is connected to a LAN comprising two segments: 172.16.1.0/24 and 172.16.2.0/24.

To enable the hosts on the two network segments to communicate with the external network through the switch, and the hosts on the LAN can communicate with each other, do the following:

- Assign two IP addresses to VLAN-interface 1 on the switch.
- Set the switch as the gateway on all PCs of the two networks.

Network diagram

Figure 1-4 Network diagram for IP address configuration



Configuration procedure

Assign a primary IP address and a secondary IP address to VLAN-interface 1.

```

<Switch> system-view
[Switch] interface Vlan-interface 1
[Switch-Vlan-interface1] ip address 172.16.1.1 255.255.255.0
[Switch-Vlan-interface1] ip address 172.16.2.1 255.255.255.0 sub

```

Set the gateway address to 172.16.1.1 on the PCs attached to the subnet 172.16.1.0/24, and to 172.16.2.1 on the PCs attached to the subnet 172.16.2.0/24.

Ping a host on the subnet 172.16.1.0/24 from the switch to check the connectivity.

```

<Switch> ping 172.16.1.2
PING 172.16.1.2: 56 data bytes, press CTRL_C to break
Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=255 time=25 ms
Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=255 time=27 ms

```

```
Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=255 time=26 ms
Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=255 time=26 ms
Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=255 time=26 ms
```

```
--- 172.16.1.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 25/26/27 ms
```

The output information shows the switch can communicate with the hosts on the subnet 172.16.1.0/24.

Ping a host on the subnet 172.16.2.0/24 from the switch to check the connectivity.

```
<Switch> ping 172.16.2.2
```

```
PING 172.16.2.2: 56 data bytes, press CTRL_C to break
Reply from 172.16.2.2: bytes=56 Sequence=1 ttl=255 time=25 ms
Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=255 time=26 ms
Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=255 time=26 ms
Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=255 time=26 ms
Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=255 time=26 ms
```

```
--- 172.16.2.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 25/25/26 ms
```

The output information shows the switch can communicate with the hosts on the subnet 172.16.2.0/24.

2 IP Performance Configuration

When configuring IP performance, go to these sections for information you are interested in:

- [IP Performance Overview](#)
- [Configuring IP Performance](#)
- [Displaying and Maintaining IP Performance Configuration](#)
- [IP Performance Configuration Example](#)



Note

Support for Canceling the System-Defined ACLs for ICMP Attack Guard is added. For details, refer to [Canceling the System-Defined ACLs for ICMP Attack Guard](#).

IP Performance Overview

Introduction to IP Performance Configuration

In some network environments, you need to adjust the IP parameters to achieve best network performance. The IP performance configuration supported by S3600 Series Ethernet Switches includes:

- Configuring TCP attributes
- Enabling reception of directed broadcasts to a directly connected network
- Disabling ICMP to send error packets
- Canceling the System-Defined ACLs for ICMP Attack Guard

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.

Configuring IP Performance

IP Performance Configuration Task List

Complete the following tasks to configure IP performance:

Task	Remarks
Configuring TCP Attributes	Optional

Task	Remarks
Enabling Reception of Directed Broadcasts to a Directly Connected Network	Optional
Disabling ICMP to Send Error Packets	Optional
Canceling the System-Defined ACLs for ICMP Attack Guard	Optional

Configuring TCP Attributes

TCP optional parameters that can be configured include:

- synwait timer: When sending a SYN packet, TCP starts the synwait timer. If no response packets are received before the synwait timer times out, the TCP connection is not successfully created.
- finwait timer: When the TCP connection is changed into FIN_WAIT_2 state, finwait timer will be started. If no FIN packets are received within the timer timeout, the TCP connection will be terminated. If FIN packets are received, the TCP connection state changes to TIME_WAIT. If non-FIN packets are received, the system restarts the timer from receiving the last non-FIN packet. The connection is broken after the timer expires.
- Size of TCP receive/send buffer

Follow these steps to configure TCP attributes:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure TCP synwait timer's timeout value	tcp timer syn-timeout <i>time-value</i>	Optional 75 seconds by default.
Configure TCP finwait timer's timeout value	tcp timer fin-timeout <i>time-value</i>	Optional 675 seconds by default.
Configure the size of TCP receive/send buffer	tcp window <i>window-size</i>	Optional 8 kilobytes by default.

Enabling Reception of Directed Broadcasts to a Directly Connected Network

Directed broadcasts refer to broadcast packets sent to a specific network. In the destination IP address of a directed broadcast, the network ID is the ID of network where the receiving interface resides and the host ID is all-ones. Enabling the device to receive directed broadcasts will give hackers an opportunity to attack the network, thus bringing forth great potential dangers to the network. Therefore, the reception of directed broadcasts to a directly connected network is disabled on S3600 series Ethernet switches by default. However, you should enable the feature when:

- Using the UDP Helper function to convert broadcasts to unicasts and forward them to a specified server.
- Using the Wake on LAN function to forward directed broadcasts to a host on the remote network.

Follow these steps to enable the switch to receive directed broadcasts:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the device to receive directed broadcasts	ip forward-broadcast	Required Disabled by default.

Disabling ICMP to Send Error Packets

Sending error packets is a major function of ICMP protocol. In case of network abnormalities, ICMP packets are usually sent by the network or transport layer protocols to notify corresponding devices so as to facilitate control and management.

Although sending ICMP error packets facilitate control and management, it still has the following disadvantages:

- Sending a lot of ICMP packets will increase network traffic.
- If receiving a lot of malicious packets that cause it to send ICMP error packets, the device's performance will be reduced.
- As the ICMP redirection function increases the routing table size of a host, the host's performance will be reduced if its routing table becomes very large.
- If a host sends malicious ICMP destination unreachable packets, end users may be affected.

You can disable the device from sending such ICMP error packets for reducing network traffic and preventing malicious attacks.

Follow these steps to disable sending ICMP error packets:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Disable sending ICMP redirects	undo icmp redirect send	Required Enabled by default.
Disable sending ICMP destination unreachable packets	undo icmp unreachable send	Required Enabled by default.

Canceling the System-Defined ACLs for ICMP Attack Guard

ICMP attacks are common in networks. To guard against malicious ICMP attacks, the device pre-defines some ACLs to match the incoming ICMP packets and process them separately, thus reducing ICMP attacks' impact on normal data packets and increasing network stability.

In a secure network, you can cancel the system-defined ACLs for ICMP attack guard, and thus increase the available ACL resources.

Follow these steps to cancel the system-defined ACLs for ICMP attack guard:

To do ...	Use the command...	Remarks
Enter system view	system-view	—

To do ...	Use the command...	Remarks
Cancel the system-defined ACLs for ICMP attack guard	undo icmp acl-priority	Required By default, the system keeps the system-defined ACLs for ICMP attack guard.



Note

Before canceling the system-defined ACLs for ICMP attack guard, check ICMP attack vulnerabilities in the network to make sure that the network can operate properly after you cancel the system-defined ACLs for ICMP attack guard.

Displaying and Maintaining IP Performance Configuration

To do...	Use the command...	Remarks
Display TCP connection status	display tcp status	Available 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 [socketype <i>sock-type</i>] [<i>task-id</i> <i>socket-id</i>]	
Display the forwarding information base (FIB) entries	display fib	
Display the FIB entries matching the destination IP address	display fib <i>ip_address1</i> [{ <i>mask1</i> <i>mask-length1</i> } [<i>ip_address2</i> { <i>mask2</i> <i>mask-length2</i> } longer] longer]	
Display the FIB entries filtering through a specific ACL	display fib acl <i>number</i>	
Display the FIB entries in the buffer which begin with, include or exclude the specified character string.	display fib { begin include exclude } <i>regular-expression</i>	
Display the FIB entries filtering through a specific prefix list	display fib ip-prefix <i>ip-prefix-name</i>	
Display the total number of the FIB entries	display fib statistics	

To do...	Use the command...	Remarks
Clear IP traffic statistics	reset ip statistics	Available in user view
Clear TCP traffic statistics	reset tcp statistics	
Clear UDP traffic statistics	reset udp statistics	

IP Performance Configuration Example

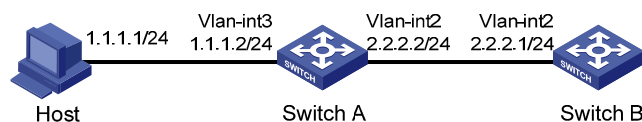
Enabling the Reception of Directed Broadcasts to a Directly Connected Network

Network requirements

As shown in [Figure 2-1](#), the host's interface and VLAN-interface 3 of Switch A are on the same network segment (1.1.1.0/24). VLAN-interface 2 of Switch A and VLAN-interface 2 of Switch B are on another network segment (2.2.2.0/24). The default gateway of the host is VLAN-interface 3 (IP address 1.1.1.2/24) of Switch A. Configure a static route on Switch B to the host.

Network diagram

Figure 2-1 Network diagram for enabling the reception of directed broadcast



Configuration procedure

1) Configure Switch A

Enable Switch A to receive directed broadcasts.

```
<SwitchA> system-view
```

```
[SwitchA] ip forward-broadcast
```

Configure IP addresses for VLAN-interface 3 and VLAN-interface 2.

```
[SwitchA] interface vlan-interface 3
```

```
[SwitchA-Vlan-interface3] ip address 1.1.1.2 24
```

```
[SwitchA-Vlan-interface3] quit
```

```
[SwitchA] interface vlan-interface 2
```

```
[SwitchA-Vlan-interface2] ip address 2.2.2.2 24
```

2) Configure Switch B

Enable Switch B to receive directed broadcasts.

```
<SwitchB> system-view
```

```
[SwitchB] ip forward-broadcast
```

Configure a static route to Host.

```
[SwitchB] ip route-static 1.1.1.1 24 2.2.2.2
```

Configure an IP address for VLAN-interface 2.

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] ip address 2.2.2.1 24
```

After the above configurations, if you ping the subnet broadcast address 2.2.2.255 on Host, the ping packets can be received by VLAN-interface 2 of Switch B. However, if you disable the **ip forward-broadcast** command, the ping packets cannot be received by the VLAN-interface 2 of Switch B.

Table of Contents

1 Voice VLAN Configuration	1-1
Voice VLAN Overview	1-1
How an IP Phone Works	1-1
How S3600 Series Switches Identify Voice Traffic	1-3
Setting the Voice Traffic Transmission Priority	1-4
Configuring Voice VLAN Assignment Mode of a Port	1-4
Support for Voice VLAN on Various Ports	1-4
Security Mode of Voice VLAN	1-6
Voice VLAN Configuration	1-6
Configuration Prerequisites	1-6
Configuring QoS Priority Settings for Voice Traffic on an Interface	1-6
Configuring the Voice VLAN to Operate in Automatic Voice VLAN Assignment Mode	1-7
Configuring the Voice VLAN to Operate in Manual Voice VLAN Assignment Mode	1-8
Displaying and Maintaining Voice VLAN	1-10
Voice VLAN Configuration Example	1-11
Voice VLAN Configuration Example (Automatic Voice VLAN Assignment Mode)	1-11
Voice VLAN Configuration Example (Manual Voice VLAN Assignment Mode)	1-12

1 Voice VLAN Configuration



Note

The Configuring QoS Priority Settings for Voice Traffic on an Interface is added. For the detailed configuration, refer to [Configuring QoS Priority Settings for Voice Traffic on an Interface](#).

When configuring voice VLAN, go to these sections for information you are interested in:

- [Voice VLAN Overview](#)
- [Voice VLAN Configuration](#)
- [Displaying and Maintaining Voice VLAN](#)
- [Voice VLAN Configuration Example](#)

Voice VLAN Overview

Voice VLANs are VLANs configured specially for voice traffic. By adding the ports connected with voice devices to voice VLANs, you can have voice traffic transmitted within voice VLANs and perform QoS-related configuration for voice traffic as required, thus ensuring the transmission priority of voice traffic and voice quality.

How an IP Phone Works

IP phones can convert analog voice signals into digital signals to enable them to be transmitted in IP-based networks. Used in conjunction with other voice devices, IP phones can offer large-capacity and low-cost voice communication solutions. As network devices, IP phones need IP addresses to operate properly in a network. An IP phone can acquire an IP address automatically or through manual configuration. The following part describes how an IP phone acquires an IP address automatically.



Note

The following part only describes the common way for an IP phone to acquire an IP address. The detailed process may vary by manufacture. Refer to the corresponding user manual for the detailed information.

When an IP phone applies for an IP address from a DHCP server, the IP phone can also apply for the following extensive information from the DHCP server through the Option184 field:

- IP address of the network call processor (NCP)
- IP address of the secondary NCP server
- Voice VLAN configuration

- Failover call routing

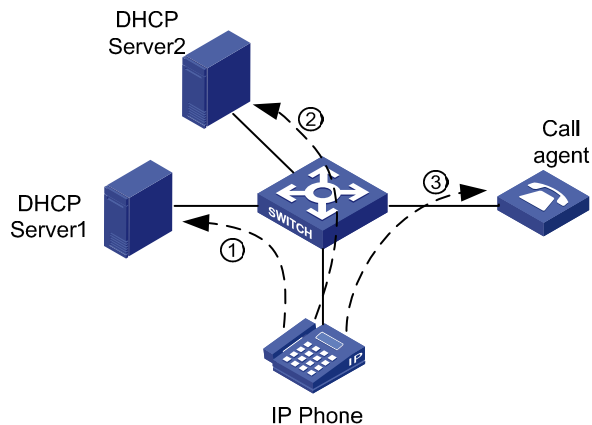


Note

Refer to DHCP Operation for information about the Option184 field.

Following describes the way an IP phone acquires an IP address.

Figure 1-1 Network diagram for IP phones



As shown in [Figure 1-1](#), the IP phone needs to work in conjunction with the DHCP server and the NCP to establish a path for voice data transmission. An IP phone goes through the following three phases to become capable of transmitting voice data.

- 2) After the IP phone is powered on, it sends an untagged DHCP request message containing four special requests in the Option 184 field besides the request for an IP address. The message is broadcast in the default VLAN of the receiving port. After receiving the DHCP request message, DHCP Server 1, which resides in the default VLAN of the port receiving the message, responds as follows:
 - If DHCP Server 1 does not support Option 184, it returns the IP address assigned to the IP phone but ignores the other four special requests in the Option 184 field. Without information about voice VLAN, the IP phone can only send untagged packets in the default VLAN of the port the IP phone is connected to. In this case, you need to manually configure the default VLAN of the port as a voice VLAN.



Note

In cases where an IP phone obtains an IP address from a DHCP server that does not support Option 184, the IP phone directly communicates through the gateway after it obtains an IP address. It does not go through the steps described below.

- If DHCP Server 1 supports Option 184, it returns the IP address assigned to the IP phone, the IP address of the NCP, the voice VLAN ID, and so on.

- 3) On acquiring the voice VLAN ID and NCP address from DHCP Server 1, the IP phone communicates with the specified NCP to download software, ignores the IP address assigned by DHCP Server 1, and sends a new DHCP request message carrying the voice VLAN tag to the voice VLAN.
- 4) After receiving the DHCP request, DHCP Server 2 residing in the voice VLAN assigns a new IP address to the IP phone and sends a tagged response message to the IP phone. After the IP phone receives the tagged response message, it sends voice data packets tagged with the voice VLAN tag to communicate with the voice gateway. In this case, the port connecting to the IP phone must be configured to allow the packets tagged with the voice VLAN tag to pass.

**Note**

- An untagged packet carries no VLAN tag.
 - A tagged packet carries the tag of a VLAN.
-

To set an IP address and a voice VLAN for an IP phone manually, just make sure that the voice VLAN ID to be set is consistent with that of the switch and the NCP is reachable to the IP address to be set.

How S3600 Series Switches Identify Voice Traffic

S3600 series Ethernet switches determine whether a received packet is a voice packet by checking its source MAC address against an organizationally unique identifier (OUI) list. If a match is found, the packet is considered as a voice packet. Ports receiving packets of this type will be added to the voice VLAN automatically for transmitting voice data.

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

**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. S3600 series Ethernet switches support OUI address mask configuration. You can adjust the matching depth of MAC address by setting different OUI address masks.

The following table lists the five default OUI addresses on S3600 series switches.

Table 1-1 Default OUI addresses pre-defined on the switch

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

Setting the Voice Traffic Transmission Priority

In order to improve transmission quality of voice traffic, the switch by default re-marks the priority of the traffic in the voice VLAN as follows:

- Set the CoS (802.1p) priority to 6.
- Set the DSCP value to 46.

Configuring Voice VLAN Assignment Mode of a Port

A port can work in automatic voice VLAN assignment mode or manual voice VLAN assignment mode. You can configure the voice VLAN assignment mode for a port according to data traffic passing through the port.

Processing mode of untagged packets sent by IP voice devices

- Automatic voice VLAN assignment 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. The voice VLAN uses the aging mechanism to maintain the number of ports in the voice VLAN. When the aging timer expires, the ports whose OUI addresses are not updated (that is, no voice traffic passes) will be removed from the voice VLAN. In voice VLAN assignment automatic mode, ports can not be added to or removed from a voice VLAN manually.
- Manual voice VLAN assignment mode: In this mode, you need to add a port to a voice VLAN or remove a port from a voice VLAN manually.

Processing mode of tagged packets sent by IP voice devices

Tagged packets from IP voice devices are forwarded based on their tagged VLAN IDs, whether the automatic or manual voice VLAN assignment mode is used.



Caution

If the voice traffic transmitted by an IP voice device carries VLAN tags, and 802.1x authentication and guest VLAN is enabled on the port which the IP voice device is connected to, 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.

Support for Voice VLAN on Various Ports

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

For different types of IP phones, the support for voice VLAN varies with port types and port configuration. For IP phones capable of acquiring IP address and voice VLAN automatically, the support for voice VLAN is described in [Table 1-2](#).

Table 1-2 Matching relationship between port types and voice devices capable of acquiring IP address and voice VLAN automatically

Voice VLAN assignment mode	Voice traffic type	Port type	Supported or not
Automatic	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, and the default VLAN is 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	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 and the voice VLAN.
		Hybrid	Supported Make sure the default VLAN of the port exists and is not a voice VLAN, and the default VLAN and the voice VLAN is in the list of the tagged VLANs whose traffic is permitted by the access port.
	Untagged 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.

IP phones acquiring IP address and voice VLAN through manual configuration can forward only tagged traffic, so the matching relationship is relatively simple, as shown in [Table 1-3](#):

Table 1-3 Matching relationship between port types and voice devices acquiring voice VLAN through manual configuration

Voice VLAN assignment mode	Port type	Supported or not
Automatic	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, and the default VLAN is in the list of the tagged VLANs whose traffic is permitted by the access port.
Manual	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, and the default VLAN and the voice VLAN is in the list of the tagged VLANs whose traffic is permitted by the access port.

Security Mode of Voice VLAN

On S3600 series Ethernet switches, a voice VLAN can operate in the security mode. Voice VLANs operating in this mode only permit voice data, enabling you to perform voice traffic-specific priority configuration. With the security mode disabled, both voice data and service data can be transmitted in a voice VLAN.

Voice VLAN Configuration

Configuration Prerequisites

- Create the corresponding VLAN before configuring a voice VLAN.
- VLAN 1 (the default VLAN) cannot be configured as a voice VLAN.

Configuring QoS Priority Settings for Voice Traffic on an Interface

In voice VLAN applications, you can improve the quality of voice traffic by configuring the appropriate QoS priority settings, including the Class of Service (CoS) and Differentiated Services Code Point (DSCP) values, for voice traffic. Voice traffic carries its own QoS priority settings. You can configure the device either to modify or not to modify the QoS priority settings carried by incoming voice traffic.

Follow these steps to configure QoS priority settings for voice traffic:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the interface to trust the QoS priority settings in incoming voice traffic, that is, not to modify the CoS and DSCP values marked for incoming traffic of the voice VLAN	voice vlan qos trust	Required Use either command By default, an interface modifies the CoS value and the DSCP value marked for voice VLAN traffic into 6 and 46 respectively.
Configure the interface to modify the CoS and DSCP values marked for incoming traffic of the voice VLAN into specified values	voice vlan qos <i>cos-value</i> <i>dscp-value</i>	The voice vlan qos command and the voice vlan qos trust command can overwrite each other, whichever is configured last.



Note

Configure the QoS priority settings for voice traffic on an interface before enabling voice VLAN on the interface. If the configuration order is reversed, your priority trust setting will fail.

Configuring the Voice VLAN to Operate in Automatic Voice VLAN Assignment Mode

Follow these steps to configure a voice VLAN to operate in automatic voice VLAN assignment mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set an OUI address that can be identified by the voice VLAN	voice vlan mac-address <i>oui</i> mask <i>oui-mask</i> [description <i>text</i>]	Optional By default, the switch determines the voice traffic according to the default OUI address.
Enable the voice VLAN security mode	voice vlan security enable	Optional By default, the voice VLAN security mode is enabled.
Set the voice VLAN aging timer	voice vlan aging <i>minutes</i>	Optional The default aging timer is 1440 minutes.
Enable the voice VLAN function globally	voice vlan <i>vlan-id</i> enable	Required
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	Required
Enable the voice VLAN function on a port	voice vlan enable	Required By default, voice VLAN is disabled.

To do...	Use the command...	Remarks
Enable the voice VLAN legacy function on the port	voice vlan legacy	Optional By default, voice VLAN legacy is disabled.
Set the voice VLAN assignment mode of the port to automatic	voice vlan mode auto	Optional The default voice VLAN assignment mode on a port is automatic.



Caution

- A port working in automatic voice VLAN assignment mode cannot be assigned to the voice VLAN manually. Therefore, if a VLAN is configured as the voice VLAN and a protocol-based VLAN at the same time, the protocol-based VLAN function cannot be bound with the port. For information about protocol-based VLANs, refer to *VLAN Configuration* in this manual.
- For a port operating in automatic voice VLAN assignment mode, its default VLAN cannot be configured as the 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 voice VLAN assignment mode to the local devices as well as the IRF of the voice VLAN but does so immediately after the restart or the changes.

Configuring the Voice VLAN to Operate in Manual Voice VLAN Assignment Mode

Follow these steps to configure a voice VLAN to operate in manual voice VLAN assignment mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set an OUI address that can be identified by the voice VLAN	voice vlan mac-address <i>oui mask oui-mask</i> [description text]	Optional Without this address, the default OUI address is used.
Enable the voice VLAN security mode	voice vlan security enable	Optional By default, the voice VLAN security mode is enabled.
Set the voice VLAN aging timer	voice vlan aging <i>minutes</i>	Optional The default aging timer is 1,440 minutes.
Enable the voice VLAN function globally	voice vlan vlan-id enable	Required

To do...			Use the command...	Remarks
Enter port view			interface <i>interface-type</i> <i>interface-number</i>	Required
Enable voice VLAN on a port			voice vlan enable	Required By default, voice VLAN is disabled on a port.
Enable the voice VLAN legacy function on the port			voice vlan legacy	Optional By default, voice VLAN legacy is disabled.
Set voice VLAN assignment mode on a port to manual			undo voice vlan mode auto	Required The default voice VLAN assignment mode on a port is automatic.
Quit to system view			quit	—
Add a port in manual voice VLAN assignment mode to the voice VLAN	Access port	Enter VLAN view	vlan <i>vlan-id</i>	Required By default, all the ports belong to VLAN 1.
		Add the port to the VLAN	port <i>interface-list</i>	
	Trunk or Hybrid port	Enter port view	interface <i>interface-type</i> <i>interface-num</i>	
		Add the port to the VLAN	port trunk permit vlan <i>vlan-id</i> port hybrid vlan <i>vlan-id</i> { tagged untagged }	
		Configure the voice VLAN to be the default VLAN of the port	port trunk pvid vlan <i>vlan-id</i> port hybrid pvid vlan <i>vlan-id</i>	Optional Refer to Table 1-2 to determine whether or not this operation is needed.



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.
- The voice VLAN legacy feature realizes the communication between H3C device and other vendor's voice device by automatically adding the voice VLAN tag to the voice data coming from other vendors' voice device. The **voice vlan legacy** command can be executed before voice VLAN is enabled globally and on a port, but it takes effect only after voice VLAN is enabled globally and on the port.



Note

To assign a trunk port or a hybrid port to the voice VLAN, refer to *VLAN Configuration* of this manual for the related command.

Displaying and Maintaining Voice VLAN

To do...	Use the command...	Remarks
Display information about the ports on which voice VLAN configuration fails	display voice vlan error-info	In any view
Display the voice VLAN configuration status	display voice vlan status	
Display the OUI list	display voice vlan oui	
Display the ports operating in the voice VLAN	display vlan <i>vlan-id</i>	

Voice VLAN Configuration Example

Voice VLAN Configuration Example (Automatic Voice VLAN Assignment Mode)

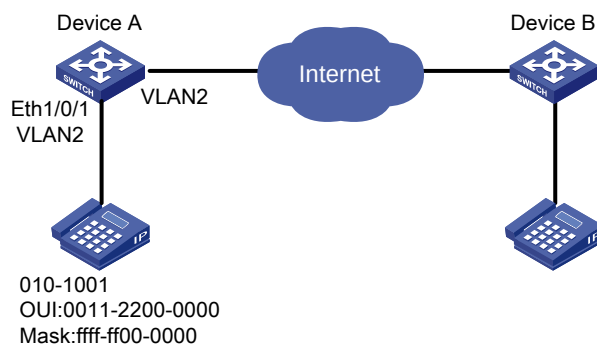
Network requirements

Create a voice VLAN and configure it to operate in automatic voice VLAN assignment mode to enable the port to which an IP phone is connected to join or exit the voice VLAN automatically and voice traffic to be transmitted within the voice VLAN.

- Create VLAN 2 and configure it as the voice VLAN, with the aging timer being 100 minutes.
- The IP phone sends tagged packets. It is connected to Ethernet 1/0/1, a hybrid port, with VLAN 6 being its default VLAN. Set this port to operate in automatic voice VLAN assignment mode.
- You need to add a user-defined OUI address 0011-2200-000, with the mask being ffff-ff00-0000 and the description string being "test".

Network diagram

Figure 1-2 Network diagram for voice VLAN configuration (automatic voice VLAN assignment mode)



Configuration procedure

Create VLAN 2 and VLAN 6.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] vlan 6
[DeviceA-vlan6] quit
```

Set the voice VLAN aging timer.

```
[DeviceA] voice vlan aging 100
```

Add a user-defined OUI address 0011-2200-000 and set the description string to "test".

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

Enable the voice VLAN function globally.

```
[DeviceA] voice vlan 2 enable
```

Configure the voice VLAN to operate in automatic voice VLAN assignment mode on Ethernet 1/0/1. This operation is optional. By default, a port operates in automatic voice VLAN assignment mode.

```
[DeviceA] interface Ethernet 1/0/1
[DeviceA-Ethernet1/0/1] voice vlan mode auto
```

Configure Ethernet 1/0/1 as a hybrid port.

```
[DeviceA-Ethernet1/0/1] port link-type hybrid
```

Configure VLAN 6 as the default VLAN of Ethernet 1/0/1, and configure Ethernet 1/0/1 to permit packets with the tag of VLAN 6.

```
[DeviceA-Ethernet1/0/1] port hybrid pvid vlan 6
```

```
[DeviceA-Ethernet1/0/1] port hybrid vlan 6 tagged
```

Enable the voice VLAN function on Ethernet 1/0/1.

```
[DeviceA-Ethernet1/0/1] voice vlan enable
```

Voice VLAN Configuration Example (Manual Voice VLAN Assignment Mode)

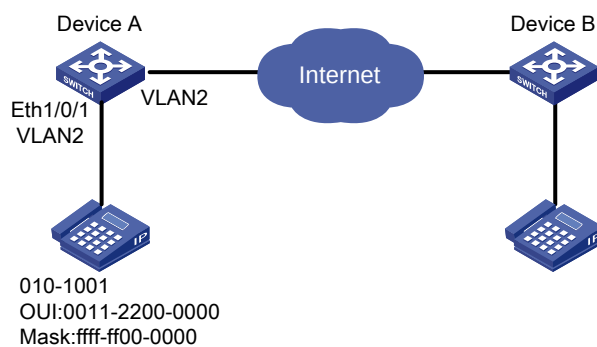
Network requirements

Create a voice VLAN and configure it to operate in manual voice VLAN assignment mode. Add the port to which an IP phone is connected to the voice VLAN to enable voice traffic to be transmitted within the voice VLAN.

- Create VLAN 2 and configure it as a voice VLAN. Set the voice VLAN to operate in security mode
- The IP phone sends untagged packets. It is connected to Ethernet 1/0/1, a hybrid port. Set this port to operate in manual voice VLAN assignment mode.
- You need to add a user-defined OUI address 0011-2200-000, with the mask being ffff-ff00-0000 and the description string being “test”.

Network diagram

Figure 1-3 Network diagram for voice VLAN configuration (manual voice VLAN assignment mode)



Configuration procedure

Enable the security mode for the voice VLAN so that the ports in the voice VLAN permit valid voice packets only. This operation is optional. The security mode is enabled by default.

```
<DeviceA> system-view
```

```
[DeviceA] voice vlan security enable
```

Add a user-defined OUI address 0011-2200-000 and set the description string to “test”.

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

Create VLAN 2 and configure it as a voice VLAN.

```
[DeviceA] vlan 2
```

```
[DeviceA-vlan2] quit
```

```
[DeviceA] voice vlan 2 enable
```

Configure Ethernet 1/0/1 to operate in manual voice VLAN assignment mode.

```
[DeviceA] interface Ethernet 1/0/1
```

```
[DeviceA-Ethernet1/0/1] undo voice vlan mode auto
```

Configure Ethernet 1/0/1 as a hybrid port.

```
[DeviceA-Ethernet1/0/1] port link-type hybrid
```

Configure the voice VLAN as the default VLAN of Ethernet 1/0/1, and add the voice VLAN to the list of untagged VLANs whose traffic is permitted by the port.

```
[DeviceA-Ethernet1/0/1] port hybrid pvid vlan 2
```

```
[DeviceA-Ethernet1/0/1] port hybrid vlan 2 untagged
```

Enable the voice VLAN function on Ethernet 1/0/1.

```
[DeviceA-Ethernet1/0/1] voice vlan enable
```

Verification

Display the OUI addresses, the corresponding OUI address masks and the corresponding description strings that the system supports.

```
<DeviceA> display voice vlan oui
```

Oui Address	Mask	Description
0003-6b00-0000	ffff-ff00-0000	Cisco phone
000f-e200-0000	ffff-ff00-0000	H3C Aolynk phone
0011-2200-0000	ffff-ff00-0000	test
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3Com phone

Display the status of the current voice VLAN.

```
<DeviceA> display voice vlan status
```

```
Voice Vlan status: ENABLE
```

```
Voice Vlan ID: 2
```

```
Voice Vlan security mode: Security
```

```
Voice Vlan aging time: 1440 minutes
```

```
Current voice vlan enabled port mode:
```

PORT	MODE

Ethernet1/0/1	MANUAL

Table of Contents

1 GVRP Configuration	1-1
Introduction to GVRP	1-1
GARP.....	1-1
GVRP.....	1-4
Protocol Specifications	1-4
GVRP Configuration.....	1-4
GVRP Configuration Tasks	1-4
Enabling GVRP	1-4
Configuring GVRP Timers	1-5
Configuring GVRP Port Registration Mode	1-6
Displaying and Maintaining GVRP.....	1-7
GVRP Configuration Example	1-7
GVRP Configuration Example	1-7

1 GVRP Configuration

When configuring GVRP, go to these sections for information you are interested in:

- [Introduction to GVRP](#)
- [GVRP Configuration](#)
- [Displaying and Maintaining GVRP](#)
- [GVRP Configuration Example](#)

Introduction to GVRP

GARP VLAN registration protocol (GVRP) is an implementation of generic attribute registration protocol (GARP). GARP is introduced as follows.

GARP

The generic attribute registration protocol (GARP), provides a mechanism that allows participants in a GARP application to distribute, propagate, and register with other participants in a bridged LAN the attributes specific to the GARP application, such as the VLAN or multicast attribute.

GARP itself does not exist on a device as an entity. GARP-compliant application entities are called GARP applications. One example is GVRP. When a GARP application entity is present on a port on your device, this port is regarded a GARP application entity.

GARP messages and timers

1) GARP messages

GARP members communicate with each other through the messages exchanged between them. The messages performing important functions for GARP fall into three types: Join, Leave and LeaveAll.

- When a GARP entity wants its attribute information to be registered on other devices, it sends Join messages to these devices. A GARP entity also sends Join messages when it receives Join messages from other entities or it wants some of its statically configured attributes to be registered on other GARP entities.
- When a GARP entity wants some of its attributes to be deregistered on other devices, it sends Leave messages to these devices. A GARP entity also sends Leave messages when it receives Leave messages from other entities for deregistering some attributes or it has some attributes statically deregistered.
- Once a GARP entity is launched, the LeaveAll timer is triggered at the same time. The GARP entity sends out LeaveAll messages after the timer times out. LeaveAll messages deregister all the attributes, through which the attribute information of the entity can be registered again on the other GARP entities.

Leave messages, LeaveAll messages, together with Join messages ensure attribute information can be deregistered and re-registered.

Through message exchange, all the attribute information to be registered can be propagated to all the GARP-enabled switches in the same LAN.

2) GARP timers

Timers determine the intervals of sending different types of GARP messages. GARP defines four timers to control the period of sending GARP messages.

- **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 make sure the devices can receive Join messages, each Join message is sent twice. If the first Join message sent is not responded for a specific period, a second one is sent. The period is determined by this timer.
- **Leave:** When a GARP entity expects to deregister a piece of attribute information, it sends out a Leave message. Any GARP entity receiving this message starts its Leave timer, and deregisters 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.



Note

- The settings of GARP timers apply to all GARP applications, such as GVRP, on a LAN.
 - Unlike other three timers, which are set on a port basis, the LeaveAll timer is set in system view and takes effect globally.
 - A GARP application entity may send LeaveAll messages at the interval set by its LeaveAll timer or the LeaveAll timer on another device on the network, whichever is smaller. This is because each time a device on the network receives a LeaveAll message it resets its LeaveAll timer.
-

Operating mechanism of GARP

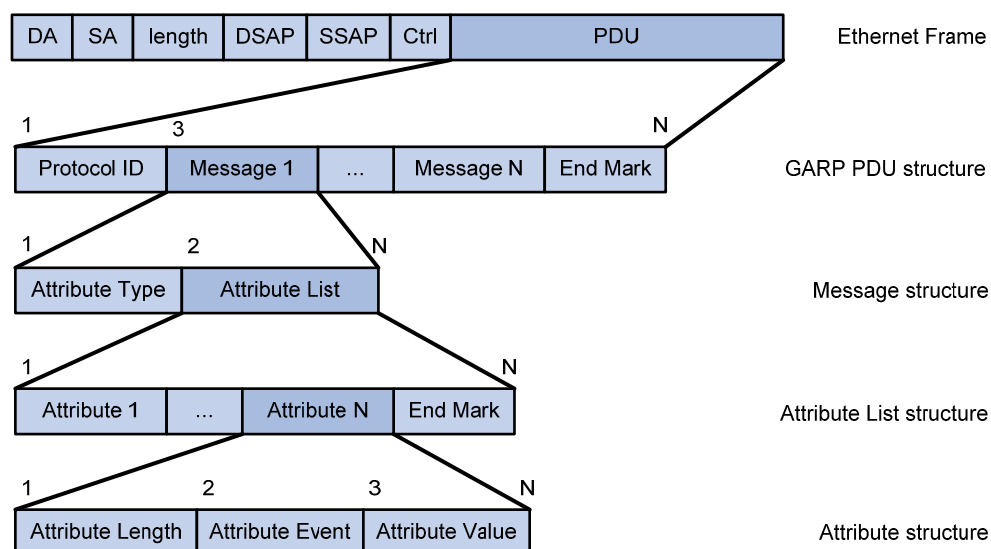
Through the mechanism of GARP, the configuration information on a GARP member will be propagated within the whole LAN. A GARP member can be a terminal workstation or a bridge; it instructs other GARP members to register/deregister its attribute information by declaration/recant, and register/deregister other GARP member's attribute information according to other member's declaration/recant. When a port receives an attribute declaration, the port will register this attribute. When a port receives an attribute recant, the port will deregister this attribute.

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.

GARP message format

The GARP packets are in the following format:

Figure 1-1 Format of GARP packets



The following table describes the fields of a GARP packet.

Table 1-1 Description of GARP 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 (in bytes)
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	For GVRP packets, the value of this field is the VLAN ID; however, for LeaveAll messages, this field is invalid.
End Mark	End mark of an GARP PDU	The value of this field is fixed to 0x00.

GVRP

As an implementation of GARP, GARP VLAN registration protocol (GVRP) maintains dynamic VLAN registration information and propagates the information to the other switches through GARP.

With GVRP enabled on a device, the VLAN registration information received by the device from other devices is used to dynamically update the local VLAN registration information, including the information about the VLAN members, the ports through which the VLAN members can be reached, and so on. The device also propagates the local VLAN registration information to other devices so that all the devices in the same LAN can have the same VLAN information. VLAN registration information propagated by GVRP includes static VLAN registration information, which is manually configured locally on each device, and dynamic VLAN registration information, which is received from other devices.

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

- Normal. A port in this mode can dynamically register/deregister VLANs and propagate dynamic/static VLAN information.
- Fixed. A port in this mode cannot register/deregister VLANs dynamically. It only propagates static VLAN information. Besides, the port permits only static VLANs, that is, it propagates only static VLAN information to the other GARP members.
- Forbidden. A port in this mode cannot register/deregister VLANs dynamically. It permits only the default VLAN (namely, VLAN 1), that is, the port propagates only the information about VLAN 1 to the other GARP members.

Protocol Specifications

GVRP is defined in IEEE 802.1Q standard.

GVRP Configuration

GVRP Configuration Tasks

Complete the following tasks to configure GVRP:

Task	Remarks
Enabling GVRP	Required
Configuring GVRP Timers	Optional
Configuring GVRP Port Registration Mode	Optional

Enabling GVRP

Configuration Prerequisite

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

Configuration procedure

Follow these steps to enable GVRP:

To do ...	Use the command ...	Remarks
Enter system view	system-view	—
Enable GVRP globally	gvrp	Required By default, GVRP is disabled globally.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable GVRP on the port	gvrp	Required By default, GVRP is disabled on the port.



Note

- After you enable GVRP on a trunk port, you cannot change the port to a different type.
- Use the **port trunk permit all** command to permit the traffic of all dynamically registered VLANs to pass through a trunk port with GVRP enabled.

Configuring GVRP Timers

Follow these steps to configure GVRP timers:

To do ...	Use the command ...	Remarks
Enter system view	system-view	—
Configure the LeaveAll timer	garp timer leaveall <i>timer-value</i>	Optional By default, the LeaveAll timer is set to 1,000 centiseconds.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the Hold, Join, and Leave timers	garp timer { hold join leave } <i>timer-value</i>	Optional By default, the Hold, Join, and Leave timers are set to 10, 20, and 60 centiseconds respectively.

Note that:

- The setting of each timer must be a multiple of 5 (in centiseconds).
- 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 1-2 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.
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

**Note**

The following are recommended GVRP timer settings:

- GARP hold timer: 100 centiseconds (1 second)
- GARP Join timer: 600 centiseconds (6 seconds)
- GARP Leave timer: 3000 centiseconds (30 seconds)
- GARP LeaveAll timer: 120000 centiseconds (2 minutes)

Configuring GVRP Port Registration Mode

Follow these steps to configure GVRP port registration mode:

To do ...	Use the command ...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure GVRP port registration mode	gvrp registration { fixed forbidden normal }	Optional By default, GVRP port registration mode is normal.

Displaying and Maintaining GVRP

To do ...	Use the command ...	Remarks
Display GARP statistics	display garp statistics [interface <i>interface-list</i>]	Available in any view
Display the settings of the GARP timers	display garp timer [interface <i>interface-list</i>]	
Display GVRP statistics	display gvrp statistics [interface <i>interface-list</i>]	
Display the global GVRP status	display gvrp status	
Clear GARP statistics	reset garp statistics [interface <i>interface-list</i>]	

GVRP Configuration Example

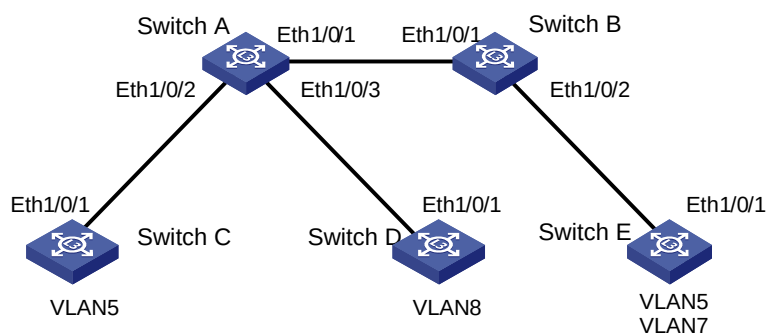
GVRP Configuration Example

Network requirements

- Enable GVRP on all the switches in the network so that the VLAN configurations on Switch C and Switch E can be applied to all switches in the network, thus implementing dynamic VLAN information registration and refresh.
- By configuring the GVRP registration modes of specific Ethernet ports, you can enable the corresponding VLANs in the switched network to communicate with each other.

Network diagram

Figure 1-2 Network diagram for GVRP configuration



Configuration procedure

1) Configure Switch A

Enable GVRP globally.

```
<SwitchA> system-view
```

```
[SwitchA] gvrp
```

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

```
[SwitchA] interface Ethernet 1/0/1
```

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



```
[SwitchA-Ethernet1/0/1] port trunk permit vlan all

# Enable GVRP on Ethernet1/0/1.

[SwitchA-Ethernet1/0/1] gvrp
[SwitchA-Ethernet1/0/1] quit

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

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

# Enable GVRP on Ethernet1/0/2.

[SwitchA-Ethernet1/0/2] gvrp
[SwitchA-Ethernet1/0/2] quit

# Configure Ethernet1/0/3 to be a trunk port and to permit the packets of all the VLANs.

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

# Enable GVRP on Ethernet1/0/3.

[SwitchA-Ethernet1/0/3] gvrp
[SwitchA-Ethernet1/0/3] quit

2) Configure Switch B

# The configuration procedure of Switch B is similar to that of Switch A and is thus omitted.

3) Configure Switch C

# Enable GVRP on Switch C, which is similar to that of Switch A and is thus omitted.

# Create VLAN 5.

[SwitchC] vlan 5
[SwitchC-vlan5] quit

4) Configure Switch D

# Enable GVRP on Switch D, which is similar to that of Switch A and is thus omitted.

# Create VLAN 8.

[SwitchD] vlan 8
[SwitchD-vlan8] quit

5) Configure Switch E

# Enable GVRP on Switch E, which is similar to that of Switch A and is thus omitted.

# Create VLAN 5 and VLAN 7.

[SwitchE] vlan 5
[SwitchE-vlan5] quit
[SwitchE] vlan 7
[SwitchE-vlan7] quit

6) Display the VLAN information dynamically registered on Switch A, Switch B, and Switch E.

# Display the VLAN information dynamically registered on Switch A.

[SwitchA] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
```

```

5, 7, 8,

# Display the VLAN information dynamically registered on Switch B.
[SwitchB] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 7, 8,

# Display the VLAN information dynamically registered on Switch E.
[SwitchE] display vlan dynamic
Total 1 dynamic VLAN exist(s).
The following dynamic VLANs exist:
8

7) Configure Ethernet1/0/1 on Switch E to operate in fixed GVRP registration mode and display the
VLAN information dynamically registered on Switch A, Switch B, and Switch E.

# Configure Ethernet1/0/1 on Switch E to operate in fixed GVRP registration mode.
[SwitchE] interface Ethernet 1/0/1
[SwitchE-Ethernet1/0/1] gvrp registration fixed

# Display the VLAN information dynamically registered on Switch A.
[SwitchA] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 7, 8,

# Display the VLAN information dynamically registered on Switch B.
[SwitchB] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 7, 8,

# Display the VLAN information dynamically registered on Switch E.
[SwitchE-Ethernet1/0/1] display vlan dynamic
No dynamic vlans exist!

8) Configure Ethernet1/0/1 on Switch E to operate in forbidden GVRP registration mode and display
the VLAN registration information dynamically registered on Switch A, Switch B, and Switch E.

# Configure Ethernet1/0/1 on Switch E to operate in forbidden GVRP registration mode.
[SwitchE-Ethernet1/0/1] gvrp registration forbidden

# Display the VLAN information dynamically registered on Switch A.
[SwitchA] display vlan dynamic
Total 2 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 8,

# Display the VLAN information dynamically registered on Switch B.
[SwitchB] display vlan dynamic
Total 2 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 8,

```

Display the VLAN information dynamically registered on Switch E.

```
[SwitchE] display vlan dynamic
```

```
No dynamic vlans exist!
```

Table of Contents

1 Port Basic Configuration	1-1
Ethernet Port Configuration	1-1
Initially Configuring a Port	1-1
Configuring Port Auto-Negotiation Speed	1-2
Limiting Traffic on individual Ports.....	1-3
Configuring Flow Control on a Port	1-3
Duplicating the Configuration of a Port to Other Ports	1-4
Configuring Loopback Detection for an Ethernet Port.....	1-5
Enabling Loopback Test	1-7
Enabling the System to Test Connected Cable	1-8
Configuring the Interval to Perform Statistical Analysis on Port Traffic.....	1-8
Enabling Giant-Frame Statistics Function	1-9
Disabling Up/Down Log Output on a Port	1-9
Configuring Storm Control on a Port	1-10
Setting the Port State Change Delay	1-11
Displaying and Maintaining Basic Port Configuration	1-12
Ethernet Port Configuration Example	1-12
Troubleshooting Ethernet Port Configuration	1-13

1 Port Basic Configuration

When performing basic port configuration, go to these sections for information you are interested in:

- [Ethernet Port Configuration](#)
- [Ethernet Port Configuration Example](#)
- [Troubleshooting Ethernet Port Configuration](#)



Note

- The configuration of flow control on Ethernet ports is added. For the detailed configuration, refer to [Configuring Flow Control on a Port](#).
- The configuration of loopback port auto-shutdown and loopback detection on Ethernet ports in bulk is added. For the detailed configuration, refer to [Configuring Loopback Detection for an Ethernet Port](#).
- The configuration of the support for the kbps keyword in storm suppression thresholds is added. For the detailed configuration, refer to [Configuring Storm Control on a Port](#).

Ethernet Port Configuration

Initially Configuring a Port

Follow these steps to initially configure a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the Ethernet port	undo shutdown	Optional By default, the port is enabled. Use the shutdown command to disable the port.
Set the description string for the Ethernet port	description <i>text</i>	Optional By default, the description string of an Ethernet port is null.
Set the duplex mode of the Ethernet port	duplex { auto full half }	Optional The optical interface of an SFP port does not support the half keyword By default, the duplex mode of the port is auto (auto-negotiation).

To do...	Use the command...	Remarks
Set the speed of the Ethernet port	speed { 10 100 1000 auto }	Optional - By default, the speed of an Ethernet port is determined through auto-negotiation (the auto keyword). - Use the 1000 keyword for Gigabit Ethernet ports only. - The optical interface of an SFP port does not support the 10 or 100 keyword
Set the medium dependent interface (MDI) mode of the Ethernet port	mdi { across auto normal }	Optional By default, the MDI mode of an Ethernet port is auto .
Set the maximum frame size allowed on the Ethernet port to 9,216 bytes	jumboframe enable	Optional By default, the maximum frame size allowed on an Ethernet is 9,216 bytes. To set the maximum frame size allowed on an Ethernet port to 1,536 bytes, use the undo jumboframe enable command.

Configuring Port Auto-Negotiation Speed

You can configure an auto-negotiation speed for a port by using the **speed auto** command.

Take a 10/100/1000 Mbps port as an example.

- If you expect that 10 Mbps is the only available auto-negotiation speed of the port, you just need to configure **speed auto 10**.
- If you expect that 10 Mbps and 100 Mbps are the available auto-negotiation speeds of the port, you just need to configure **speed auto 10 100**.
- If you expect that 10 Mbps and 1000 Mbps are the available auto-negotiation speeds of the port, you just need to configure **speed auto 10 1000**.

Follow these steps to configure auto-negotiation speeds for a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the available auto-negotiation speed(s) for the port	speed auto [10 100 1000]*	Optional - By default, the port speed is determined through auto-negotiation. - Use the 1000 keyword for Gigabit Ethernet ports only.



Note

- Only ports on the front panel of the device support the auto-negotiation speed configuration feature. And ports on the extended interface card do not support this feature currently.
- After you configure auto-negotiation speed(s) for a port, if you execute the **undo speed** command or the **speed auto** command, the auto-negotiation speed setting of the port restores to the default setting.
- The effect of executing **speed auto 10 100 1000** equals to that of executing **speed auto**, that is, the port is configured to support all the auto-negotiation speeds: 10 Mbps, 100 Mbps, and 1000 Mbps.

Limiting Traffic on individual Ports

By performing the following configurations, you can limit the incoming broadcast/multicast/unknown unicast 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.

Follow these steps to limit traffic on port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Limit broadcast traffic received on each port	broadcast-suppression { <i>ratio</i> pps <i>max-pps</i> }	Optional By default, the switch does not suppress broadcast traffic.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Limit broadcast traffic received on the current port	broadcast-suppression { <i>ratio</i> pps <i>max-pps</i> }	Optional By default, the switch does not suppress broadcast traffic.
Limit multicast traffic received on the current port	multicast-suppression { <i>ratio</i> pps <i>max-pps</i> }	Optional By default, the switch does not suppress multicast traffic.
Limit unknown unicast traffic received on the current port	unicast-suppression { <i>ratio</i> pps <i>max-pps</i> }	Optional By default, the switch does not suppress unknown unicast traffic.

Configuring Flow Control on a Port

In situations where the receiving port is unable to process received frames, you can use the flow control function to enable the receiving port to inform the sending port to stop sending the frames for a while, thus preventing frames from being dropped.

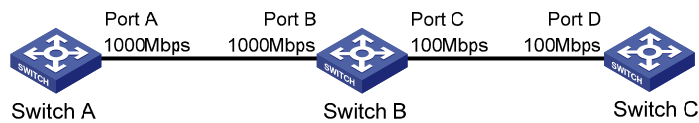
The flow control function is implemented on a port by sending and receiving pause frames. Flow control operates in one of the following two modes on a port:

- TxRx mode, where the port can receive and send pause frames.

- Rx mode, where the port only can receive pause frames.

In [Figure 1-1](#), when both Port A and Port B forward packets at 1000 Mbps, Port C is congested. To avoid packet loss, you can enable flow control on Port A, and Port B.

Figure 1-1 Configure flow control on a port



Configure flow control in TxRx mode on Port B, and flow control in Rx mode on Port A:

- When congestions occur on Port C, Switch B buffers the frames. When the amount of the buffered frames exceeds a certain value, Switch B can realize that the traffic from Port B to Port C is too heavy and exceeds the forwarding capacity of Port C. As a result, Port B in TxRx mode sends pause frames to Port A to inform Port A to suspend packet sending.
- Upon receiving the pause frames from Port B, Port A suspends sending packets to Port B.
- When part of the buffered frames of Switch B are sent out Port C and the amount of the buffered frames drops to a certain level, Port B sends traffic recovery frames to Port A to inform Port A to resume frame sending. Thus, packet loss on Port C is avoided.

Follow these steps to configure flow control on a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure flow control to operate in TxRx mode	flow-control	Required Use either command
Configure flow control to operate in Rx mode	flow-control no-pauseframe-sending	By default, flow control is disabled on a port.



Caution

Reflector ports and fabric ports do not support the **flow-control no-pauseframe-sending** command.

Duplicating the Configuration of a Port to Other Ports

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

Specifically, the following types of port configuration can be duplicated from one port to other ports: VLAN configuration, protocol-based VLAN configuration, LACP configuration, QoS configuration, GARP configuration, STP configuration and initial port configuration. Refer to the command manual for the configurations that can be duplicated.

Follow these steps to duplicate the configuration of a port to specific ports:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Duplicate the configuration of a port to specific ports	copy configuration source { <i>interface-type interface-number</i> aggregation-group source-agg-id } destination { <i>interface-list</i> [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.

Configuring Loopback Detection for an Ethernet Port

Loopback detection is used to monitor if a port of a switch is looped back.

After you enable loopback detection on Ethernet ports, the switch can monitor if an external loopback occurs on them. If there is a loopback port found, the switch will deal with the loopback port according to your configuration.

- 1) If a loop is found on an access port, the system will set the port to the **block** state (ports in this state cannot forward data packets), send log and trap messages to the terminal, and remove the corresponding MAC forwarding entry.
 - If you have additionally enabled the loopback port auto-shutdown function on the port, the system will shut down the port, and send log and trap messages to the terminal. After the loop is removed, you need to use the **undo shutdown** command to bring up the port.
 - If you have not enabled the loopback port auto-shutdown function on the port, the port will automatically resume the normal forwarding state after the loop is removed.
- 2) If a loop is found on a trunk or hybrid port, the system sends log and trap messages to the terminal. If you have additionally enabled the loopback port control function or the loopback port auto-shutdown function, the system will deal with the port accordingly:
 - If the loopback port control function is enabled on the port, the system will set the port to the **block** state (ports in this state cannot forward data packets), send log and trap messages to the terminal, and remove the corresponding MAC forwarding entry. After the loop is removed, the port will automatically resume the normal forwarding state.
 - If the loopback port auto-shutdown function is enabled on the port, the system will shut down the port and send log and trap messages to the terminal. After the loop is removed, you need to use the **undo shutdown** command to bring up the port.

**Note**

You cannot enable both the loopback port control function and the loopback port auto-shutdown function on a port. If you do so, the function configured later will take effect.

Table 1-1 Configure loopback detection for Ethernet port(s)

Operation	Command	Remarks
Enter system view	system-view	—
Enable loopback detection globally	loopback-detection enable	Optional By default, the global loopback detection function is enabled if the device boots with the default configuration file (config.def); if the device boots with null configuration, this function is disabled.
Enable loopback detection on the specified ports in bulk	loopback-detection interface-list enable	Optional By default, the loopback detection function is enabled on ports if the device boots with the default configuration file (config.def); if the device boots with null configuration, this function is disabled.
Set the interval for performing port loopback detection	loopback-detection interval-time time	Optional The default 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, the loopback detection function is enabled on ports if the device boots with the default configuration file (config.def); if the device boots with null configuration, this function is disabled.
Enable loopback port control on the trunk or hybrid port	loopback-detection control enable	Optional By default, the loopback port control function is enabled on ports if the device boots with the default configuration file (config.def); if the device boots with null configuration, this function is disabled.
Enable the loopback port auto-shutdown function	loopback-detection shutdown enable	Optional By default, the loopback port auto-shutdown function is enabled on ports if the device boots with the default configuration file (config.def); if the device boots with null configuration, this function is disabled.

Operation	Command	Remarks
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.



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.
- The **loopback-detection control enable** command and the **loopback-detection per-vlan enable** command are not applicable to access ports. When the link type of a non-access port changes to access, the two commands already configured on the port become invalid automatically.

Enabling 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.

Follow these steps to enable loopback test:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type interface-number</i>	—
Enable loopback test	loopback { external internal }	Required



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.

Note that:

- 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.

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.

Follow these steps to enable the system to test connected cables:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the system to test connected cables	virtual-cable-test	Required



Note

SFP ports do not support this function.

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
```

Follow these steps to set the interval to perform statistical analysis on port traffic:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Set the interval to perform statistical analysis on port traffic	flow-interval <i>interval</i>	Optional By default, this interval is 300 seconds.

Enabling Giant-Frame Statistics Function

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

Follow these steps to enable the giant-frame statistics function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the giant-frame statistics function	giant-frame statistics enable	Required By default, the giant-frame statistics function is not enabled.

Disabling Up/Down Log Output on a Port

An Ethernet port has three physical link statuses: Up, Down, and Administratively Down. For status transition conditions, refer to the description of the **display brief interface** command in *Basic Port Configuration Command*.

When the physical link status of an Ethernet port changes between Up and Down or Up and Administratively Down, the switch will generate Up/Down log and send the log information to the terminal automatically by default. If the status of Ethernet ports in a network changes frequently, large amount of log information may be sent to the terminal, which consumes more network resources. Additionally, too frequent log information is not convenient for you to view.

You can limit the amount of the log information sent to the terminal by disabling the Up/Down log output function on some Ethernet ports selectively. For information about log output settings, refer to the Information Center module.

Disable Up/Down log output on a port

Follow these steps to disable UP/Down log output on a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Disable a port from generating UP/Down log	undo enable log updown	Required By default, UP/Down log output is enabled.

Configuration examples

In the default conditions, where UP/DOWN log output is enabled, execute the **shutdown** command or the **undo shutdown** command on Ethernet 1/0/1. The Up/Down log information for Ethernet 1/0/1 is generated and displayed on the terminal.

```
<Sysname> system-view
```

```
System View: return to User View with Ctrl+Z.
```

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] shutdown
```

```
%Apr  5 07:25:37:634 2000 Sysname L2INF/5/PORT LINK STATUS CHANGE:- 1 -
Ethernet1/0/1 is DOWN
[Sysname-Ethernet1/0/1] undo shutdown
%Apr  5 07:25:56:244 2000 Sysname L2INF/5/PORT LINK STATUS CHANGE:- 1 -
Ethernet1/0/1 is UP
```

Disable Ethernet 1/0/1 from generating Up/Down log information and execute the **shutdown** command or the **undo shutdown** command on Ethernet 1/0/1. No Up/Down log information is generated or output for Ethernet 1/0/1.

```
[Sysname-Ethernet1/0/1] undo enable log updown
[Sysname-Ethernet1/0/1] shutdown
[Sysname-Ethernet1/0/1] undo shutdown
```

Configuring Storm Control on a Port

The storm control function is used to control traffic received on an Ethernet port.

- With traffic upper and lower thresholds specified on a port, the system periodically collects statistics about the broadcast/multicast/unicast/ traffic on the port. Once it finds that a type of traffic exceeds the specified upper threshold, it blocks this type of traffic on the port or directly shuts down the port, and outputs trap/log information according to your configuration.
- When a type of traffic on the port falls back to the specified lower threshold, the system cancels the blocking of this type of traffic on the port or brings up the port to restore traffic forwarding for the port, and outputs log/trap information according to your configuration.

Follow these steps to configure storm control on a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Set the upper and lower thresholds of broadcast/multicast/unicast traffic received on the port	storm-constrain { broadcast multicast unicast } <i>max-packets min-packets</i> { pps kbps }	Required
Set the action to be taken when a type of traffic received on the port exceeds the upper threshold.	storm-constrain control { block shutdown }	Optional By default, no action is taken when a type of traffic reaches the upper threshold.
Enable log/trap information to be output when a type of traffic received on the port exceeds the upper threshold or falls below the lower threshold	storm-constrain enable { log trap }	Optional Enabled by default.
Return to system view	quit	—
Set the interval at which the port collects traffic statistics	storm-constrain interval <i>interval-value</i>	Optional It is 10 seconds by default.



Note

- If the fabric function is enabled on a port of a device, you cannot configure the storm control function on all ports of the device.
 - If the **broadcast-suppression** command, **multicast-suppression** command or **unicast suppression** command is configured on a port, you cannot configure the storm control function on the port, and vice versa.
 - You are not recommended to set the upper and lower traffic thresholds to the same value.
 - If you specify the **block** keyword when executing the **storm-constrain control** command, only the packets beyond the upper thresholds are blocked when the overall traffic exceeds the upper threshold. In this case, the blocked packets are still taken into account when generating traffic statistics. If you specify the **shutdown** keyword when executing the command, the port will be shut down when the traffic passing through the port exceeds the upper threshold. You bring up the port again by executing the **undo shutdown** or the **undo storm-constrain { all | broadcast | multicast | unicast }** command.
-

Setting the Port State Change Delay

During a short period after you connect your switch to another device, the connecting port may go up and down frequently due to hardware compatibility, resulting in service interruption.

To avoid situations like this, you may introduce a port state change delay.



Caution

The port state change delay takes effect when the port goes down but not when the port goes up.

Follow these steps to set the port state change delay:

To do ...	Use the command ...	Remarks
Enter system view	system-view	—
Enter Ethernet interface view	interface <i>interface-type</i> <i>interface-number</i>	—

To do ...	Use the command ...	Remarks
Set the port state change delay	link-delay <i>delay-time</i>	Required No delay is introduced by default.



Note

The delay configured in this way does not take effect for ports in DLDP down state. For information about the DLDP down state, refer to *DLDP*.

Displaying and Maintaining Basic Port Configuration

To do...	Use the command...	Remarks
Display port configuration information	display interface [<i>interface-type</i> <i>interface-type interface-number</i>]	Available in any view
Display the enable/disable status of port loopback detection	display loopback-detection	
Display brief information about port configuration	display brief interface [<i>interface-type</i> [<i>interface-number</i>]] [{ begin include exclude } <i>regular-expression</i>]	
Display port information about a specified unit	display unit <i>unit-id</i> interface	
Display the storm control configurations.	display storm-constrain [<i>interface interface-type interface-number</i>] [{ begin exclude include } <i>regular-expression</i>]	
Display the statistics on the packets dropped on a port or all ports	display packet-drop { <i>interface interface-type interface-number</i> summary }	
Display the information about the port with the link-delay command configured	display link-delay	Available in user view
Clear the statistics on packets dropped on a port or all ports	reset packet-drop interface [<i>interface-type interface-number</i>]	
Clear port statistics	reset counters interface [<i>interface-type</i> <i>interface-type interface-number</i>]	Available in user view After 802.1x is enabled on a port, clearing the statistics on the port will not work.

Ethernet Port Configuration Example

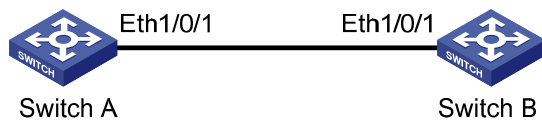
Network requirements

- Switch A and Switch B are connected to each other through two trunk port (Ethernet 1/0/1).

- Configure the default VLAN ID of both Ethernet 1/0/1 to 100.
- Allow the packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass both Ethernet 1/0/1.

Network diagram

Figure 1-2 Network diagram for Ethernet port configuration



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 1/0/1 port view.
<Sysname> system-view
[Sysname] interface ethernet 1/0/1

# Set Ethernet 1/0/1 as a trunk port.
[Sysname-Ethernet1/0/1] port link-type trunk

# Allow packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass Ethernet 1/0/1.
[Sysname-Ethernet1/0/1] port trunk permit vlan 2 6 to 50 100

# Configure the default VLAN ID of Ethernet 1/0/1 to 100.
[Sysname-Ethernet1/0/1] port trunk pvid vlan 100
  
```

Troubleshooting Ethernet Port Configuration

Symptom: Fail to configure the default VLAN ID of an Ethernet 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 the port is not a trunk or hybrid port, configure it to be a trunk or hybrid port.
- Configure the default VLAN ID of the port.

Table of Contents

1 Link Aggregation Configuration	1-1
Overview	1-1
Introduction to Link Aggregation.....	1-1
Introduction to LACP	1-1
Consistency Considerations for the Ports in Aggregation	1-1
Link Aggregation Classification	1-2
Manual Aggregation Group	1-2
Static LACP Aggregation Group.....	1-3
Dynamic LACP Aggregation Group.....	1-4
Aggregation Group Categories	1-5
Link Aggregation Configuration.....	1-6
Configuring a Manual Aggregation Group.....	1-7
Configuring a Static LACP Aggregation Group	1-7
Configuring a Dynamic LACP Aggregation Group	1-8
Configuring a Description for an Aggregation Group	1-9
Displaying and Maintaining Link Aggregation Configuration	1-9
Link Aggregation Configuration Example.....	1-10
Ethernet Port Aggregation Configuration Example	1-10

1 Link Aggregation Configuration

When configuring link aggregation, go to these sections for information you are interested in:

- [Overview](#)
- [Link Aggregation Classification](#)
- [Aggregation Group Categories](#)
- [Link Aggregation Configuration](#)
- [Displaying and Maintaining Link Aggregation Configuration](#)
- [Link Aggregation Configuration Example](#)

Overview

Introduction to Link Aggregation

Link aggregation aggregates multiple physical Ethernet ports into one logical link, also called an aggregation group.

It allows you to increase bandwidth by distributing traffic across the member ports in the aggregation group. In addition, it provides reliable connectivity because these member ports can dynamically back up each other.

Introduction to LACP

The Link Aggregation Control Protocol (LACP) is defined in IEEE 802.3ad. It uses link aggregation control protocol data units (LACPDUs) for information exchange between LACP-enabled devices.

With LACP 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.

When aggregating ports, link aggregation control automatically assigns each port an operational key based on the port speed, duplex mode, and basic configurations described in [Consistency Considerations for the Ports in Aggregation](#).

In a manual or static link aggregation group, the selected ports are assigned the same operational key. In a dynamic link aggregation group, all member ports are assigned the same operational key.

Consistency Considerations for the Ports in Aggregation

To participate in traffic sharing, member ports in an aggregation group must use the same configurations with respect to STP, QoS, GVRP, QinQ, BPDU tunnel, VLAN, port attributes, MAC address learning, and so on as shown in the following table.

Table 1-1 Consistency considerations for ports in an aggregation

Category	Considerations
STP	State of port-level STP (enabled or disabled) Attribute of the link (point-to-point or otherwise) connected to the port Port path cost STP priority STP packet format Loop protection Root protection Port type (whether the port is an edge port)
QoS	Rate limiting Priority marking 802.1p priority Congestion avoidance Traffic redirecting Traffic accounting
Link type	Link type of the ports (trunk, hybrid, or access)
GVRP	GVRP state on ports (enabled or disabled) GVRP registration type GARP timer settings
VLAN-VPN	State of VLAN-VPN (enabled or disabled) TPID on the ports State of inner-to-outer tag priority replication (enabled or disabled)

**Note**

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

Link Aggregation Classification

Depending on different aggregation modes, the following three types of link aggregation exist:

- Manual aggregation
- Static LACP aggregation
- Dynamic LACP aggregation

Manual Aggregation Group

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 you cannot enable LACP on ports in a manual aggregation group.

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, only the selected ports can forward user service packets.

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

- Among the ports in an aggregation group that are in up state, the system determines the master port with one of the following settings being the highest (in descending order) as the master port: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed. The ports with their rate, duplex mode and link type being the same as that of the master port are selected ports, and the rest are unselected ports.
- There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the selected ports in an aggregation group exceeds the maximum number supported by the device, those with lower port numbers operate as the selected ports, and others as unselected ports.

Among the selected ports in an aggregation group, the one with smallest port number operates as the master port. Other selected ports are the member ports.

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.

Static LACP Aggregation Group

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, all the member ports in up state form one or multiple dynamic aggregations with LACP enabled. LACP cannot be disabled on static aggregation ports.

Port status of static aggregation group

A port in a static aggregation group can be in one of the two states: selected or unselected.

- Both the selected and the unselected ports in the up state can transceive LACP protocol packets.
- Only the selected ports can transceive service packets; the unselected ports cannot.

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

- Among the ports in an aggregation group that are in up state, the system determines the master port with one of the following settings being the highest (in descending order) as the master port: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed. The ports with their rate, duplex mode and link type being the same as that of the master port are selected port, and the rest are unselected ports.

- The ports connected to a peer device different from the one the master port is connected to or those 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 are unselected ports.
- 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 selected ports in an aggregation group exceeds the maximum number supported by the device, those with lower port numbers operate as the selected ports, and others as unselected ports.

Dynamic LACP Aggregation Group

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. Ports can be aggregated into a dynamic aggregation group only when they are connected to the same peer device and have the same speed, duplex mode, and basic configurations, and their peer ports have the same configurations.

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.

Port status of dynamic aggregation group

A port in a dynamic aggregation group can be in one of the two states: selected and unselected.

- Both the selected and the unselected ports can receive/transmit LACP protocol packets;
- The selected ports can receive/transmit user service packets, but the unselected ports cannot.
- In a dynamic 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.



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.
-

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, 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 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.
-

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, multicast MAC addresses, or the static ARP protocol cannot be added to an 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.
 - Do not add ports with the inter-VLAN MAC address replicating function of the selective QinQ feature enabled to an aggregation group.
 - Do not add ports with IP filtering enabled to an aggregation group.
 - Do not add ports with ARP intrusion detection enabled to an aggregation group.
 - Do not add ports with source IP addresses/source MAC addresses statically bound to them to an aggregation group.
 - Web-authentication-enabled ports cannot be added to an aggregation group.
-

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 will be removed from the group).

For a manual aggregation group, a port can only be manually added/removed to/from the manual aggregation group.

Follow these steps to configure a manual aggregation group:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a manual aggregation group	link-aggregation group <i>agg-id</i> mode manual	Required
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Add the Ethernet port to the aggregation group	port link-aggregation group <i>agg-id</i>	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.

Configuring a Static LACP Aggregation Group

You can create a static LACP aggregation group, or remove an existing static LACP aggregation group (after that, the system will re-aggregate the original member ports in the group to form one or multiple 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.

Follow these steps to configure a static LACP aggregation group:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a static aggregation group	link-aggregation group <i>agg-id</i> mode static	Required
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Add the port to the aggregation group	port link-aggregation group <i>agg-id</i>	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.

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.

Follow these steps to configure a dynamic LACP aggregation group:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the system priority	lacp system-priority <i>system-priority</i>	Optional By default, the system priority is 32,768.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable LACP on the port	lacp enable	Required By default, LACP is disabled on a port.

To do...	Use the command...	Remarks
Configure the port priority	lacp port-priority <i>port-priority</i>	Optional By default, the port priority is 32,768.



Note

Changing the system priority may affect the priority relationship between the aggregation peers, and thus affect the selected/unselected status of member ports in the dynamic aggregation group.

Configuring a Description for an Aggregation Group

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a description for an aggregation group	link-aggregation group <i>agg-id</i> description <i>agg-name</i>	Optional By default, no description is configured for an aggregation group.



Caution

If you have saved the current configuration with the **save** command, after system reboot, the configuration concerning manual and static aggregation groups and their descriptions still exists, but that of dynamic aggregation groups and their descriptions gets lost.

Displaying and Maintaining Link Aggregation Configuration

To do...	Use the command...	Remarks
Display summary information of all aggregation groups	display link-aggregation summary	Available in any view
Display detailed information of a specific aggregation group or all aggregation groups	display link-aggregation verbose [<i>agg-id</i>]	
Display link aggregation details of a specified port or port range	display link-aggregation interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>]	
Display local device ID	display lacp system-id	
Clear LACP statistics about a specified port or port range	reset lacp statistics [interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>]]	Available in user view

Link Aggregation Configuration Example

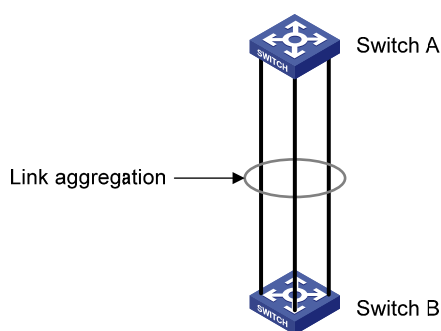
Ethernet Port Aggregation Configuration Example

Network requirements

- Switch A connects to Switch B with three ports Ethernet 1/0/1 to Ethernet 1/0/3. It is required that 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.

Network diagram

Figure 1-1 Network diagram for link aggregation configuration



Configuration procedure



Note

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.

```
<Sysname> system-view
```

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

Add Ethernet 1/0/1 through Ethernet 1/0/3 to aggregation group 1.

```
[Sysname] interface Ethernet1/0/1
```

```
[Sysname-Ethernet1/0/1] port link-aggregation group 1
```

```
[Sysname-Ethernet1/0/1] quit
```

```
[Sysname] interface Ethernet 1/0/2
```

```
[Sysname-Ethernet1/0/2] port link-aggregation group 1
```

```
[Sysname-Ethernet1/0/2] quit
```

```
[Sysname] interface Ethernet1/0/3
```

```
[Sysname-Ethernet1/0/3] port link-aggregation group 1
```

2) Adopting static LACP aggregation mode

Create static aggregation group 1.

```
<Sysname> system-view
[Sysname] link-aggregation group 1 mode static

# Add Ethernet 1/0/1 through Ethernet 1/0/3 to aggregation group 1.

[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] port link-aggregation group 1
[Sysname-Ethernet1/0/1] quit
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] port link-aggregation group 1
[Sysname-Ethernet1/0/2] quit
[Sysname] interface Ethernet1/0/3
[Sysname-Ethernet1/0/3] port link-aggregation group 1
```

3) Adopting dynamic LACP aggregation mode

Enable LACP on Ethernet 1/0/1 through Ethernet 1/0/3.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] lacp enable
[Sysname-Ethernet1/0/1] quit
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] lacp enable
[Sysname-Ethernet1/0/2] quit
[Sysname] interface Ethernet1/0/3
[Sysname-Ethernet1/0/3] lacp enable
```



Caution

The three LACP-enabled ports can be aggregated into one dynamic aggregation group to implement load sharing only when they have the same basic configuration (such as rate, duplex mode, and so on).

Table of Contents

1 Port Isolation Configuration	1-1
Port Isolation Overview	1-1
Port Isolation Configuration	1-1
Displaying and Maintaining Port Isolation Configuration	1-2
Port Isolation Configuration Example	1-2

1 Port Isolation Configuration

When configuring port isolation, go to these sections for information you are interested in:

- [Port Isolation Overview](#)
- [Port Isolation Configuration](#)
- [Displaying and Maintaining Port Isolation Configuration](#)
- [Port Isolation Configuration Example](#)

Port Isolation Overview

The port isolation feature is used to secure and add privacy to the data traffic and prevent malicious attackers from obtaining the user information. With 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 (a port in an isolation group does not forward traffic to the other ports in the isolation group).

The ports in an isolation group must reside on the same switch or different units of an IRF fabric.



Note

- Currently, you can create only one isolation group on an S3600 series Ethernet switch. The number of Ethernet ports in an isolation group is not limited.
 - An isolation group only isolates the member ports in it.
-

Port Isolation Configuration

You can perform the following operations to add an Ethernet port to an isolation group, thus isolating Layer 2 and Layer 3 data among the ports in the isolation group.

Follow these steps to configure port isolation:

To do ...	Use the command ...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Add the Ethernet port to the isolation group	port isolate	Required By default, an isolation group contains no port.

**Note**

- When a member port of an aggregation group joins/leaves an isolation group, the other ports in the same aggregation group will join/leave the isolation group at the same time.
 - For ports that belong to an aggregation group and an isolation group simultaneously, removing a port from the aggregation group has no effect on the other ports. That is, the rest ports remain in the aggregation group and the isolation group.
 - Ports that belong to an aggregation group and an isolation group simultaneously are still isolated even when you remove the aggregation group in system view.
 - Adding an isolated port to an aggregation group causes all the ports in the aggregation group on the local unit to be added to the isolation group.
 - S3600 series Ethernet switches support cross-device port isolation if IRF fabric is enabled.
 - For S3600 series Ethernet switches belonging to the same IRF Fabric, the port isolation configuration performed on a port of a cross-device aggregation group cannot be synchronized to the other ports of the aggregation group if the ports reside on other units. That is, to add multiple ports in a cross-device aggregation group to the same isolation group, you need to perform the configuration for each of the ports individually.
-

Displaying and Maintaining Port Isolation Configuration

To do ...	Use the command ...	Remarks
Display information about the Ethernet ports added to the isolation group	display isolate port	Available in any view

Port Isolation Configuration Example

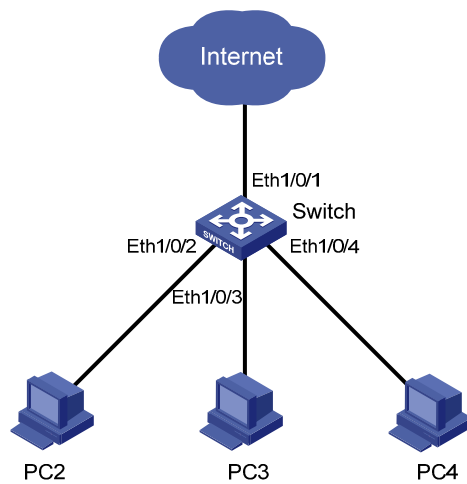
Network requirements

As shown in [Figure 1-1](#), 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 to isolate PC2, PC3 and PC4 to disable them from communicating directly with each other.

Network diagram

Figure 1-1 Network diagram for port isolation configuration



Configuration procedure

Add Ethernet1/0/2, Ethernet1/0/3, and Ethernet1/0/4 to the isolation group.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface ethernet1/0/2
[Sysname-Ethernet1/0/2] port isolate
[Sysname-Ethernet1/0/2] quit
[Sysname] interface ethernet1/0/3
[Sysname-Ethernet1/0/3] port isolate
[Sysname-Ethernet1/0/3] quit
[Sysname] interface ethernet1/0/4
[Sysname-Ethernet1/0/4] port isolate
[Sysname-Ethernet1/0/4] quit
[Sysname] quit
```

Display information about the ports in the isolation group.

```
<Sysname> display isolate port
Isolated port(s) on UNIT 1:
Ethernet1/0/2, Ethernet1/0/3, Ethernet1/0/4
```

Table of Contents

1 Port Security Configuration	1-1
Port Security Overview	1-1
Introduction	1-1
Port Security Modes	1-2
Port Security Features	1-7
Port Security Configuration Task List	1-8
Enabling Port Security	1-8
Setting the Maximum Number of Secure MAC Addresses Allowed on a Port	1-9
Setting the Port Security Mode	1-10
Configuring Port Security Features	1-11
Configuring Guest VLAN for a Port in macAddressOrUserLoginSecure mode	1-12
Ignoring the Authorization Information from the RADIUS Server	1-13
Configuring Secure MAC Addresses	1-13
Displaying and Maintaining Port Security Configuration	1-15
Port Security Configuration Examples	1-15
Port Security Mode autoLearn Configuration Example	1-15
Port Security Mode macAddressWithRadius Configuration Example	1-16
Port Security Mode userLoginWithOUI Configuration Example	1-18
Port Security Mode macAddressElseUserLoginSecureExt Configuration Example	1-20
Port Security Mode macAddressAndUserLoginSecureExt Configuration Example	1-22
Guest VLAN Configuration Example	1-24
2 Port Binding Configuration	2-1
Port Binding Overview	2-1
Introduction	2-1
Configuring Port Binding	2-2
Displaying and Maintaining Port Binding Configuration	2-2
Port Binding Configuration Example	2-2
Port Binding Configuration Example	2-2

1 Port Security Configuration



Note

The following new features are added:

- The port in the **macAddressOrUserLoginSecure** mode supports guest VLAN configuration. For details, refer to [Configuring Guest VLAN for a Port in macAddressOrUserLoginSecure mode](#).
 - The security MAC addresses that the port learns automatically supports aging. For details, refer to [Configuring Secure MAC Addresses](#).
-

When configuring port security, go to these sections for information you are interested in:

- [Port Security Overview](#)
 - [Port Security Configuration Task List](#)
 - [Displaying and Maintaining Port Security Configuration](#)
 - [Port Security Configuration Examples](#)
-



Note

The security modes of the port security feature provide extended and combined use of 802.1X authentication and MAC authentication. They apply to scenarios that require both 802.1X authentication and MAC authentication. For scenarios that require only 802.1X authentication or MAC authentication, you are recommended to configure 802.1X authentication or MAC authentication rather than port security for simplicity.

Port Security Overview

Introduction

Port security is a security mechanism for network access control. It is an expansion to the current 802.1X and MAC authentication.

Port security allows you to configure a port to operate in an intended security mode to control the MAC address learning or user authentication on the port. This enables the switch to learn legal source MAC addresses, so as to implement network security management as needed.

With port security enabled, packets whose source MAC addresses cannot be learned by your switch in a security mode are considered illegal packets; the events that cannot pass 802.1X authentication or MAC authentication are considered illegal.

Upon detection of illegal frames or events, the switch takes the pre-defined action automatically. While enhancing system security, this reduces your maintenance efforts greatly.

Port Security Modes

By configuring a port of your switch to operate in an intended security mode, you can control how the port learns source MAC addresses and thereby filters illegal packets.

[Table 1-1](#) describes the port security modes.

Table 1-1 Description of port security modes

On the port, if you want to...	Use the security mode...	
Control MAC address learning	autoLearn	
	secure	
Perform 802.1X authentication	userLogin	
	userLoginSecure	
	userLoginSecureExt	
	userLoginWithOUI	
Perform MAC authentication	macAddressWithRadius	
Perform a combination of MAC authentication and 802.1X authentication	And	macAddressAndUserLoginSecure
		macAddressAndUserLoginSecureExt
	Else	macAddressElseUserLoginSecure
		macAddressElseUserLoginSecureExt
	Or	macAddressOrUserLoginSecure
		macAddressOrUserLoginSecureExt

Tip

These security mode naming rules may help you remember the modes:

- **userLogin** specifies 802.1X authentication and port-based access control.
- **userLogin** with **Secure** specifies 802.1X authentication and MAC-based access control.
- **macAddress** specifies MAC authentication.
- **And** specifies that both MAC authentication and 802.1X authentication are required. A user can access the network only after passing both authentications.
- **Else** specifies that the authentication method before **Else** is applied first. If the authentication fails, whether to turn to the authentication method following **Else** depends on the protocol type of the authentication request.
- In a security mode with **Or**, which authentication method is to be used depends on the protocol type of the authentication request.
- **Ext** indicates allowing multiple 802.1X users to be authenticated and serviced at the same time.

autoLearn mode vs. secure mode

- In **autoLearn** mode, a port can learn MAC addresses. These dynamically learned MAC addresses are secure MAC addresses. You can also configure secure MAC addresses by using the **mac-address security** command. A secure MAC addresses never ages out by default. When the number of secure MAC addresses reaches the upper limit, the port turns to **secure** mode. In

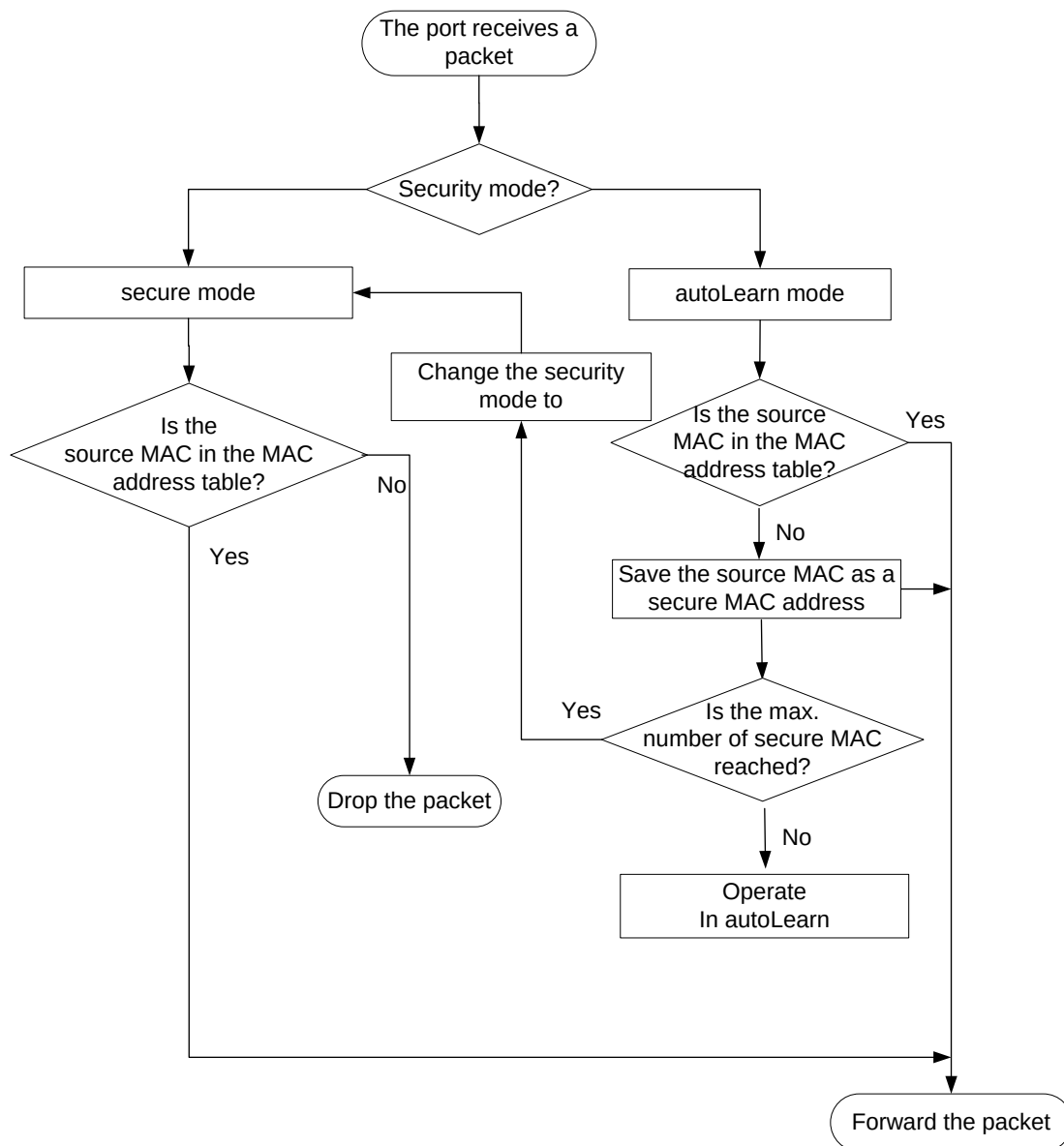
addition, you can configure dynamic MAC addresses by using the **mac-address dynamic** command for a port in **autoLearn** mode.

- In **secure** mode, MAC address learning is disabled on the port and you can configure static and dynamic MAC addresses (by using the **mac-address static** or **mac-address dynamic** command).

A port in **autoLearn** or **secure** mode allows only frames sourced from the MAC addresses that are in the MAC address table to pass.

[Figure 1-1](#) shows the packet processing on a port in autoLearn/secure mode and the mode transition.

Figure 1-1 Packet processing and mode transition in autoLearn mode and secure mode



802.1X authentication

- **userLogin**: A port performs 802.1X authentication and implements port-based access control.
- **userLoginSecure**: A port performs 802.1X authentication for users and implements MAC-based access control. The port services only one user passing 802.1X authentication.
- **userLoginSecureExt**: Similar to the **userLoginSecure** mode except that this mode supports multiple online 802.1X users.

- **userLoginWithOUI:** Similar to the **userLoginSecure** mode, however, a port in this mode also permits frames from a user whose MAC address contains a specified OUI (organizationally unique identifier).



Note

For description of 802.1X authentication, refer to *802.1x and System Guard Operation*.

MAC authentication

macAddressWithRadius: A port in this mode performs MAC authentication for users.



Note

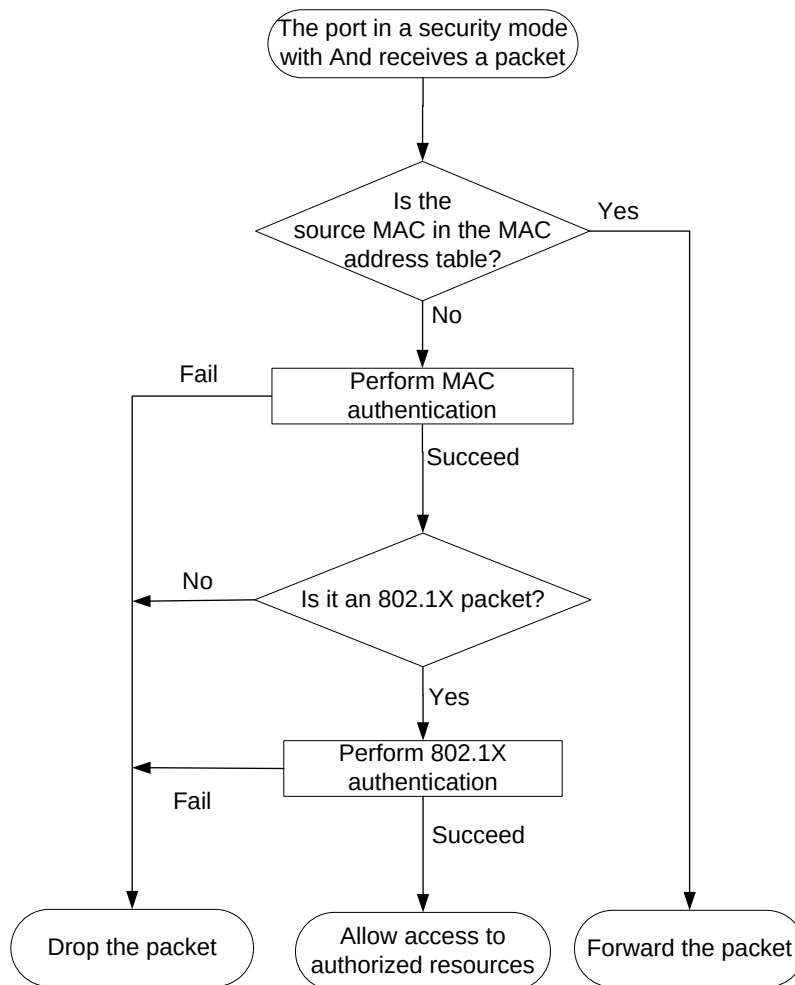
For description of MAC authentication, refer to *MAC Address Authentication Operation*.

Security modes with the And keyword

- **macAddressAndUserLoginSecure:** A port in this mode first performs MAC authentication for a user and then, if the user passes MAC authentication, performs 802.1X authentication. A user can access the network only after passing both authentications. The port supports up to one online 802.1X user.
- **macAddressAndUserLoginSecureExt:** Similar to the **macAddressAndUserLoginSecure** mode except that a port in this mode supports multiple users, as the **Ext** keyword implies.

[Figure 1-2](#) shows how the port processes packets in a security mode with the **And** keyword.

Figure 1-2 Packet processing in a security mode with the And keyword

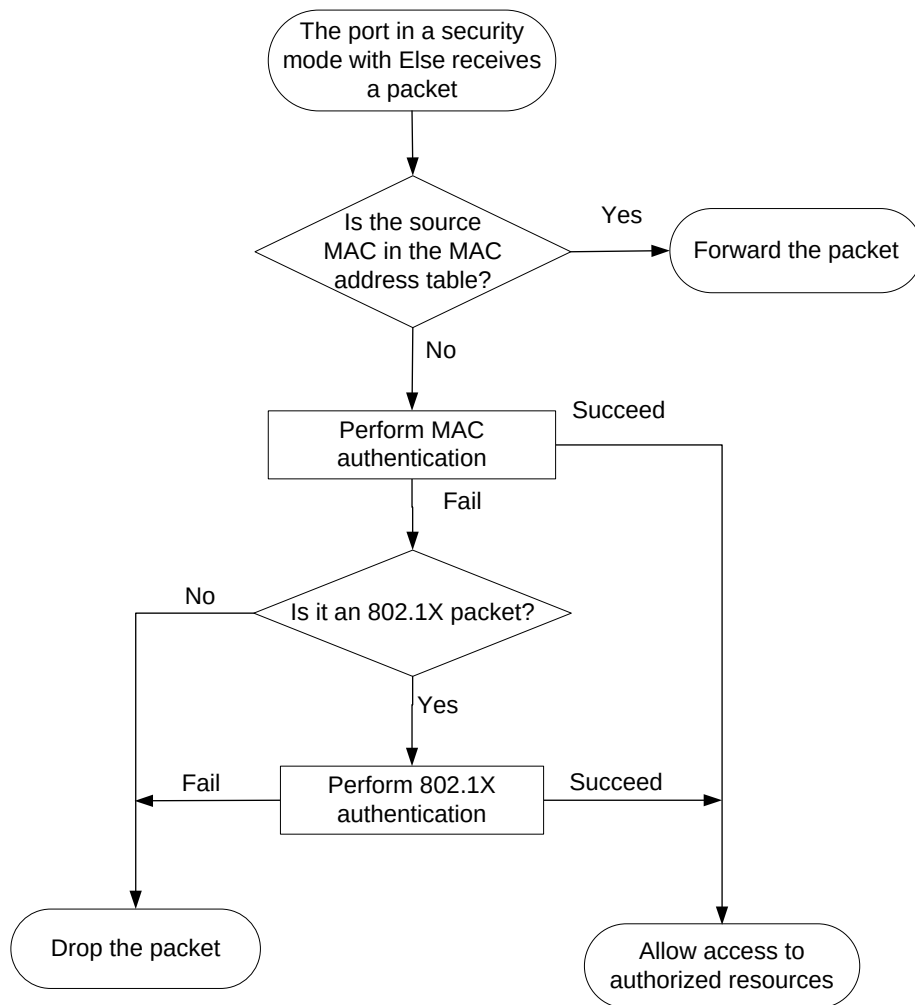


Security modes with the Else keyword

- **macAddressElseUserLoginSecure**: As the **Else** keyword implies, MAC authentication is applied first. A port in this mode performs only MAC authentication for non-802.1X frames; it performs MAC authentication for 802.1X frames and then, if the authentication fails, 802.1X authentication. The port in this mode supports only one 802.1X online user, but supports multiple MAC authenticated online users.
- **macAddressElseUserLoginSecureExt**: Similar to the **macAddressElseUserLoginSecure** mode except that the port in this mode services multiple 802.1X online users as the **Ext** keyword implies.

[Figure 1-3](#) shows how the port processes packets in a security mode with the **Else** keyword.

Figure 1-3 Packet processing in security modes with the Else keyword

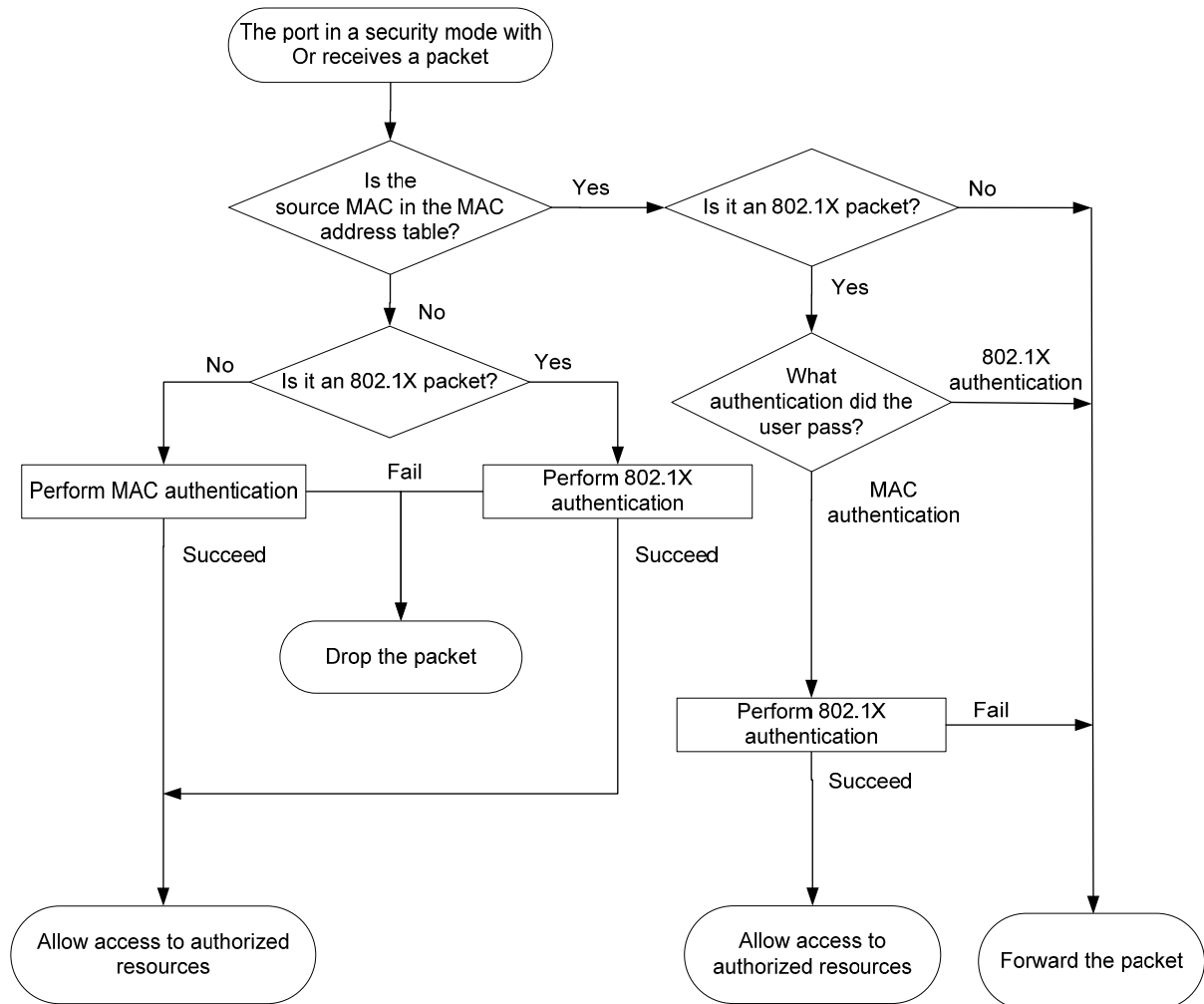


Security mode with the Or keyword

- **macAddressOrUserLoginSecure**: A port in this mode performs MAC authentication upon receiving non-802.1X frames and performs 802.1X authentication upon receiving 802.1X frames. 802.1X authentication can be applied to users who have already passed MAC authentication. The port in this mode supports up to one 802.1X online user, but supports multiple MAC authenticated online users.
- **macAddressOrUserLoginSecureExt**: Similar to the **macAddressOrUserLoginSecure** mode except that a port in this mode supports multiple 802.1X online users.

[Figure 1-4](#) shows how the port processes packets in a security mode with the **Or** keyword.

Figure 1-4 Packet processing in a security mode with the Or keyword



Port Security Features

The following port security features are provided:

- NTK (need to know) feature: Checks the destination MAC addresses in outbound frames and allows frames to be sent to only devices passing authentication. This prevents illegal devices from intercepting network traffic.
- Intrusion protection feature: Checks the source MAC addresses in inbound frames or the usernames and passwords in 802.1X authentication requests, and takes the pre-defined action on each detected illegal frame or event. The action may be disabling the port temporarily, disabling the port unless you bring it up manually, or blocking frames from an illegal MAC address for three minutes (unmodifiable).
- Trap feature: Enables the device to send trap messages upon detecting specified frames that result from, for example, intrusion or user login/logout operations. This helps you monitor some special behaviors.



Note

- In **userLogin** mode, neither NTK nor intrusion protection will be triggered. In any other port security mode, the two features will be triggered upon detection of illegal frames.
- In **userLoginWithOUI** mode, intrusion protection will not be triggered even if the OUI value does not match.
- When a port operates in either the **macAddressElseUserLoginSecure** mode or the **macAddressElseUserLoginSecureExt** mode, intrusion protection will be triggered only after both MAC authentication and 802.1X authentication on the same packet fail.

Port Security Configuration Task List

Complete the following tasks to configure port security:

Task		Remarks
Enabling Port Security		Required
Setting the Maximum Number of Secure MAC Addresses Allowed on a Port		Optional
Setting the Port Security Mode		Required
Configuring Port Security Features	Configuring the NTK feature	Optional Choose one or more features as required.
	Configuring intrusion protection	
	Configuring trapping	
Configuring Guest VLAN for a Port in macAddressOrUserLoginSecure mode		Optional
Ignoring the Authorization Information from the RADIUS Server		Optional
Configuring Secure MAC Addresses		Optional

Enabling Port Security

Configuration Prerequisites

Before enabling port security, disable 802.1X and MAC authentication globally.

Enabling Port Security

Follow these steps to enable port security:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable port security	port-security enable	Required Disabled by default



Caution

Enabling port security resets the following configurations on a port to the bracketed defaults. Then values of these configurations cannot be changed manually; the system will adjust them based on the port security mode automatically.

- 802.1X (disabled), port access control method (macbased), and port authorization mode (auto)
- MAC authentication (disabled)



Note

- For details about 802.1X authentication, refer to the relevant sections in *802.1x and System-Guard Operation*.
- For details about MAC authentication, refer to sections in *MAC Address Authentication Operation*.
- The port security feature does not support the quick EAD deployment feature in 802.1X.

Setting the Maximum Number of Secure MAC Addresses Allowed on a Port

You can set a limit on the number of users to be authenticated on a port. The number of authenticated users allowed, however, cannot exceed the upper limit. The maximum number of users on a port in a security mode is determined by the maximum number of secure MAC addresses or the maximum number of authenticated users that the security mode supports, whichever is smaller.

By setting the maximum number of MAC addresses allowed on a port, you can:

- Control the maximum number of users who are allowed to access the network through the port
- Control the number of secure MAC addresses that can be added with port security

This configuration is independent of the maximum number of MAC addresses that can be learned by the port in MAC address management.

Follow these steps to set the maximum number of MAC addresses allowed on a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Set the maximum number of MAC addresses allowed on the port	port-security max-mac-count <i>count-value</i>	Required Not limited by default

Setting the Port Security Mode

Follow these steps to set the port security mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the OUI value for user authentication	port-security oui <i>OUI-value</i> index <i>index-value</i>	Optional In userLoginWithOUI mode, a port allows only one 802.1X user and one user whose source MAC address contains a specified OUI to pass authentication at the same time.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Set the port security mode	port-security port-mode { autolearn mac-and-userlogin-secure mac-and-userlogin-secure-ext mac-authentication mac-else-userlogin-secure mac-else-userlogin-secure-ext secure userlogin userlogin-secure userlogin-secure-ext userlogin-secure-or-mac userlogin-secure-or-mac-ext userlogin-withoui }	Required By default, a port operates in noRestriction mode. In this mode, access to the port is not restricted. You can set a port security mode as needed.



Note

- Before setting the port to operate in the **autoLearn** mode, be sure to set the maximum number of secure MAC addresses allowed on the port with the **port-security max-mac-count** command.
- When the port operates in the **autoLearn** mode, you cannot change the maximum number of secure MAC addresses allowed on the port.
- After you set the port security mode to **autoLearn**, you cannot configure any static or blackhole MAC addresses on the port.
- After enabling port security, you can change the port security mode of a port only when the port is operating in **noRestriction** mode, the default mode. To change the port security mode of a port operating in any other mode, use the **undo port-security port-mode** command to restore the default port security mode first.

If the **port-security port-mode** *mode* command has been executed on a port, none of the following can be configured on the same port:

- Maximum number of secure MAC addresses that the port can learn
- Reflector port for port mirroring
- Fabric port
- Link aggregation

Configuring Port Security Features

Configuring the NTK feature

Follow these steps to configure the NTK feature:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the NTK feature	port-security ntk-mode { ntkonly ntk-withbroadcasts ntk-withmulticasts }	Required By default, NTK is disabled on a port, namely all frames are allowed to be sent.

Configuring intrusion protection

Follow these steps to configure the intrusion protection feature:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Set the corresponding action to be taken by the switch when intrusion protection is triggered	port-security intrusion-mode { blockmac disableport disableport-temporarily }	Required By default, intrusion protection is disabled.
Return to system view	quit	—
Set the timer during which the port remains disabled	port-security timer disableport <i>timer</i>	Optional 20 seconds by default



Note

The **port-security timer disableport** command is used in conjunction with the **port-security intrusion-mode disableport-temporarily** command to set the length of time period during which the port remains disabled.



Caution

If you configure the NTK feature and execute the **port-security intrusion-mode blockmac** command on the same port, the switch will be unable to disable the packets whose destination MAC address is illegal from being sent out that port; that is, the NTK feature configured will not take effect on the packets whose destination MAC address is illegal.

Configuring trapping

Follow these steps to configure port security trapping:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable sending traps for the specified type of event	port-security trap { addresslearned dot1xlogfailure dot1xlogoff dot1xlogon intrusion ralmlogfailure ralmlogoff ralmlogon }	Required By default, no trap is sent.

Configuring Guest VLAN for a Port in macAddressOrUserLoginSecure mode

Users fails the authentication can access certain specified VLAN. This VLAN is called guest VLAN. For details about guest VLAN, refer to the sections covering 802.1x and System-Guard.

A port in **macAddressOrUserLoginSecure** mode supports guest VLAN configurations. The port can connect multiple users; but services only one user at a time.

- 1) When the first user of the port initiates 802.1X or MAC authentication:
 - If the user fails the authentication, the port is added to the guest VLAN, and all the other users of the port are authorized to access the guest VLAN.
 - If the user passes the authentication, authentication requests from other users are not handled because only one user is allowed to pass authentication using the port. The other users will fail the authentication, but the port will not be added to the guest VLAN.
- 2) After the port is added to the guest VLAN:
 - The users of the port can initiate 802.1X authentication. If a user passes authentication, the port leaves the guest VLAN and is added to the original VLAN, that is, the one the port belongs to before it is added to the guest VLAN). The port then does not handle other users' authentication requests.
 - MAC authentication is also allowed. However, MAC authentication in this case cannot be triggered by user requests; the switch will use the first MAC address learned in the guest VLAN to initiate MAC authentication at a certain interval. If the authentication succeeds, the port leaves the guest VLAN.

Follow these steps to configure a guest VLAN for a port in **macAddressOrUserLoginSecure** mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the interval at which the switch triggers MAC authentication after a port is added to the guest VLAN	port-security timer guest-vlan-reauth <i>interval</i>	Optional
Enter Ethernet port view	interface <i>interface-type interface-number</i>	—
Set the security mode to macAddressOrUserLoginSecure	port-security port-mode userlogin-secure-or-mac	Required
Specify a VLAN as the guest VLAN of the port	port-security guest-vlan <i>vlan-id</i>	Required

Note that:

- Only an existing VLAN can be specified as a guest VLAN. Make sure the guest VLAN of a port contain the resources that the users need.

- If one user of the port has passed or is undergoing authentication, you cannot specify a guest VLAN for it.
- When a user using a port with a guest VLAN specified fail the authentication, the port is added to the guest VLAN and users of the port can access only the resources in the guest VLAN.
- Multiple users may connect to one port in the **macAddressOrUserLoginSecure** mode for authentication; however, after a guest VLAN is specified for the port, only one user can pass the security authentication. In this case, the authentication client software of the other 802.1X users displays messages about the failure; MAC authentication does not have any client software and therefore no such messages will be displayed.
- To change the security mode from **macAddressOrUserLoginSecure** mode of a port that is assigned to a guest VLAN, execute the **undo port-security guest-vlan** command first to remove the guest VLAN configuration.
- For a port configured with both the **port-security guest-vlan** and **port-security intrusion-mode disableport** commands, when authentication of a user fails, only the intrusion detection feature is triggered. The port is not added to the specified guest VLAN.
- It is not recommended to configure the **port-security guest-vlan** and **port-security intrusion-mode blockmac** commands simultaneously for a port. Because when the authentication of a user fails, the blocking MAC address feature will be triggered and packets of the user will be dropped, making the user unable to access the guest VLAN.

Ignoring the Authorization Information from the RADIUS Server

After an 802.1X user or MAC-authenticated user passes Remote Authentication Dial-In User Service (RADIUS) authentication, the RADIUS server delivers the authorization information to the device. You can configure a port to ignore the authorization information from the RADIUS server.

Follow these steps to configure a port to ignore the authorization information from the RADIUS server:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Ignore the authorization information from the RADIUS server	port-security authorization ignore	Required By default, a port uses the authorization information from the RADIUS server.

Configuring Secure MAC Addresses

In **autoLearn** mode, a port can learn MAC addresses. These dynamically learned MAC addresses are secure MAC addresses. You can also configure secure MAC addresses by using the **mac-address security** command. A secure MAC addresses never ages out by default. .One MAC address can only be added to the table of one port as a secure MAC address. This feature allows binding a secure MAC address to one port in the same VLAN.

After the security port is set to **autoLearn**, the port changes its way of learning MAC addresses as follows.

- The port deletes original dynamic MAC addresses.

- If the amount of secure MAC address entries has not yet reach the maximum number, the port will learn new MAC addresses and save them as secure MAC addresses.
- If the amount of secure MAC address entries 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 manually configured secure MAC addresses are written to the configuration file; they will not get lost no matter whether the port is up or down. As long as the configuration file is saved, the secure MAC addresses can be restored after the switch restarts.

Configuring a secure MAC address entry manually

Before configuring a secure MAC address entry for a port manually, ensure that:

- Port security is enabled.
- The maximum number of secure MAC addresses allowed on the port is set.
- The security mode of the port is set to **autoLearn**.

Follow these steps to configure a secure MAC address entry manually:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Add a secure MAC address entry	In system view	mac-address security <i>mac-address interface interface-type interface-number vlan vlan-id</i>	Either is required.
	In Ethernet port view	interface <i>interface-type interface-number</i>	By default, no secure MAC address entry is configured.
		mac-address security <i>mac-address vlan vlan-id</i>	

Configuring an aging time for learned secure MAC address entries

By default, learned secure MAC addresses will never age out; they are deleted only when the port security feature is disabled or the security mode is not **autoLearn** any more. However, the learned secure MAC addresses are not deleted when the security mode turns to the **secure** mode from **autoLearn**.

You can configure an aging time for secure MAC address entries. When the timer of an entry expires, the entry is removed from the secure MAC address table.

Follow these steps to configure an aging time for learned secure MAC address entries:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable port security	port-security enable	—
Configure the aging time for learned secure MAC address entries	port-security timer autolearn <i>age</i>	Required Aging of MAC address entries is disabled by default.

To do...	Use the command...	Remarks
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Set the maximum number of secure MAC addresses allowed on the port	port-security max-mac-count <i>count-value</i>	Required By default, there is no limit on the number of secure MAC addresses.
Set the security mode of the port to autoLearn	port-security port-mode autolearn	Required By default, a port operates in noRestriction mode, and access to the port is not restricted.



Note

After you execute the **port-security timer autolearn** command, you can display secure MAC address entries by the **display mac-address security** command. Though the aging time field displayed has a value of "NOAGED", the aging of secure MAC address entries is enabled already.

Displaying and Maintaining Port Security Configuration

To do...	Use the command...	Remarks
Display information about port security configuration	display port-security [interface <i>interface-list</i>]	Available in any view
Display information about secure MAC address configuration	display mac-address security [interface <i>interface-type interface-number</i>] [vlan <i>vlan-id</i>] [count]	

Port Security Configuration Examples

Port Security Mode autoLearn Configuration Example

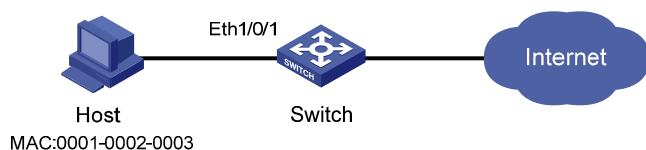
Network requirements

Restrict Ethernet 1/0/1 of the switch as follows:.

- Allow a maximum of 80 users to access the port without authentication and permit the port to learn and add the MAC addresses of the users as secure MAC addresses.
- To ensure that Host can access the network, add the MAC address 0001-0002-0003 of Host as a secure MAC address to the port in VLAN 1.
- After the number of secure MAC addresses reaches 80, the port stops learning MAC addresses. If any frame with an unknown MAC address arrives, intrusion protection is triggered and the port will be disabled and stay silent for 30 seconds.

Network diagram

Figure 1-5 Network diagram for port security mode autoLearn



Configuration procedure

```
# Enter system view.
<Switch> system-view

# Enable port security.
[Switch] port-security enable

# Enter Ethernet1/0/1 port view.
[Switch] interface Ethernet 1/0/1

# Set the maximum number of MAC addresses allowed on the port to 80.
[Switch-Ethernet1/0/1] port-security max-mac-count 80

# Set the port security mode to autoLearn.
[Switch-Ethernet1/0/1] port-security port-mode autolearn

# Add the MAC address 0001-0002-0003 of Host as a secure MAC address to the port in VLAN 1.
[Switch-Ethernet1/0/1] mac-address security 0001-0002-0003 vlan 1

# Configure the port to be silent for 30 seconds after intrusion protection is triggered.
[Switch-Ethernet1/0/1] port-security intrusion-mode disableport-temporarily
[Switch-Ethernet1/0/1] quit
[Switch] port-security timer disableport 30
```

Port Security Mode macAddressWithRadius Configuration Example

Network requirements

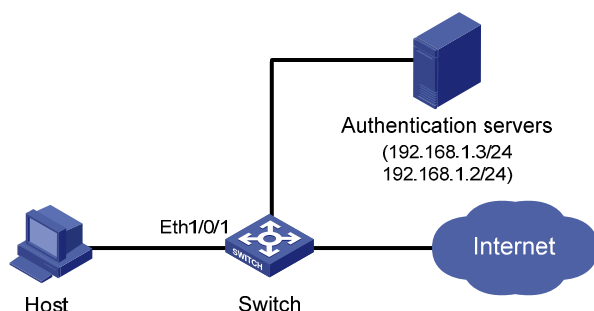
The host connects to the switch through port Ethernet 1/0/1, and the switch authenticates the host with a RADIUS server. If the authentication succeeds, the host is authorized to access the Internet.

Restrict port Ethernet 1/0/1 of the switch as follows:

- The switch performs MAC authentication for users.
- All users belong to the domain **aabbcc.net**, and each of them uses the MAC address as username and password for authentication.
- Whenever a packet fails MAC authentication, intrusion protection is triggered to filter packets whose source MAC addresses are the same as that of the packet failing the authentication, ensuring the security of the port.

Network diagram

Figure 1-6 Network diagram for configuring port security mode `macAddressWithRadius`



Configuration procedure



Note

- The following configurations involve some AAA/RADIUS configuration commands. For details about the commands, refer to *AAA Operation*.
- Configurations on the user host and the RADIUS server are omitted.

- Configure RADIUS parameters

Create a RADIUS scheme named **radius1**.

```
<Switch> system-view
```

```
[Switch] radius scheme radius1
```

Specify the primary RADIUS authentication server and primary RADIUS accounting server.

```
[Switch-radius-radius1] primary authentication 192.168.1.3
```

```
[Switch-radius-radius1] primary accounting 192.168.1.2
```

Specify the secondary RADIUS authentication server and secondary RADIUS accounting server.

```
[Switch-radius-radius1] secondary authentication 192.168.1.2
```

```
[Switch-radius-radius1] secondary accounting 192.168.1.3
```

Set the shared key for message exchange between the switch and the RADIUS authentication servers to **name**.

```
[Switch-radius-radius1] key authentication name
```

Set the shared key for message exchange between the switch and the accounting RADIUS servers to **name**.

```
[Switch-radius-radius1] key accounting name
```

Configure the switch to send a username without the domain name to the RADIUS server.

```
[Switch-radius-radius1] user-name-format without-domain
```

```
[Switch-radius-radius1] quit
```

Create a domain named **aabbcc.net** and enter its view.

```
[Switch] domain aabbcc.net
```

Specify the RADIUS scheme for the domain.

```
[Switch-isp-aabbcc.net] scheme radius-scheme radius1
[Switch-isp-aabbcc.net] quit

# Set aabbcc.net as the default user domain.
[Switch] domain default enable aabbcc.net

# Configure the switch to use MAC addresses as usernames for authentication, specifying that the MAC
addresses should be lowercase without separators.
[Switch] mac-authentication authmode usernameasmacaddress usernameformat without-hyphen

# Specify the ISP domain for MAC authentication.
[Switch] mac-authentication domain aabbcc.net

# Enable port security.
[Switch] port-security enable

# Set the port security mode to mac-authentication.
[Switch] interface Ethernet 1/0/1
[Switch-Ethernet1/0/1] port-security port-mode mac-authentication

# Configure the port to drop packets whose source addresses are the same as that of the packet failing
MAC authentication after intrusion protection is triggered.
[Switch-Ethernet1/0/1] port-security intrusion-mode blockmac
```

Port Security Mode userLoginWithOUI Configuration Example

Network requirements

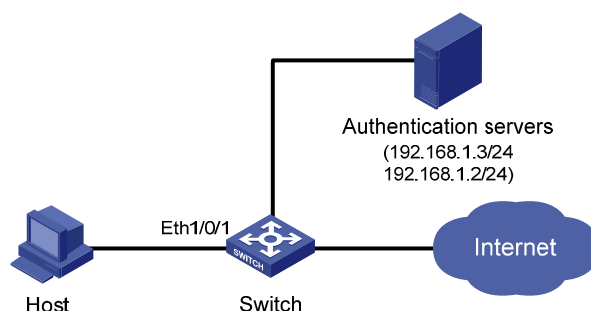
The host connects to the switch through port Ethernet 1/0/1, and the switch authenticates the host with a RADIUS server. If the authentication succeeds, the host is authorized to access the Internet.

Restrict Ethernet 1/0/1 of the switch as follows:

- Allow one 802.1X user to get online.
- Set two OUI values, and allow only one user whose MAC address matches one of the two OUI values to get online.
- Configure port security trapping to monitor the operations of the 802.1X-authenticated user.

Network diagram

Figure 1-7 Network diagram for configuring port security mode userLoginWithOUI



Configuration procedure



Note

- The following configurations involve some AAA/RADIUS configuration commands. For details about the commands, refer to *AAA Operation*.
 - Configurations on the user host and the RADIUS server are omitted.
-

- Configure RADIUS parameters

Create a RADIUS scheme named **radius1**.

```
<Switch> system-view
```

```
[Switch] radius scheme radius1
```

Specify the primary RADIUS authentication server and primary RADIUS accounting server.

```
[Switch-radius-radius1] primary authentication 192.168.1.3
```

```
[Switch-radius-radius1] primary accounting 192.168.1.2
```

Specify the secondary RADIUS authentication server and secondary RADIUS accounting server.

```
[Switch-radius-radius1] secondary authentication 192.168.1.2
```

```
[Switch-radius-radius1] secondary accounting 192.168.1.3
```

Set the shared key for message exchange between the switch and the RADIUS authentication servers to **name**.

```
[Switch-radius-radius1] key authentication name
```

Set the shared key for message exchange between the switch and the accounting RADIUS servers to **name**.

```
[Switch-radius-radius1] key accounting name
```

Set the interval and the number of packet transmission attempts for the switch to send packets to the RADIUS server.

```
[Switch-radius-radius1] timer 5
```

```
[Switch-radius-radius1] retry 5
```

Set the timer for the switch to send real-time accounting packets to the RADIUS server to 15 minutes.

```
[Switch-radius-radius1] timer realtime-accounting 15
```

Configure the switch to send a username without the domain name to the RADIUS server.

```
[Switch-radius-radius1] user-name-format without-domain
```

```
[Switch-radius-radius1] quit
```

Create a domain named **aabbcc.net** and enter its view.

```
[Switch] domain aabbcc.net
```

Specify **radius1** as the RADIUS scheme of the user domain, and the local authentication scheme as the backup scheme when the RADIUS server is not available.

```
[Switch-isp-aabbcc.net] scheme radius-scheme radius1 local
```

Set the maximum number of users of the ISP domain to 30.

```
[Switch-isp-aabbcc.net] access-limit enable 30
```

Enable the idle disconnecting function and set the related parameters.

```
[Switch-isp-aabbcc.net] idle-cut enable 20 2000
```

```
[Switch-isp-aabbcc.net] quit

# Set aabbcc.net as the default user domain.
[Switch] domain default enable aabbcc.net

# Create a local user.
[Switch] local-user localuser
[Switch-luser-localuser] service-type lan-access
[Switch-luser-localuser] password simple localpass
• Configure port security

# Enable port security.
[Switch] port-security enable

# Add two OUI values.
[Switch] port-security oui 1234-0100-1111 index 1
[Switch] port-security oui 1234-0200-1111 index 2

# Set the port security mode to userlogin-withoui.
[Switch] interface Ethernet 1/0/1
[Switch-Ethernet1/0/1] port-security port-mode userlogin-withoui
[Switch-Ethernet1/0/1] quit

# Configure port security trapping.
[Switch] port-security trap dot1xlogfailure
[Switch] port-security trap dot1xlogon
[Switch] port-security trap dot1xlogoff
```

Port Security Mode **macAddressElseUserLoginSecureExt** Configuration Example

Network requirements

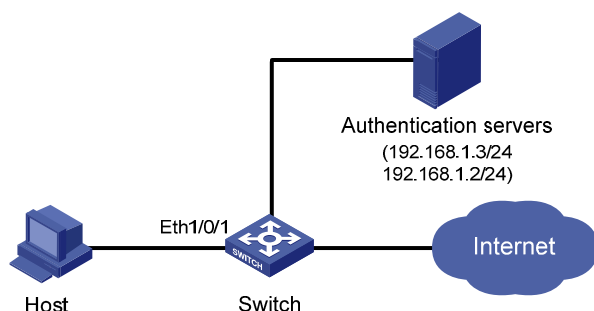
The host connects to the switch through port Ethernet 1/0/1, and the switch authenticates the host with a RADIUS server. If the authentication succeeds, the host is authorized to access the Internet.

Restrict port Ethernet 1/0/1 of the switch as follows:

- Perform MAC authentication of users and then 802.1X authentication if MAC authentication fails.
- Allow up to 64 802.1X authenticated users to get online. The total number of 802.1X authenticated users and MAC authenticated users cannot exceed 200.
- All users belong to the domain **aabbcc.net**, and each user uses the MAC address of the host as the username and password for authentication.
- Enable NTK feature to prevent packets from being sent to unknown destination MAC addresses.

Network diagram

Figure 1-8 Network diagram for configuring port security mode macAddressElseUserLoginSecureExt



Configuration procedure



Note

- The following configurations involve some AAA/RADIUS configuration commands. For details about the commands, refer to *AAA Operation*.
- Configurations on the user host and the RADIUS server are omitted.

- Configure RADIUS parameters

Create a RADIUS scheme named **radius1**.

```
<Switch> system-view
```

```
[Switch] radius scheme radius1
```

Specify the primary RADIUS authentication server and primary RADIUS accounting server.

```
[Switch-radius-radius1] primary authentication 192.168.1.3
```

```
[Switch-radius-radius1] primary accounting 192.168.1.2
```

Specify the secondary RADIUS authentication server and secondary RADIUS accounting server.

```
[Switch-radius-radius1] secondary authentication 192.168.1.2
```

```
[Switch-radius-radius1] secondary accounting 192.168.1.3
```

Set the shared key for message exchange between the switch and the RADIUS authentication servers to **name**.

```
[Switch-radius-radius1] key authentication name
```

Set the shared key for message exchange between the switch and the accounting RADIUS servers to **name**.

```
[Switch-radius-radius1] key accounting name
```

Set the interval and the number of packet transmission attempts for the switch to send packets to the RADIUS server.

```
[Switch-radius-radius1] timer 5
```

```
[Switch-radius-radius1] retry 5
```

Set the timer for the switch to send real-time accounting packets to the RADIUS server to 15 minutes.

```

[Switch-radius-radius1] timer realtime-accounting 15

# Configure the switch to send a username without the domain name to the RADIUS server.
[Switch-radius-radius1] user-name-format without-domain
[Switch-radius-radius1] quit

# Create a domain named aabbcc.net and enter its view.
[Switch] domain aabbcc.net

# Specify the RADIUS scheme for the domain.
[Switch-isp-aabbcc.net] scheme radius-scheme radius1

# Enable the idle disconnecting function and set the related parameters.
[Switch-isp-aabbcc.net] idle-cut enable 20 2000
[Switch-isp-aabbcc.net] quit

# Set aabbcc.net as the default user domain.
[Switch] domain default enable aabbcc.net

# Set the maximum number of concurrent 802.1X users.
[Switch] dot1x max-user 64

# Configure the switch to use MAC addresses as usernames for authentication, specifying that the MAC
addresses should be lowercase without separators.
[Switch] mac-authentication authmode usernameasmacaddress usernameformat without-hyphen

# Specify the ISP domain for MAC authentication.
[Switch] mac-authentication domain aabbcc.net

# Enable port security.
[Switch] port-security enable

# Set the maximum number of secure MAC addresses allowed on the port to 200.
[Switch] interface Ethernet 1/0/1
[Switch-Ethernet1/0/1] port-security max-mac-count 200

# Set the port security mode to mac-else-userlogin-secure-ext.
[Switch-Ethernet1/0/1] port-security port-mode mac-else-userlogin-secure-ext

# Set the NTK mode of the port to ntkonly.
[Switch-Ethernet1/0/1] port-security ntk-mode ntkonly

```

Port Security Mode **macAddressAndUserLoginSecureExt** Configuration Example

Network requirements

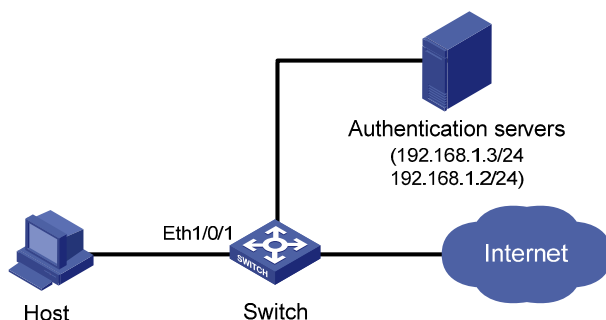
The host connects to the switch through port Ethernet 1/0/1, and the switch authenticates the host with a RADIUS server. After the authentication succeeds, the host is authorized to access the Internet.

Restrict Ethernet 1/0/1 of the switch as follows:

- Perform MAC authentication for users and then 802.1X authentication after MAC authentication succeeds.
- All users belong to the domain **aabbcc.net**, and each user uses the MAC address of the host as the username and password for authentication.

Network diagram

Figure 1-9 Network diagram for configuring port security mode macAddressElseUserLoginSecureExt



Configuration procedure



Note

- The following configurations involve some AAA/RADIUS configuration commands. For details about the commands, refer to *AAA Operation*.
- Configurations on the user host and the RADIUS server are omitted.

- Configure RADIUS parameters

Create a RADIUS scheme named **radius1**.

```
<Switch> system-view
```

```
[Switch] radius scheme radius1
```

Specify the primary RADIUS authentication server and primary RADIUS accounting server.

```
[Switch-radius-radius1] primary authentication 192.168.1.3
```

```
[Switch-radius-radius1] primary accounting 192.168.1.2
```

Specify the secondary RADIUS authentication server and secondary RADIUS accounting server.

```
[Switch-radius-radius1] secondary authentication 192.168.1.2
```

```
[Switch-radius-radius1] secondary accounting 192.168.1.3
```

Set the shared key for message exchange between the switch and the RADIUS authentication servers to **name**.

```
[Switch-radius-radius1] key authentication name
```

Set the shared key for message exchange between the switch and the accounting RADIUS servers to **name**.

```
[Switch-radius-radius1] key accounting name
```

Set the interval and the number of packet transmission attempts for the switch to send packets to the RADIUS server.

```
[Switch-radius-radius1] timer 5
```

```
[Switch-radius-radius1] retry 5
```

Set the timer for the switch to send real-time accounting packets to the RADIUS server to 15 minutes.

```

[Switch-radius-radius1] timer realtime-accounting 15

# Configure the switch to send a username without the domain name to the RADIUS server.
[Switch-radius-radius1] user-name-format without-domain
[Switch-radius-radius1] quit

# Create a domain named aabbcc.net and enter its view.
[Switch] domain aabbcc.net

# Specify the RADIUS scheme for the domain.
[Switch-isp-aabbcc.net] scheme radius-scheme radius1

# Enable the idle disconnecting function and set the related parameters.
[Switch-isp-aabbcc.net] idle-cut enable 20 2000
[Switch-isp-aabbcc.net] quit

# Set aabbcc.net as the default user domain.
[Switch] domain default enable aabbcc.net

# Configure the switch to use the MAC address as username and password for authentication,
specifying that the MAC address should be lowercase without separators.
[Switch] mac-authentication authmode usernameasmacaddress usernameformat without-hyphen

# Specify the ISP domain for MAC authentication.
[Switch] mac-authentication domain aabbcc.net

# Enable port security.
[Switch] port-security enable

# Set the port security mode to macAddressAndUserLoginSecureExt.
[Switch] interface Ethernet 1/0/1
[Switch-Ethernet1/0/1] port-security port-mode mac-and-userlogin-secure-ext

```

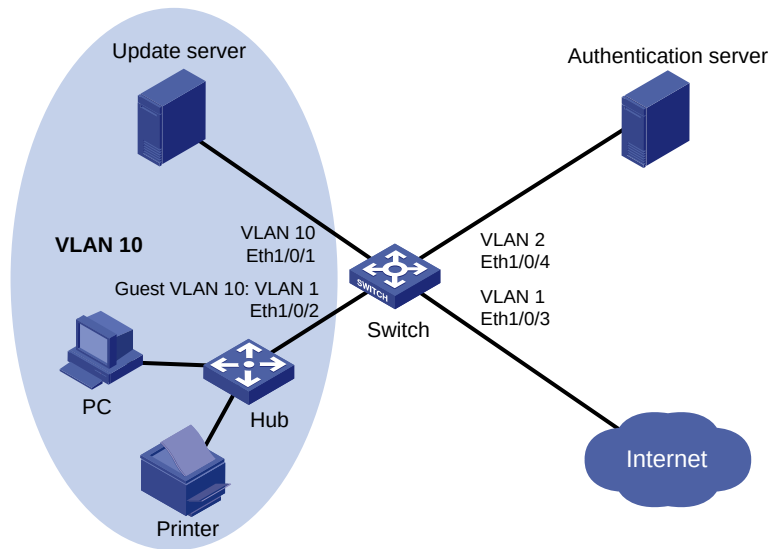
Guest VLAN Configuration Example

Network requirements

As shown in [Figure 1-10](#), Ethernet 1/0/2 connects to a PC and a printer, which are not used at the same time. Configure the port to operate in **macAddressOrUserLoginSecure** mode and specify a guest VLAN for the port.

- The PC must pass 802.1X authentication to connect to the network while the printer must pass MAC authentication to achieve network connectivity.
- The switch's port Ethernet 1/0/3 connects to the Internet. This port is assigned to VLAN 1. Normally, the port Ethernet 1/0/2 is also assigned to VLAN.
- VLAN 10 is intended to be a guest VLAN. It contains an update server for users to download and upgrade their client software. When a user fails authentication, port Ethernet 1/0/2 is added to VLAN 10. Then the user can access only VLAN 10. The port goes back to VLAN 1 when the user passes authentication.

Figure 1-10 Network diagram for guest VLAN configuration



Configuration procedure



Note

The following configuration steps include configurations of AAA and RADIUS. For details about these commands, refer to *AAA Command*. The configurations on the 802.1X client and the RADIUS server are omitted.

Configure RADIUS scheme 2000.

```
<Switch> system-view
[Switch] radius scheme 2000
[Switch-radius-2000] primary authentication 10.11.1.1 1812
[Switch-radius-2000] primary accounting 10.11.1.1 1813
[Switch-radius-2000] key authentication abc
[Switch-radius-2000] key accounting abc
[Switch-radius-2000] user-name-format without-domain
[Switch-radius-2000] quit
```

Configure the ISP domain and apply the scheme 2000 to the domain.

```
[Switch] domain system
[Switch-isp-system] scheme radius-scheme 2000
[Switch-isp-system] quit
```

Set the username type for MAC authentication to MAC address that requires no hyphenated lowercase MAC addresses as the username and password.

```
[Switch] mac-authentication authmode usernameasmacaddress usernameformat without-hyphen
```

Configure the ISP domain for MAC authentication.

```
[Switch] mac-authentication domain system
```

Enable port security.

```
[Switch] port-security enable
```

Specify the switch to trigger MAC authentication at an interval of 60 seconds.

```
[Switch] port-security timer guest-vlan timer 60
```

Create VLAN 10 and assign the port Ethernet 1/0/1 to it.

```
[Switch] vlan 10
```

```
[Switch-vlan10] port Ethernet 1/0/1
```

Set the security mode of the port Ethernet 1/0/2 to **macAddressOrUserLoginSecure**.

```
[Switch] interface Ethernet1/0/2
```

```
[Switch-Ethernet1/0/2] port-security port-mode userlogin-secure-or-mac
```

specify VLAN 10 as the guest VLAN of the port.

```
[Switch-Ethernet1/0/2] port-security guest-vlan 10
```

You can display the guest VLAN configuration information by the **display current-configuration** or **display interface ethernet 1/0/2** command.

If a user fails the authentication, you can use the **display vlan 10** command to view if the guest VLAN specified for the port is effective.

2 Port Binding Configuration



Note

The port-MAC-IP binding feature is added, For details, refer to [Configuring Port Binding](#).

When configuring port binding, go to these sections for information you are interested in:

- [Port Binding Overview](#)
- [Displaying and Maintaining Port Binding Configuration](#)
- [Port Binding Configuration Example](#)

Port Binding Overview

Introduction

Binding is a simple security mechanism. Through the binding configuration on the switch, you can filter the packets forwarded on the ports. When a port receives a packet, it searches the binding entry. If the information carried in the packet matches the information in the binding entry, the port forwards the packet. Otherwise, the port discards the packet.

Currently, the switch provides the following binding policies:

- Port-IP binding: binds a port to an IP address. On the bound port, the switch forwards only the packets sourced from the bound IP address.
- Port-MAC binding: binds a port to a MAC address. On the bound port, the switch forwards only the packets sourced from the bound MAC address.
- Port-MAC-IP binding: binds a MAC address and an IP address to a port. On the port, if the source IP address of a received packet matches a binding entry, the port forwards the packet only if the source MAC address of the packet also matches the entry. If the source IP address of a packet does not match any entry in the port-MAC-IP binding table, the port forwards the packet.
- IP-MAC binding: binds an IP address to a MAC address. The switch forwards only the packets sourced from the bound source MAC address and source IP address.



Note

When a port is bound, the binding applies only to the port.

Configuring Port Binding

Follow these steps to configure port binding:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Create a port-MAC-IP binding entry	In system view	am user-bind mac-addr <i>mac-address</i> ip-addr <i>ip-address</i> [interface <i>interface-type interface-number</i>]	Either is required. By default, no binding is configured.
	In Ethernet port view	interface <i>interface-type interface-number</i>	
		am user-bind { ip-addr <i>ip-address</i> mac-addr <i>mac-address</i> [ip-addr <i>ip-address</i>] }	



Note

- Ensure that the IP address or MAC address in a port binding is unique in all port bindings.
- For the same port, port-IP-MAC binding is mutually exclusive with port-IP binding.

Displaying and Maintaining Port Binding Configuration

To do...	Use the command...	Remarks
Display port binding information	display am user-bind [interface <i>interface-type interface-number</i> ip-addr <i>ip-addr</i> mac-addr <i>mac-addr</i>]	Available in any view

Port Binding Configuration Example

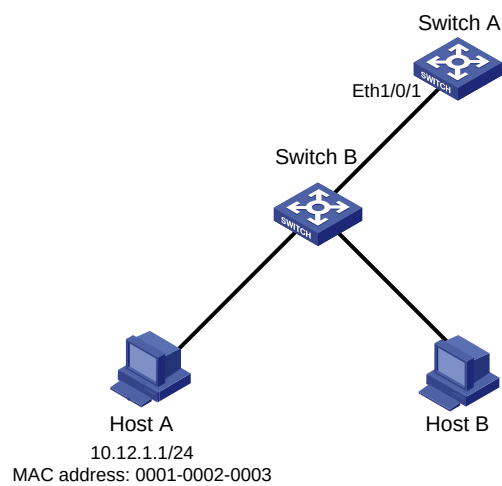
Port Binding Configuration Example

Network requirements

It is required to bind the MAC and IP addresses of Host A to Ethernet 1/0/1 on Switch A, so as to prevent malicious users from using the IP address they steal from Host A to access the network.

Network diagram

Figure 2-1 Network diagram for port binding configuration



Configuration procedure

Configure Switch A as follows:

Enter system view.

```
<SwitchA> system-view
```

Enter Ethernet 1/0/1 port view.

```
[SwitchA] interface Ethernet 1/0/1
```

Bind the MAC address and the IP address of Host A to Ethernet 1/0/1.

```
[SwitchA-Ethernet1/0/1] am user-bind mac-addr 0001-0002-0003 ip-addr 10.12.1.1
```

Table of Contents

1 DLDP Configuration	1-1
Overview	1-1
Introduction	1-1
DLDP Fundamentals	1-2
DLDP Configuration	1-8
Performing Basic DLDP Configuration	1-8
Resetting DLDP State	1-9
Displaying and Maintaining DLDP	1-10
DLDP Configuration Example	1-10

1 DLDP Configuration

When configuring DLDP, go to these sections for information you are interested in:

- [Overview](#)
- [DLDP Configuration](#)
- [DLDP Configuration Example](#)

Overview

Introduction

A special kind of links, namely, unidirectional links, may occur in a network. When a unidirectional link appears, 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 link can cause problems such as loops in a Spanning Tree Protocol (STP) enabled network.

As for fiber links, two kinds of unidirectional links exist:

- Fiber cross-connection, as shown in [Figure 1-1](#)
- Fibers that are not connected or disconnected, as shown in [Figure 1-2](#), the hollow lines in which refer to fibers that are not connected or disconnected.

The 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

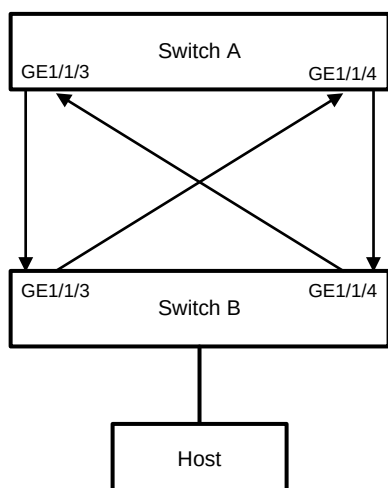
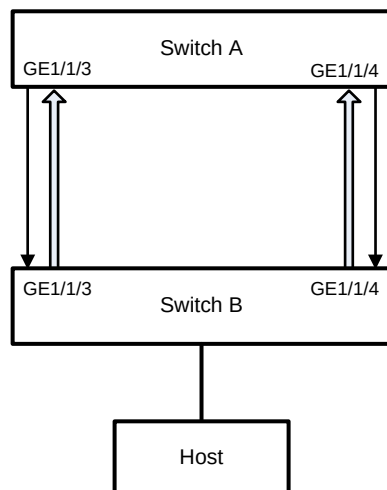


Figure 1-2 Fiber broken or not connected



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.
- 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.

 Note

- In order for DLDP to detect fiber disconnection in one direction, you need to configure the port to work in mandatory full duplex mode at a mandatory rate.
 - When the port determines the duplex mode and speed through auto-negotiation, even if DLDP is enabled, it does not take effect when the fiber in one direction is disconnected. In this case, the port is considered down.
-

DLDP Fundamentals

DLDP packets

DLDP detects link status by exchanging the following types of packets.

Table 1-1 DLDP packet types

DLDP packet type	Function
Advertisement	Notifies the neighbor devices of the existence of the local device. An advertisement packet carries only the local port information, and it does not require response from the peer end.

DLDP packet type	Function
RSY-Advertisement packets (referred to as RSY packets hereafter)	Advertisement packet with the RSY flag set to 1. RSY advertisement packets are sent to request synchronizing the neighbor information when neighbor information is not locally available or a neighbor information entry ages out.
Flush-Advertisement packets (referred to as flush packets hereafter)	Advertisement packet with the flush flag set to 1. A flush packet carries only the local port information (instead of the neighbor information) and is used to trigger neighbors to remove the information about the local device.
Probe	Probe packets are used to probe the existence of a neighbor. Echo packets are required from the corresponding neighbor. Probe packets carry the local port information. Neighbor information is optional for probe packets. A probe packet carrying neighbor information probes the specified neighbors; A probe packet carrying no neighbor information probes all the neighbors.
Echo	Response to probe packets. An echo packet carries the information about the response port and the neighbor information it maintains. Upon receiving an echo packet, a port checks whether the neighbor information carried in the echo packet is consistent with that of itself. If yes, the link between the local port and the neighbor is regarded as bidirectional.
Disable	Disable packets are used to notify the peer end that the local end is in the disable state. Disable packets carry only the local port information instead of the neighbor information. When a port detects a unidirectional link and enters the disable state, the port sends disable packets to the neighbor. A port enters the disable state upon receiving a disable packet.
LinkDown	Linkdown packets are used to notify unidirectional link emergencies (a unidirectional link emergency occurs when the local port is down and the peer port is up). Linkdown packets carry only the local port information instead of the neighbor information. In some conditions, a port is considered to be physically down if the link connecting to the port is physically abnormal (for example, the Rx line of the fiber on the port is disconnected, while the Tx line operates properly). But for the peer end, as Rx signals can still be received on the physical layer, the port is still considered to be normal. Such a situation is known as unidirectional link emergency. When a unidirectional link emergency occurs, DLDP sends linkdown packets immediately to inform the peer of the link abnormality. Without linkdown packets, the peer can detect the link abnormality only after a period when the corresponding neighbor information maintained on the neighbor device ages out, which is three times the advertisement interval. Upon receiving a linkdown packet, if the peer end operates in the enhanced mode, it enters the disable state, and sets the receiving port to the DLDP down state (auto shutdown mode) or gives an alarm to the user (manual shutdown mode).
Recover Probe	Recover probe packets are used to detect whether a link recovers to implement the port auto-recovery mechanism. Recover probe packets carry only the local port information instead of the neighbor information. They request for recover echo packets as the response. A port in the DLDP down state sends a recover probe packet every two seconds.
Recover Echo	Recover echo packets are response to recover probe packets in the port auto-recovery mechanism. A link is considered to restore to the bidirectional state if a port on one end sends a recover probe packet, receives a recover echo packet, and the neighbor information contained in the recover echo packet is consistent with that of the local port.

DLDP status

A link can be in one of these DLDP states: initial, inactive, active, advertisement, probe, disable, and delaydown.

Table 1-2 DLDP status

Status	Description
Initial	Initial status before DLDP is enabled.
Inactive	DLDP is enabled but the corresponding link is down
Active	This state indicates that: • DLDP is enabled and the link is up. • The neighbor entries are 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
Probe	DLDP sends packets to check whether the link is a unidirectional link. 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 remove the corresponding neighbor immediately, neither does it change 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.

DLDP timers

Table 1-3 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 5 seconds.
Probe sending timer	The interval is 0.5 seconds. In the probe state, DLDP sends two probe packets in a 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 remove the corresponding neighbor immediately, neither does it change 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.

DLDP operating mode

DLDP can operate in two modes: normal mode and enhanced mode.

Table 1-4 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.)



Note

- In normal DLDP mode, only fiber cross-connected unidirectional links (as shown in [Figure 1-1](#)) can be detected.
- In enhanced DLDP mode, two types of unidirectional links can be detected. One is fiber cross-connected links (as shown in [Figure 1-1](#)). The other refers to fiber pairs with one fiber not connected or disconnected (as shown in [Figure 1-2](#)). To detect unidirectional links that are of the latter type, you need to configure the ports to operate at specific speed and in full duplex mode. Otherwise, DLDP cannot take effect.

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 1-5 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 1-6 Process received DLDP packets

Packet type	Processing procedure	
Advertisement packet	Extracts neighbor information	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.
		If the neighbor entry already exists on the local device, DLDP updates the entry aging timer.
Flush packet	Deletes the neighbor entry from the local device	
Probe packet	Sends echo packets containing both neighbor and its own information to the peer	Creates the neighbor entry if this neighbor entry does not exist on the local device.
		If the neighbor entry already exists on the local device, updates the entry aging timer.

Packet type	Processing procedure				
Echo packet	Checks whether the local device is in the probe state	No	Discards this echo packet		
		Yes	Checks whether neighbor information in the packet is the same as that on the local device	No	Discards this echo packet
				Yes	Sets the neighbor flag bit to bidirectional link
					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.

3) If no echo packet is received from the neighbor, DLDP performs the following processing:

Table 1-7 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	

DLDP neighbor state

A DLDP neighbor can be in one of these two states: two way and unknown. You can check the state of a DLDP neighbor by using the **display dldp** command.

Table 1-8 Description on the two DLDP neighbor states

DLDP neighbor state	Description
Two way	The link to the neighbor operates properly.
Unknown	The device is detecting the neighbor and the neighbor state is unknown.

Link Auto-recovery Mechanism

If the shutdown mode of a port is set to auto shutdown, the port is set to the DLDP down state when DLDP detects the link connecting to the port is a unidirectional link. A port in DLDP down state does not forward service packets or receive/send protocol packets except DLDPDUs.

A port in the DLDP down state recovers when the corresponding link recovers. A port in the DLDP down state sends recover probe packets periodically. On receiving a correct recover echo packet (which means that the unidirectional link is restored to a bidirectional link), it is brought up by DLDP. The detailed process is as follows.

- 1) A port in the DLDP down state sends a recover probe packet every 2 seconds. Recover probe packets carry only the local port information.
- 2) Upon receiving a recover probe packet, the peer end responds with a recover echo packet.
- 3) Upon receiving a recover echo packet, the local end checks to see if the neighbor information carried in the recover echo packet is consistent with that of the local port. If yes, the link between

the local port and the neighbor is considered to be recovered to bidirectional, the port changes from the disable state to the active state, and neighboring relationship is reestablished between the local port and the neighbor.



Note

Only ports in the DLDAP down state can send and process recover probe packets and recover echo packets. The auto-recovery mechanism does apply to ports that are shut down manually.

DLDAP Configuration

Performing Basic DLDAP Configuration

Follow these steps to perform basic DLDAP configuration:

To do ...			Use the command ...	Remarks
Enter system view			system-view	—
Enable DLDAP	Enable DLDAP on all optical ports of the switch		dldap enable	Required. By default, DLDAP is disabled.
	Enable DLDAP on the current port (a non-optical port or an optical port)	Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	
		Enable DLDAP	dldap enable	
Set the authentication mode and password			dldap authentication-mode { none simple <i>simple-password</i> md5 <i>md5-password</i> }	Optional. By default, the authentication mode is none .
Set the interval of sending DLDAP packets			dldap interval <i>timer-value</i>	Optional. By default, the interval is 5 seconds.
Set the delaydown timer			dldap delaydown-timer <i>delaydown-time</i>	Optional By default, the delaydown timer expires after 1 second it is triggered.
Set the DLDAP handling mode when an unidirectional link is detected			dldap unidirectional-shutdown { auto manual }	Optional. By default, the handling mode is auto .
Set the DLDAP operating mode			dldap work-mode { enhance normal }	Optional. By default, DLDAP works in normal mode.

Note the following when performing basic DLDAP configuration.

- DLDAP can detect unidirectional links only after the links are connected. Therefore, before enabling DLDAP, make sure that optical fibers or copper twisted pairs are connected.

- To ensure unidirectional links can be detected, make sure DLDAP is enabled on both sides; and the interval for sending advertisement packets, authentication mode, and password are the same on both sides.
- The interval for sending advertisement packets ranges from 1 to 100 seconds and defaults to 5 seconds. You can adjust this setting as needed to enable DLDAP to respond in time to link failures. If the interval is too long, STP loops may occur before unidirectional links are terminated; if the interval is too short, network traffic may increase in vain and available bandwidth decreases. Normally, the interval is shorter than one-third of the STP convergence time, which is generally 30 seconds.
- DLDAP does not process any link aggregation control protocol (LACP) event, and treats each link in the aggregation group as independent.
- When connecting two DLDAP-enabled devices, make sure the software running on them is of the same version. Otherwise, DLDAP may operate improperly.
- When you use the **dldap enable/dldap disable** command in system view to enable/disable DLDAP on all optical ports of the switch, the configuration takes effect on the existing optical ports, instead of those added subsequently.
- Make sure the authentication mode and password configured on both sides are the same for DLDAP to operate properly.
- When DLDAP 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 disconnected.
- When DLDAP works in normal mode, the system can identify unidirectional links caused by fiber cross-connection.
- When the device is busy with services and the CPU utilization is high, DLDAP may issue mistaken reports. You are recommended to configure the operating mode of DLDAP as manual after unidirectional links are detected, so as to reduce the influence of mistaken reports.

Resetting DLDAP State

You can reset the DLDAP state for the ports shut down by DLDAP due to unidirectional links to enable DLDAP detection again.



Note

This function is only applicable to ports that are in DLDAP down state.

Follow these steps to reset DLDAP state:

To do ...	Use the command ...	Remarks
Reset DLDAP state for all the ports shut down by DLDAP	system-view	Select either of the two.
	dldap reset	
Reset the DLDAP state for a port shut down by DLDAP	interface <i>interface-type</i> <i>interface-number</i>	
	dldap reset	

Displaying and Maintaining DLDP

To do ...	Use the command ...	Remarks
Display the DLDP configuration of a unit or a port	display dldp { <i>unit-id</i> <i>interface-type interface-number</i> }	Available in any view.

DLDP Configuration Example

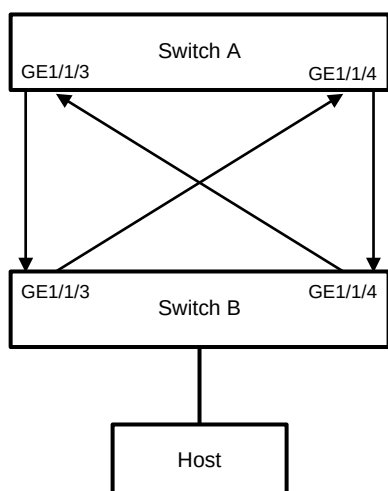
Network requirements

As shown in [Figure 1-3](#),

- Switch A and Switch B are connected through two pairs of fibers. Both of them support DLDP. All the ports involved operate in mandatory full duplex mode, with their rates all being 1,000 Mbps.
- Suppose the fibers between Switch A and Switch B are cross-connected. DLDP disconnects the unidirectional links after detecting them.
- After the fibers are connected correctly, the ports shut down by DLDP are restored.

Network diagram

Figure 1-3 Network diagram for DLDP configuration



Configuration procedure

1) Configure Switch A

Configure the ports to work in mandatory full duplex mode at a rate of 1,000 Mbps.

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/1/3
[SwitchA-GigabitEthernet1/1/3] duplex full
[SwitchA-GigabitEthernet1/1/3] speed 1000
[SwitchA-GigabitEthernet1/1/3] quit
[SwitchA] interface gigabitethernet 1/1/4
[SwitchA-GigabitEthernet1/1/4] duplex full
[SwitchA-GigabitEthernet1/1/4] speed 1000
[SwitchA-GigabitEthernet1/1/4] quit
```

Enable DLDP globally.

```
[SwitchA] dldp enable
# Set the interval for sending DLDP packets to 15 seconds.
[SwitchA] dldp interval 15
# Configure DLDP to work in enhanced mode.
[SwitchA] dldp work-mode enhance
# Set the DLDP handling mode for unidirectional links to auto.
[SwitchA] dldp unidirectional-shutdown auto
# Display the DLDP state.
[SwitchA] 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 shut down by DLDP.

```
[SwitchA] dldp reset
```

2) Configure Switch B

The configuration of Switch B is the same to that of Switch A and is thus omitted.

Table of Contents

1 MAC Address Table Management	1-1
Overview	1-1
Introduction to MAC Address Table	1-1
Introduction to MAC Address Learning	1-2
Managing MAC Address Table	1-4
Configuring MAC Address Table Management	1-5
MAC Address Table Management Configuration Task List	1-5
Configuring a MAC Address Entry	1-5
Setting the MAC Address Aging Timer	1-6
Setting the Maximum Number of MAC Addresses a Port Can Learn	1-7
Enabling Destination MAC Address Triggered Update	1-7
Assigning MAC Addresses for Ethernet Ports	1-8
Displaying MAC Address Table Information	1-9
Configuration Example	1-9
Adding a Static MAC Address Entry Manually	1-9

1 MAC Address Table Management

When configuring MAC address table management, go to these sections for information you are interested in:

- [Overview](#)
- [Configuring MAC Address Table Management](#)
- [Displaying MAC Address Table Information](#)
- [Configuration Example](#)



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 part related to multicast protocol.
 - The function of destination MAC address triggered update was introduced. For more information, refer to [Enabling Destination MAC Address Triggered Update](#).
 - The function of assigning MAC addresses to Ethernet ports was introduced. For more information, refer to [Assigning MAC Addresses for Ethernet Ports](#).
-

Overview

Introduction to MAC Address Table

An Ethernet switch is mainly used to forward packets at the data link layer, that is, transmit the packets to the corresponding ports according to the destination MAC address of the packets. To forward packets quickly, a switch maintains a MAC address table, which is a Layer 2 address table recording the MAC address-to-forwarding port association. Each entry in a MAC address table contains the following fields:

- Destination MAC address
- ID of the VLAN which a port belongs to
- Forwarding egress port numbers on the local switch

When forwarding a packet, an Ethernet switch adopts one of the two forwarding methods based upon the MAC address table entries.

- Unicast forwarding: If the destination MAC address carried in the packet is included in a MAC address table entry, the switch forwards the packet through the forwarding egress port in the entry.
- Broadcast forwarding: If the destination MAC address carried in the packet is not included in the MAC address table, the switch broadcasts the packet to all ports except the one receiving the packet.

Introduction to MAC Address Learning

MAC address table entries can be updated and maintained through the following two ways:

- Manual configuration
- MAC address learning

Generally, the majority of MAC address entries are created and maintained through MAC address learning. The following describes the MAC address learning process of a switch:

- 1) As shown in [Figure 1-1](#), User A and User B are both in VLAN 1. When User A communicates with User B, the packet from User A needs to be transmitted to Ethernet 1/0/1. At this time, the switch records the source MAC address of the packet, that is, the address MAC-A of User A to the MAC address table of the switch, forming an entry shown in [Figure 1-2](#).

Figure 1-1 MAC address learning diagram (1)

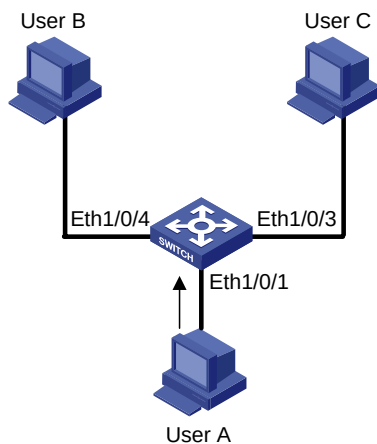
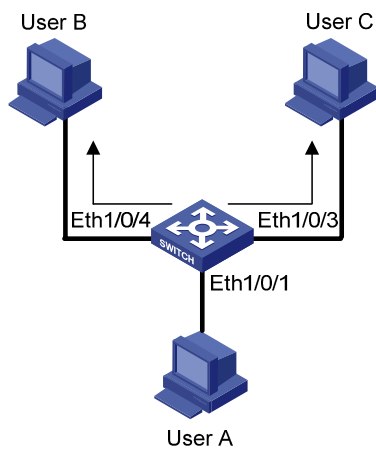


Figure 1-2 MAC address table entry of the switch (1)

MAC-address	Port	VLAN ID
MAC-A	Ethernet1/0/1	1

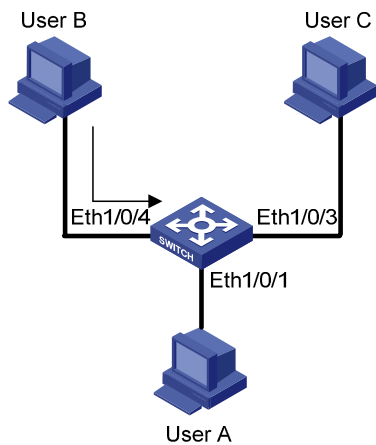
- 2) After learning the MAC address of User A, the switch starts to forward the packet. Because there is no MAC address and port information of User B in the existing MAC address table, the switch forwards the packet to all ports except Ethernet 1/0/1 to ensure that User B can receive the packet.

Figure 1-3 MAC address learning diagram (2)



- 3) Because the switch broadcasts the packet, both User B and User C can receive the packet. However, User C is not the destination device of the packet, and therefore does not process the packet. Normally, User B will respond to User A, as shown in [Figure 1-4](#). When the response packet from User B is sent to Ethernet 1/0/4, the switch records the association between the MAC address of User B and the corresponding port to the MAC address table of the switch.

Figure 1-4 MAC address learning diagram (3)



- 4) At this time, the MAC address table of the switch includes two forwarding entries shown in [Figure 1-5](#). When forwarding the response packet, the switch unicasts the packet instead of broadcasting it to User A through Ethernet 1/0/1, because MAC-A is already in the MAC address table.

Figure 1-5 MAC address table entries of the switch (2)

MAC-address	Port	VLAN ID
MAC-A	Ethernet1/0/1	1
MAC-B	Ethernet1/0/4	1

- 5) After this interaction, the switch directly unicasts the packets destined for User A and User B based on the corresponding MAC address table entries.



Note

- Under some special circumstances, for example, User B is unreachable or User B receives the packet but does not respond to it, the switch cannot learn the MAC address of User B. Hence, the switch still broadcasts the packets destined for User B.
 - The switch learns only unicast addresses by using the MAC address learning mechanism but directly drops any packet with a broadcast source MAC address.
-

Managing MAC Address Table

Aging of MAC address table

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 starts an aging timer for an entry when dynamically creating the entry. The switch removes the MAC address entry if no more packets with the MAC address recorded in the entry are received within the aging time.



Note

- The MAC address aging timer only takes effect on dynamic MAC address entries.
 - With the destination MAC address triggered update function enabled, when a switch finds a packet with a destination address matching one MAC address entry within the aging time, it updates the entry and restarts the aging timer.
-

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

Configuring MAC Address Table Management

MAC Address Table Management Configuration Task List

Complete the following tasks to configure MAC address table management:

Task	Remarks
Configuring a MAC Address Entry	Required
Setting the MAC Address Aging Timer	Optional
Setting the Maximum Number of MAC Addresses a Port Can Learn	Optional
Enabling Destination MAC Address Triggered Update	Optional
Assigning MAC Addresses for Ethernet Ports	Optional

Configuring a MAC Address Entry

You can add, modify, or remove a MAC address entry, remove all MAC address entries 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.

Adding a MAC address entry in system view

Follow these steps to add a MAC address entry in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Add a MAC address entry	mac-address { static dynamic blackhole } <i>mac-address interface interface-type interface-number vlan vlan-id</i>	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.

Adding a MAC address entry in Ethernet port view

Follow these steps to add a MAC address entry in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Add a MAC address entry	mac-address { static dynamic blackhole } <i>mac-address</i> vlan <i>vlan-id</i>	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.

Setting the MAC Address Aging Timer

Setting an appropriate MAC address aging timer is important for the switch to run efficiently.

- If the aging timer is set 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 timer is set too short, the switch may remove valid MAC address entries. This decreases the forwarding performance of the switch.

Follow these steps to set aging time of MAC address entries:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the MAC address aging timer	mac-address timer { aging <i>age</i> no-aging }	Required The default is 300 seconds.

Normally, you are recommended to use the default aging timer, namely, 300 seconds. The **no-aging** keyword specifies that MAC address entries never age out.



Note

MAC address aging configuration applies to all ports, but only takes effect on dynamic MAC addresses, which are either learnt or configured.

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. By searching the MAC address table, the switch directly forwards the packets destined for these MAC addresses through the hardware, improving the forwarding efficiency. A MAC address table too big in size may prolong the time for searching MAC address entries, thus decreasing the forwarding performance of the switch.

By setting the maximum number of MAC addresses that can be learnt from individual ports, the administrator 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.

Follow these steps to set the maximum number of MAC addresses a port can learn:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Set the maximum number of MAC addresses the port can learn	mac-address max-mac-count <i>count</i>	Required By default, the number of the MAC addresses a port can learn is not limited.



Note

If you have configured the maximum number of MAC addresses that a port can learn, you cannot enable the MAC address authentication or port security functions on the port, and vice versa.

Enabling Destination MAC Address Triggered Update

By default, a switch updates its MAC address entries based on the source MAC addresses of packets. However, this may cause the switch to perform unnecessary broadcasts in some applications. For example, when a port aggregation group is used in an IRF fabric for communications, MAC address entries of some ports in the aggregation group may not be updated in time, resulting in unnecessary broadcasts.

The destination MAC address triggered update function solves the above problem by allowing the switch to update its MAC address entries according to destination MAC addresses in addition to source MAC addresses. This function improves the availability of the MAC address table.

Follow these steps to enable destination MAC address triggered update:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable destination MAC address triggered update	mac-address aging destination-hit enable	Required Disabled by default

Assigning MAC Addresses for Ethernet Ports

By default, no Ethernet port of an S3600 switch is configured with a MAC address. Therefore, when the switch sends Layer 2 protocol packets, for example, BPDUs of STP, it uses the MAC address predefined in the protocol as the source address to send the BPDUs. As switches in your network may use the same source MAC address for Layer 2 protocol data units (PDUs), different ports on a switch may learn the same MAC address, thus affecting the maintenance of the MAC address table.

To avoid the problem, you are allowed to assign MAC addresses to the Ethernet ports on an S3600 series switch. The idea is to assign a MAC address (called the start port MAC address) for the start Ethernet port, that is, Ethernet 1/0/1, and each of the following ports uses the MAC address of the preceding port plus 1 as its MAC address.

For example, if you configure 000f-e200-0001 as the start port MAC address, then port Ethernet 1/0/2 will take MAC address 000f-e200-0002, and so on.

Follow these steps to configure the start port MAC address:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the start port MAC address	port-mac <i>start-mac-address</i>	Required No start port MAC address is configured by default.



Note

The start port MAC address must be a valid unicast address.

With the port MAC address configuration, the switch uses the MAC address of a port as the source MAC address when sending the following Layer 2 PDUs out of the port:

- LACP
- STP
- NDP/NTDP
- GVRP
- DLDP

Port MAC address configuration does not affect service packet forwarding.

Displaying MAC Address Table Information

To do...	Use the command...	Remarks
Display information about the MAC address table	display mac-address [<i>display-option</i>]	Available in any view
Display the aging time of the dynamic MAC address entries in the MAC address table	display mac-address aging-time	
Display the configured start port MAC address	display port-mac	

Configuration Example

Adding a Static MAC Address Entry Manually

Network requirements

The server connects to the switch through Ethernet 1/0/2. To prevent the switch from broadcasting packets destined for the server, it is required to add the MAC address of the server to the MAC address table of the switch, which then forwards packets destined for the server through Ethernet 1/0/2.

- The MAC address of the server is 000f-e20f-dc71.
- Port Ethernet 1/0/2 belongs to VLAN 1.

Configuration procedure

Enter system view.

```
<Sysname> system-view
```

```
[Sysname]
```

Add a MAC address, with the VLAN, ports, and states specified.

```
[Sysname] mac-address static 000f-e20f-dc71 interface Ethernet 1/0/2 vlan 1
```

Display information about the current MAC address table.

```
[Sysname] display mac-address interface Ethernet 1/0/2
```

```
MAC ADDR          VLAN ID  STATE          PORT INDEX      AGING TIME(s)
000f-e20f-dc71     1        Config static  Ethernet1/0/2    NOAGED
000f-e20f-a7d6     1        Learned        Ethernet1/0/2    AGING
000f-e20f-b1fb     1        Learned        Ethernet1/0/2    AGING
000f-e20f-f116     1        Learned        Ethernet1/0/2    AGING
--- 4 mac address(es) found on port Ethernet1/0/2 ---
```

Table of Contents

1 Auto Detect Configuration	1-1
Introduction to the Auto Detect Function	1-1
Auto Detect Configuration	1-1
Auto Detect Basic Configuration	1-2
Auto Detect Implementation in Static Routing	1-2
Auto Detect Implementation in VRRP	1-3
Auto Detect Implementation in VLAN Interface Backup	1-4
Auto Detect Configuration Examples	1-6
Configuration Example for Auto Detect Implementation with Static Routing	1-6
Configuration Example for Auto Detect Implementation with VRRP	1-7
Configuration Example for Auto Detect Implementation with VLAN Interface Backup	1-8

1 Auto Detect Configuration

When configuring the auto detect function, go to these sections for information you are interested in:

- [Introduction to the Auto Detect Function](#)
- [Auto Detect Configuration](#)
- [Auto Detect Configuration Examples](#)

Introduction to the Auto Detect Function

The Auto Detect function uses Internet Control Message Protocol (ICMP) request/reply packets to test network connectivity regularly between the Auto Detect-enabled switch and the detected object.

The detected object of the Auto Detect function is a detected group, which is a set of IP addresses. To check the reachability to a detected group, a switch enabled with Auto Detect sends ICMP requests to the IP addresses in the group and waits for the ICMP replies from the group based on the user-defined policy (which includes the number of ICMP requests and the timeout waiting for a reply). Then according to the check result, the switch determines whether to make the applications using the detected group take effect.

Currently, the following features are used in conjunction with Auto Detect:

- Static route
- Virtual Router Redundancy Protocol (VRRP)
- Interface backup



Note

- When the Auto Detect feature is used in conjunction with multiple features (static routing, VRRP, or interface backup), if the detected object is the same, you can apply a detected group to multiple features, thus reducing the configuration workload.
 - For details about static routing, refer to the Routing Protocol part of the manual.
 - For details about VRRP, refer the VRRP part of the manual.
-

Auto Detect Configuration

Complete the following tasks to configure auto detect:

Task	Remarks
Auto Detect Basic Configuration	Required
Auto Detect Implementation in Static Routing	Optional

Task	Remarks
Auto Detect Implementation in VRRP	Optional
Auto Detect Implementation in VLAN Interface Backup	Optional

Auto Detect Basic Configuration

Follow these steps to configure the auto detect function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a detected group and enter detected group view	detect-group <i>group-number</i>	Required
Add an IP address to be detected to the detected group	detect-list <i>list-number</i> ip address <i>ip-address</i> [nexthop <i>ip-address</i>]	Required
Specify a relationship between detected IP addresses in the group	option [and or]	Optional By default, the and keyword is specified.
Set an interval between detecting operations	timer loop <i>interval</i>	Optional By default, the detecting interval is 15 seconds.
Set the number of ICMP requests during a detecting operation	retry <i>retry-times</i>	Optional By default, the number is 2.
Set a timeout waiting for an ICMP reply	timer wait <i>seconds</i>	Optional By default, the timeout is 2 seconds.
Display the detected group configuration	display detect-group [<i>group-number</i>]	Available in any view



Note

If the relationship between IP addresses of a detected group is **and**, any unreachable IP address in the group makes the detected group unreachable and the remaining IP addresses will not be detected. If the relationship is **or**, any reachable IP address makes the detected group reachable and the remaining IP addresses will not be detected.

Auto Detect Implementation in Static Routing

A static route is a special route. It is manually configured by the administrator. With a static route configured, the data packets to the specified destination will be forwarded along the path specified by the administrator.

The disadvantage of using static routes is that they cannot adapt to network topology changes. If a fault or a topology change occurs to the network, the routes may be unreachable and the network may break.

To avoid such problems, you can configure another route to back up the static route and use the Auto Detect function to judge the validity of the static route. If the static route is valid, packets are forwarded according to the static route, and the other route is standby. If the static route is invalid, packets are forwarded according to the backup route. In this way, the communication is not interrupted, and the network reliability is improved.

You can bind the static route with a detected group. The Auto Detect function will then detect the group and judge the validity of the static route according to the returned reachable/unreachable information..

- The static route is valid if the detected group is **reachable**.
- The static route is invalid if the detected group is **unreachable**.



Note

You need to create the detected group before performing the following operations.

Follow these steps to configure the auto detect function for a static route:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Bind a detected group to a static route	ip route-static <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-type interface-number</i> <i>next-hop</i> } [preference <i>preference-value</i>] [reject blackhole] detect-group <i>group-number</i>	Required

Auto Detect Implementation in VRRP



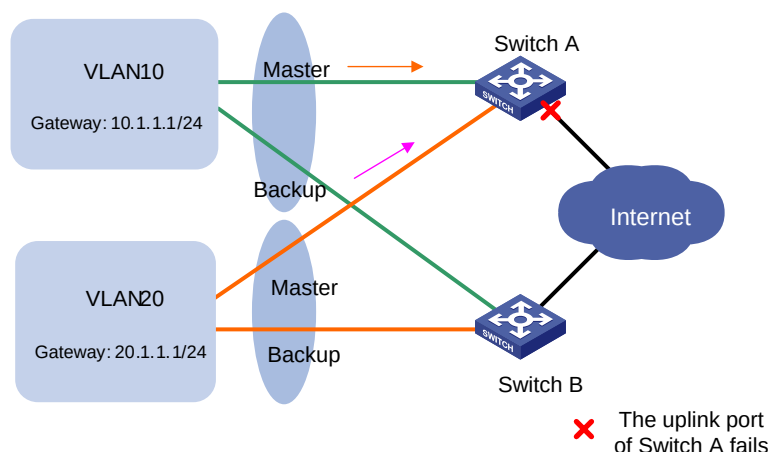
Note

Currently, auto detect implementation in VRRP is only supported on S3600-EI series Ethernet switches.

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant protocol. It assigns a set of switches acting as gateways to a backup group, which forms a virtual switch. Switches in the backup group elect a master switch based on priorities to take the responsibility of traffic forwarding. The other switches operate as backup switches. When the master switch fails, a backup switch takes over to forward traffic, thus guaranteeing the hosts in the network can communicate with the external network uninterruptedly through the virtual switch.

However, when the uplink of a switch fails, the backup group cannot sense the uplink failure. If the uplink of the master switch fails, the hosts in the LAN cannot access the external network, as shown in [Figure 1-1](#).

Figure 1-1 The uplink of the master switch fails



Using VRRP together with the Auto Detect function, you can change the priority of a switch according to the uplink status. On the master switch of the VRRP backup group, you can use the Auto Detect function to detect the paths between the master switch and other networks, and control the priority of the master switch according to the returned reachable/unreachable information, thus implementing automatic master/backup switchover and guaranteeing the communication is not interrupted.

- The master switch keeps as Master when the detected group is **reachable**.
- The priority of the master switch decreases and thus becomes a Backup when the detected group is **unreachable**.



Note

You need to create the detected group and perform VRRP-related configurations before the following operations.

Follow these steps to configure the auto detect function for VRRP:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	—
Enable the auto detect function for VRRP	vrpp vrid <i>virtual-router-id</i> track detect-group <i>group-number</i> [reduced value-reduced]	Required

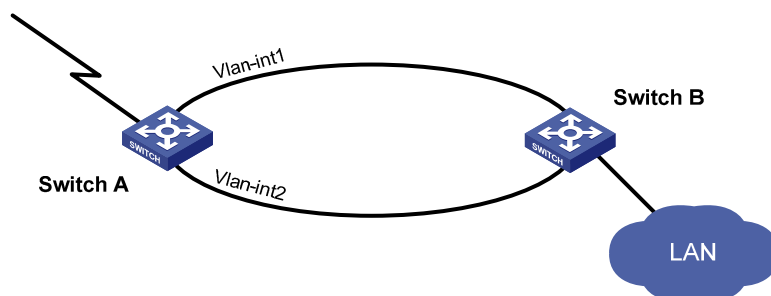
Auto Detect Implementation in VLAN Interface Backup

VLAN interface backup means backing up the VLAN interfaces on a devices. Usually, the master VLAN interface transmits traffic, while the backup VLAN interfaces stay standby. When the master VLAN interface or the link connected to the VLAN interface fails and thus cannot transmit traffic, the backup VLAN interface can be used for communication. In this way, the network reliability is improved.

As shown in [0](#), Switch A has two VLAN interfaces: VLAN-interface 1 and VLAN-interface 2. The two VLAN-interfaces back up each other. Normally, VLAN-interface 1 transmits traffic, while VLAN-interface

2 stays standby. When VLAN-interface 1 or the link connected to VLAN-interface 1 fails and thus cannot transmit traffic normally, VLAN-interface 2 takes over to transmit traffic. In this way, the traffic can be transmitted smoothly without interruption.

Figure 1-2 Schematic diagram for VLAN interface backup



Using Auto Detect can help implement VLAN interfaces backup. When data can be transmitted through two VLAN interfaces on the switch to the same destination, configure one of the VLAN interface as the active interface and the other as the standby interface. The standby interface is enabled automatically when the active fails, so as to ensure the data transmission. In this case, the Auto Detect function is implemented as follows:

- In normal situations (that is, when the detected group is **reachable**), the standby VLAN interface is down and packets are transmitted through the active VLAN interface.
- When the link between the active VLAN interface and the destination faults (that is, the detected group is **unreachable**), the system enables the backup VLAN interface.
- When the link between the active VLAN interface and the destination recovers (that is, the detected group becomes **reachable** again), the system shuts down the standby VLAN interface again.



Note

You need to create the detected group and perform configurations concerning VLAN interfaces before the following operations.

Follow these steps to configure the auto detect function for VLAN interface backup:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	—
Enable the auto detect function to implement VLAN interface backup	standby detect-group <i>group-number</i>	Required This operation is only needed on the secondary VLAN interface.

Auto Detect Configuration Examples

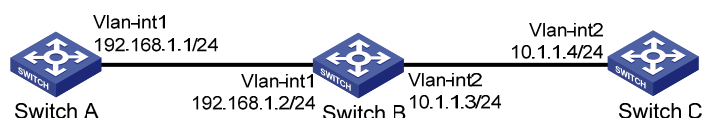
Configuration Example for Auto Detect Implementation with Static Routing

Network requirements

- Create detected group 8 on Switch A; detect the reachability of the IP address 10.1.1.4, with 192.168.1.2 as the next hop, and the detecting number set to 1.
- On switch A, configure a static route to Switch C.
- Enable the static route when the detected group 8 is **reachable**.
- To ensure normal operating of the auto detect function, configure a static route to Switch A on Switch C.

Network diagram

Figure 1-3 Network diagram for implementing the auto detect function in static route



Configuration procedure

Configure the IP addresses of all the interfaces as shown in [Figure 1-3](#). The configuration procedure is omitted.

- Configure Switch A.

Enter system view.

```
<SwitchA> system-view
```

Create detected group 8.

```
[SwitchA] 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.

```
[SwitchA-detect-group-8] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
```

```
[SwitchA-detect-group-8] quit
```

Enable the static route when the detected group is reachable. The static route is invalid when the detected group is unreachable.

```
[SwitchA] ip route-static 10.1.1.4 24 192.168.1.2 detect-group 8
```

- Configure Switch C.

Enter system view.

```
<SwitchC> system-view
```

Configure a static route to Switch A.

```
[SwitchC] ip route-static 192.168.1.1 24 10.1.1.3
```

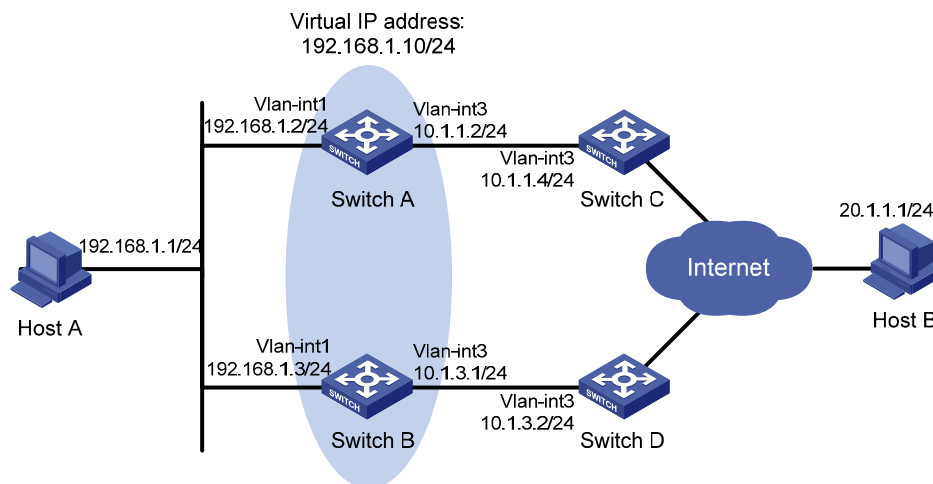
Configuration Example for Auto Detect Implementation with VRRP

Network requirements

- Switch A and switch B form VRRP group 1, whose virtual IP address is 192.168.1.10.
- Packets sourced from Host A and destined for Host B is forwarded by Switch A under normal situations.
- When the connection between Switch A and Switch C fails, Switch B becomes the master in VRRP group 1 automatically and the link from Switch B to Host B, the backup link, is enabled.

Network diagram

Figure 1-4 Network diagram for implementing the auto detect function in VRRP



Configuration procedure

Configure the IP addresses of all the interfaces as shown in [Figure 1-4](#). The configuration procedure is omitted.

- Configure Switch A.

Create detected group 9.

```
<SwitchA> system-view
[SwitchA] detect-group 9
```

Specify to detect the reachability of the IP address 10.1.1.4/24, setting the detect number to 1.

```
[SwitchA-detect-group-9] detect-list 1 ip address 10.1.1.4
[SwitchA-detect-group-9] quit
```

Enable VRRP on VLAN-interface 1 and assign a virtual IP address to the VRRP group.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] vrrp vrid 1 virtual-ip 192.168.1.10
```

Set the VRRP group priority of switch A to 110, and specify to decrease the priority by 20 when the result of detected group 9 is **unreachable**.

```
[SwitchA-Vlan-interface1] vrrp vrid 1 priority 110
[SwitchA-Vlan-interface1] vrrp vrid 1 track detect-group 9 reduced 20
```

- Configure Switch B.

Enable VRRP on VLAN-interface 1 and assign a virtual IP address to the VRRP group.

```

<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] vrrp vrid 1 virtual-ip 192.168.1.10
# Set the VRRP group priority of Switch B to 100.
[SwitchB-Vlan-interface1] vrrp vrid 1 priority 100

```

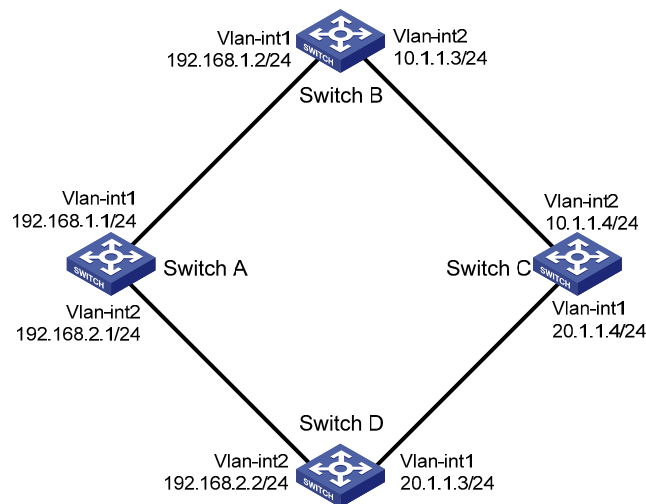
Configuration Example for Auto Detect Implementation with VLAN Interface Backup

Network requirements

- Make sure the routes between Switch A, Switch B, and Switch C, and between Switch A, Switch D, and Switch C are reachable.
- Create detected group 10 on Switch A to detect the connectivity between Switch B and Switch C.
- Configure VLAN-interface 1 to be the active interface, which is enabled when the detected group 10 is **reachable**.
- Configure VLAN-interface 2 to be the standby interface, which is enabled when the detected group 10 is **unreachable**.

Network diagram

Figure 1-5 Network diagram for VLAN interface backup



Configuration procedure

Configure the IP addresses of all the interfaces as shown in [Figure 1-5](#). The configuration procedure is omitted.

Enter system view.

```
<SwitchA> system-view
```

Create auto detected group 10.

```
[SwitchA] detect-group 10
```

Add the IP address of 10.1.1.4 to detected 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.

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

```
[SwitchA-detect-group-10] quit
```

Specify to enable VLAN-interface 2 when the result of detected group 10 is **unreachable**.

```
[SwitchA] interface vlan-interface 2
```

```
[SwitchA-Vlan-interface2] standby detect-group 10
```

Table of Contents

1 MSTP Configuration	1-1
Overview	1-1
Spanning Tree Protocol Overview	1-1
Rapid Spanning Tree Protocol Overview	1-10
Multiple Spanning Tree Protocol Overview	1-10
MSTP Implementation on Switches	1-14
Protocols and Standards	1-15
MSTP Configuration Task List	1-15
Configuring Root Bridge	1-17
Configuring an MST Region	1-17
Specifying the Current Switch as a Root Bridge/Secondary Root Bridge	1-18
Configuring the Bridge Priority of the Current Switch	1-20
Configuring How a Port Recognizes and Sends MSTP Packets	1-20
Configuring the MSTP Operation Mode	1-21
Configuring the Maximum Hop Count of an MST Region	1-22
Configuring the Network Diameter of the Switched Network	1-23
Configuring the MSTP Time-related Parameters	1-23
Configuring the Timeout Time Factor	1-25
Configuring the Maximum Transmitting Rate on the Current Port	1-25
Configuring the Current Port as an Edge Port	1-26
Setting the Link Type of a Port to P2P	1-27
Enabling MSTP	1-28
Configuring Leaf Nodes	1-29
Configuring the MST Region	1-29
Configuring How a Port Recognizes and Sends MSTP Packets	1-30
Configuring the Timeout Time Factor	1-30
Configuring the Maximum Transmitting Rate on the Current Port	1-30
Configuring a Port as an Edge Port	1-30
Configuring the Path Cost for a Port	1-30
Configuring Port Priority	1-32
Setting the Link Type of a Port to P2P	1-33
Enabling MSTP	1-33
Performing mCheck Operation	1-33
Configuration Prerequisites	1-34
Configuration Procedure	1-34
Configuration Example	1-34
Configuring Guard Functions	1-34
Configuring BPDU Guard	1-34
Configuring Root Guard	1-35
Configuring Loop Guard	1-37
Configuring TC-BPDU Attack Guard	1-38
Configuring BPDU Dropping	1-39
Configuring Digest Snooping	1-39

Introduction	1-39
Configuring Digest Snooping	1-40
Configuring Rapid Transition	1-41
Introduction	1-41
Configuring Rapid Transition	1-43
Configuring VLAN-VPN Tunnel	1-44
Introduction	1-44
Configuring VLAN-VPN tunnel	1-44
MSTP Maintenance Configuration	1-45
Introduction	1-45
Enabling Log/Trap Output for Ports of MSTP Instance	1-45
Configuration Example	1-45
Enabling Trap Messages Conforming to 802.1d Standard	1-46
Displaying and Maintaining MSTP	1-46
MSTP Configuration Example	1-47
VLAN-VPN Tunnel Configuration Example	1-49

1 MSTP Configuration

Go to these sections for information you are interested in:

- [Overview](#)
- [MSTP Configuration Task List](#)
- [Configuring Root Bridge](#)
- [Configuring Leaf Nodes](#)
- [Performing mCheck Operation](#)
- [Configuring Guard Functions](#)
- [Configuring Digest Snooping](#)
- [Configuring Rapid Transition](#)
- [Configuring VLAN-VPN Tunnel](#)
- [MSTP Maintenance Configuration](#)
- [Enabling Trap Messages Conforming to 802.1d Standard](#)
- [Displaying and Maintaining MSTP](#)
- [MSTP Configuration Example](#)
- [VLAN-VPN Tunnel Configuration Example](#)

Overview

As a Layer 2 management protocol, the Spanning Tree Protocol (STP) eliminates Layer 2 loops by selectively blocking redundant links in a network, and in the mean time, allows for link redundancy.

Like many other protocols, STP evolves as the network grows. The later versions of STP are Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP). This chapter describes the characteristics of STP, RSTP, and MSTP and the relationship among them.

Spanning Tree Protocol Overview

Why STP

Spanning tree protocol (STP) is a protocol conforming to IEEE 802.1d. It aims to eliminate loops on data link layer in a local area network (LAN). Devices running this protocol detect loops in the network by exchanging packets with one another and eliminate the loops detected by blocking specific ports until the network is pruned into one with a tree topology. As a network with a tree topology is loop-free, STP prevents packets in it from being duplicated and forwarded endlessly and prevents device and network performance degradation caused by data loops.

In the narrow sense, STP refers to IEEE 802.1d STP; in the broad sense, STP refers to the IEEE 802.1d STP and various enhanced spanning tree protocols derived from that protocol.

Protocol Packets of STP

STP uses bridge protocol data units (BPDUs), also known as configuration messages, as its protocol packets.

STP identifies the network topology by transmitting BPDUs between STP compliant network devices, typically switches and routers. BPDUs contain sufficient information for the network devices to complete the spanning tree calculation.

In STP, BPDUs come in two types:

- Configuration BPDUs, used to calculate spanning trees and maintain the spanning tree topology.
- Topology change notification (TCN) BPDUs, used to notify concerned devices of network topology changes, if any.

Basic concepts in STP

1) Root bridge

A tree network must have a root; hence the concept of **root bridge** has been introduced in STP.

There is one and only one root bridge in an entire STP-based network at a given time. But the root bridge can change because of with changes of the network topology. Therefore, the root bridge is not fixed.

Upon initialization of a network, each device generates and sends out BPDUs periodically with itself as the root bridge; after network convergence, only the root bridge generates and sends out configuration BPDUs at a certain interval, and the other devices just forward the BPDUs.

2) Root port

On a non-root bridge device, the root port is the port with the lowest path cost to the root bridge. The root port is used for communicating with the root bridge. A non-root-bridge device has one and only one root port. The root bridge has no root port.

3) Designated bridge and designated port

Refer to the following table for the description of designated bridge and designated port.

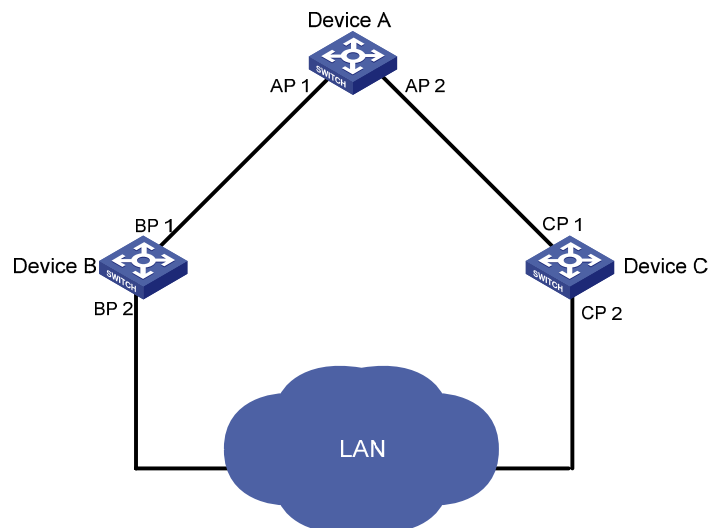
Table 1-1 Designated bridge and designated port

Classification	Designated bridge	Designated port
For a device	A designated bridge is a device that is directly connected to a switch and is responsible for forwarding BPDUs to this switch.	The port through which the designated bridge forwards BPDUs to this device
For a LAN	A designated bridge is a device responsible for forwarding BPDUs to this LAN segment.	The port through which the designated bridge forwards BPDUs to this LAN segment

[Figure 1-1](#) shows designated bridges and designated ports. In the figure, AP1 and AP2, BP1 and BP2, and CP1 and CP2 are ports on Device A, Device B, and Device C respectively.

- If Device A forwards BPDUs to Device B through AP1, the designated bridge for Device B is Device A, and the designated port is the port AP1 on Device A.
- Two devices are connected to the LAN: Device B and Device C. If Device B forwards BPDUs to the LAN, the designated bridge for the LAN is Device B, and the designated port is the port BP2 on Device B.

Figure 1-1 A schematic diagram of designated bridges and designated ports



Note

All the ports on the root bridge are designated ports.

4) Bridge ID

A bridge ID consists of eight bytes, where the first two bytes represent the bridge priority of the device, and the latter six bytes represent the MAC address of the device.



Note

The default bridge priority of an H3C device is 32768. You can use a command to configure the bridge priority of a device. For details, see [Configuring the Bridge Priority of the Current Switch](#).

5) Path cost

STP uses path costs to indicate the quality of links. A small path cost indicates a higher link quality. The path cost of a port is related to the rate of the link connecting the port. The higher the link rate, the smaller the path cost.

By comparing the path costs of different links, STP selects the most robust links and blocks the other links to prune the network into a tree.



Note

H3C devices support using multiple standards to calculate the path costs of ports, as well as using commands to configure the path costs of ports. For details, see [Configuring the Path Cost for a Port](#).

6) Port ID

A port ID used on an H3C device consists of two bytes, that is, 16 bits, where the first six bits represent the port priority, and the latter ten bits represent the port number.



Note

The default priority of all Ethernet ports on H3C devices is 128. You can use commands to configure port priorities. For details, see [Configuring Port Priority](#).

How STP works

STP identifies the network topology by transmitting configuration BPDUs between network devices. Configuration BPDUs contain sufficient information for network devices to complete the spanning tree calculation. Important fields in a configuration BPDU include:

- Root bridge ID, consisting of root bridge priority and MAC address.
- Root path cost, the cost of the shortest path to the root bridge.
- Designated bridge ID, designated bridge priority plus MAC address.
- Designated port ID, designated port priority plus port number.
- Message age, lifetime for the configuration BPDUs to be propagated within the network.
- Max age, lifetime for the configuration BPDUs to be kept in a switch.
- Hello time, configuration BPDU interval.
- Forward delay, forward delay of the port.



Note

The implementation of the STP algorithm involves only the following four parts of a configuration BPDU:

- Root bridge ID
 - Root path cost
 - Designated bridge ID
 - Designated port ID
-

1) Detailed calculation process of the STP algorithm

- Initial state

Upon initialization of a device, each device generates a BPDU with itself as the root bridge, in which the root path cost is 0, designated bridge ID is the device ID, and the designated port is the local port.

- Selection of the optimum configuration BPDU

Each device sends out its configuration BPDU and receives configuration BPDUs from other devices.

The process of selecting the optimum configuration BPDU is as follows:

Table 1-2 Selection of the optimum configuration BPDU

Step	Description
1	Upon receiving a configuration BPDU on a port, the device performs the following processing: • If the received configuration BPDU has a lower priority than that of the configuration BPDU generated by the port, the device will discard the received configuration BPDU without doing any processing on the configuration BPDU of this port. • If the received configuration BPDU has a higher priority than that of the configuration BPDU generated by the port, the device will replace the content of the configuration BPDU generated by the port with the content of the received configuration BPDU.
2	The device compares the configuration BPDUs of all the ports and chooses the optimum configuration BPDU.

**Note**

Principles for configuration BPDU comparison:

- The configuration BPDU that has the lowest root bridge ID has the highest priority.
- If all configuration BPDUs have the same root bridge ID, they will be compared for their root path costs. If the root path cost in a configuration BPDU plus the path cost corresponding to this port is S, the configuration BPDU with the smallest S value has the highest priority.
- If all configuration BPDUs have the same root path cost, the following fields are compared sequentially: designated bridge IDs, designated port IDs, and then the IDs of the ports on which the configuration BPDUs are received. The smaller these values, the higher priority for the configuration BPDU.

- Selection of the root bridge

At network initialization, each STP-compliant device on the network assumes itself to be the root bridge, with the root bridge ID being its own bridge ID. By exchanging configuration BPDUs, the devices compare one another's configuration BPDU priority. The device with the highest configuration BPDU priority is elected as the root bridge.

- Selection of the root port and designated ports

The process of selecting the root port and designated ports is as follows:

Table 1-3 Selection of the root port and designated ports

Step	Description
1	A non-root-bridge device takes the port on which the optimum configuration BPDU was received as the root port.

Step	Description
2	Based on the configuration BPDU and the path cost of the root port, the device calculates a designated port configuration BPDU for each of the rest ports. • The root bridge ID is replaced with that of the configuration BPDU of the root port. • The root path cost is replaced with that of the configuration BPDU of the root port plus the path cost corresponding to the root port. • The designated bridge ID is replaced with the ID of this device. • The designated port ID is replaced with the ID of this port.
3	The device compares the calculated configuration BPDU with the configuration BPDU on the port whose role is to be determined, and acts as follows based on the comparison result: • If the calculated configuration BPDU is superior, this port will serve as the designated port, and the configuration BPDU on the port will be replaced with the calculated configuration BPDU, which will be sent out periodically. • If the configuration BPDU on the port is superior, the device stops updating the configuration BPDUs of the port and blocks the port, so that the port only receives configuration BPDUs, but does not forward data or send configuration BPDUs.



Note

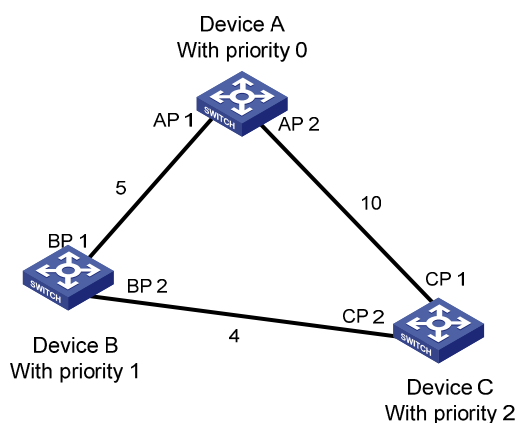
When the network topology is stable, only the root port and designated ports forward traffic, while other ports are all in the blocked state – they only receive STP packets but do not forward user traffic.

Once the root bridge, the root port on each non-root bridge, and designated ports have been successfully elected, the entire tree-shaped topology has been constructed. At this stage, “STP convergence” is complete.

2) Example of how the STP algorithm works

The following is an example of how the STP algorithm works. The specific network diagram is shown in [Figure 1-2](#). The priority of Device A is 0, the priority of Device B is 1, the priority of Device C is 2, and the path costs of these links are 5, 10 and 4 respectively.

Figure 1-2 Network diagram for STP algorithm



- Initial state of each device

The following table shows the initial state of each device.

Table 1-4 Initial state of each device

Device	Port name	BPDU of port
Device A	AP1	{0, 0, 0, AP1}
	AP2	{0, 0, 0, AP2}
Device B	BP1	{1, 0, 1, BP1}
	BP2	{1, 0, 1, BP2}
Device C	CP1	{2, 0, 2, CP1}
	CP2	{2, 0, 2, CP2}

- Comparison process and result on each device

The following table shows the comparison process and result on each device.

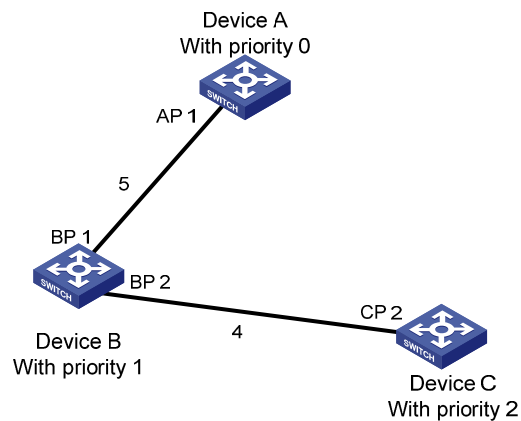
Table 1-5 Comparison process and result on each device

Device	Comparison process	BPDU of port after comparison
Device A	• Port AP1 receives the configuration BPDU of Device B {1, 0, 1, BP1}. Device A finds that the configuration BPDU of the local port {0, 0, 0, AP1} is superior to the configuration received message, and discards the received configuration BPDU. • Port AP2 receives the configuration BPDU of Device C {2, 0, 2, CP1}. Device A finds that the BPDU of the local port {0, 0, 0, AP2} is superior to the received configuration BPDU, and discards the received configuration BPDU. • Device A finds that both the root bridge and designated bridge in the configuration BPDUs of all its ports are Device A itself, so it assumes itself to be the root bridge. In this case, it does not make any change to the configuration BPDU of each port, and starts sending out configuration BPDUs periodically.	AP1: {0, 0, 0, AP1} AP2: {0, 0, 0, AP2}
Device B	• Port BP1 receives the configuration BPDU of Device A {0, 0, 0, AP1}. Device B finds that the received configuration BPDU is superior to the configuration BPDU of the local port {1, 0, 1, BP1}, and updates the configuration BPDU of BP1. • Port BP2 receives the configuration BPDU of Device C {2, 0, 2, CP2}. Device B finds that the configuration BPDU of the local port {1, 0, 1, BP2} is superior to the received configuration BPDU, and discards the received configuration BPDU.	BP1: {0, 0, 0, AP1} BP2: {1, 0, 1, BP2}
	• Device B compares the configuration BPDUs of all its ports, and determines that the configuration BPDU of BP1 is the optimum configuration BPDU. Then, it uses BP1 as the root port, the configuration BPDUs of which will not be changed. • Based on the configuration BPDU of BP1 and the path cost of the root port (5), Device B calculates a designated port configuration BPDU for BP2 {0, 5, 1, BP2}. • Device B compares the calculated configuration BPDU {0, 5, 1, BP2} with the configuration BPDU of BP2. If the calculated BPDU is superior, BP2 will act as the designated port, and the configuration BPDU on this port will be replaced with the calculated configuration BPDU, which will be sent out periodically.	Root port BP1: {0, 0, 0, AP1} Designated port BP2: {0, 5, 1, BP2}

Device	Comparison process	BPDU of port after comparison
Device C	- Port CP1 receives the configuration BPDU of Device A {0, 0, 0, AP2}. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP1}, and updates the configuration BPDU of CP1. - Port CP2 receives the configuration BPDU of port BP2 of Device B {1, 0, 1, BP2} before the message was updated. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP2}, and updates the configuration BPDU of CP2.	CP1: {0, 0, 0, AP2} CP2: {1, 0, 1, BP2}
	By comparison: - The configuration BPDUs of CP1 is elected as the optimum configuration BPDU, so CP1 is identified as the root port, the configuration BPDUs of which will not be changed. - Device C compares the calculated designated port configuration BPDU {0, 10, 2, CP2} with the configuration BPDU of CP2, and CP2 becomes the designated port, and the configuration BPDU of this port will be replaced with the calculated configuration BPDU.	Root port CP1: {0, 0, 0, AP2} Designated port CP2: {0, 10, 2, CP2}
	- Next, port CP2 receives the updated configuration BPDU of Device B {0, 5, 1, BP2}. Because the received configuration BPDU is superior to its old one, Device C launches a BPDU update process. - At the same time, port CP1 receives configuration BPDUs periodically from Device A. Device C does not launch an update process after comparison.	CP1: {0, 0, 0, AP2} CP2: {0, 5, 1, BP2}
	By comparison: - Because the root path cost of CP2 (9) (root path cost of the BPDU (5) + path cost corresponding to CP2 (4)) is smaller than the root path cost of CP1 (10) (root path cost of the BPDU (0) + path cost corresponding to CP2 (10)), the BPDU of CP2 is elected as the optimum BPDU, and CP2 is elected as the root port, the messages of which will not be changed. - After comparison between the configuration BPDU of CP1 and the calculated designated port configuration BPDU, port CP1 is blocked, with the configuration BPDU of the port remaining unchanged, and the port will not receive data from Device A until a spanning tree calculation process is triggered by a new condition, for example, the link from Device B to Device C becomes down.	Blocked port CP2: {0, 0, 0, AP2} Root port CP2: {0, 5, 1, BP2}

After the comparison processes described in the table above, a spanning tree with Device A as the root bridge is stabilized, as shown in [Figure 1-3](#).

Figure 1-3 The final calculated spanning tree



Note

To facilitate description, the spanning tree calculation process in this example is simplified, while the actual process is more complicated.

3) The BPDU forwarding mechanism in STP

- Upon network initiation, every switch regards itself as the root bridge, generates configuration BPDUs with itself as the root, and sends the configuration BPDUs at a regular interval of hello time.
- If it is the root port that received the configuration BPDU and the received configuration BPDU is superior to the configuration BPDU of the port, the device will increase message age carried in the configuration BPDU by a certain rule and start a timer to time the configuration BPDU while it sends out this configuration BPDU through the designated port.
- If the configuration BPDU received on the designated port has a lower priority than the configuration BPDU of the local port, the port will immediately send out its better configuration BPDU in response.
- If a path becomes faulty, the root port on this path will no longer receive new configuration BPDUs and the old configuration BPDUs will be discarded due to timeout. In this case, the device generates configuration BPDUs with itself as the root bridge and sends configuration BPDUs and TCN BPDUs. This triggers a new spanning tree calculation so that a new path is established to restore the network connectivity.

However, the newly calculated configuration BPDU will not be propagated throughout the network immediately, so the old root ports and designated ports that have not detected the topology change continue forwarding data through the old path. If the new root port and designated port begin to forward data as soon as they are elected, a temporary loop may occur.

4) STP timers

The following three time parameters are important for STP calculation:

- Forward delay, the period a device waits before state transition.

A link failure triggers a new round of spanning tree calculation and results in changes of the spanning tree. However, as new configuration BPDUs cannot be propagated throughout the network immediately, if the new root port and designated port begin to forward data as soon as they are elected, loops may temporarily occur.

For this reason, the protocol uses a state transition mechanism. Namely, a newly elected root port and the designated ports must go through a period, which is twice the forward delay time, before they transit to the forwarding state. The period allows the new configuration BPDUs to be propagated throughout the entire network.

- Hello time, the interval for sending hello packets. Hello packets are used to check link state.

A switch sends hello packets to its neighboring devices at a regular interval (the hello time) to check whether the links are faulty.

- Max time, lifetime of the configuration BPDUs stored in a switch. A configuration BPDU that has “expired” is discarded by the switch.

Rapid Spanning Tree Protocol Overview

Rapid spanning tree protocol (RSTP) is an optimized version of STP. RSTP allows a newly elected root port or designated port to enter the forwarding state much quicker under certain conditions than in STP. As a result, it takes a shorter time for the network to reach the final topology stability.



Note

- In RSTP, the state of a root port can transit fast under the following conditions: the old root port on the device has stopped forwarding data and the upstream designated port has started forwarding data.
 - In RSTP, the state of a designated port can transit fast under the following conditions: the designated port is an edge port or a port connected with a point-to-point link. If the designated port is an edge port, it can enter the forwarding state directly; if the designated port is connected with a point-to-point link, it can enter the forwarding state immediately after the device undergoes handshake with the downstream device and gets a response.
-

Multiple Spanning Tree Protocol Overview

Why MSTP

1) Disadvantages of STP and RSTP

STP does not support rapid state transition of ports. A newly elected root port or designated port must wait twice the forward delay time before transiting to the forwarding state, even if it is a port on a point-to-point link or it is an edge port (an edge port refers to a port that directly connects to a user terminal rather than to another device or a shared LAN segment.)

RSTP supports rapid convergence. Like STP, it is of the following disadvantages: all bridges in a LAN are on the same spanning tree; redundant links cannot be blocked by VLAN; the packets of all VLANs are forwarded along the same spanning tree.

2) Features of MSTP

The multiple spanning tree protocol (MSTP) overcomes the shortcomings of STP and RSTP. In addition to support for rapid network convergence, it also allows data flows of different VLANs to be forwarded along their own paths, thus providing a better load sharing mechanism for redundant links.

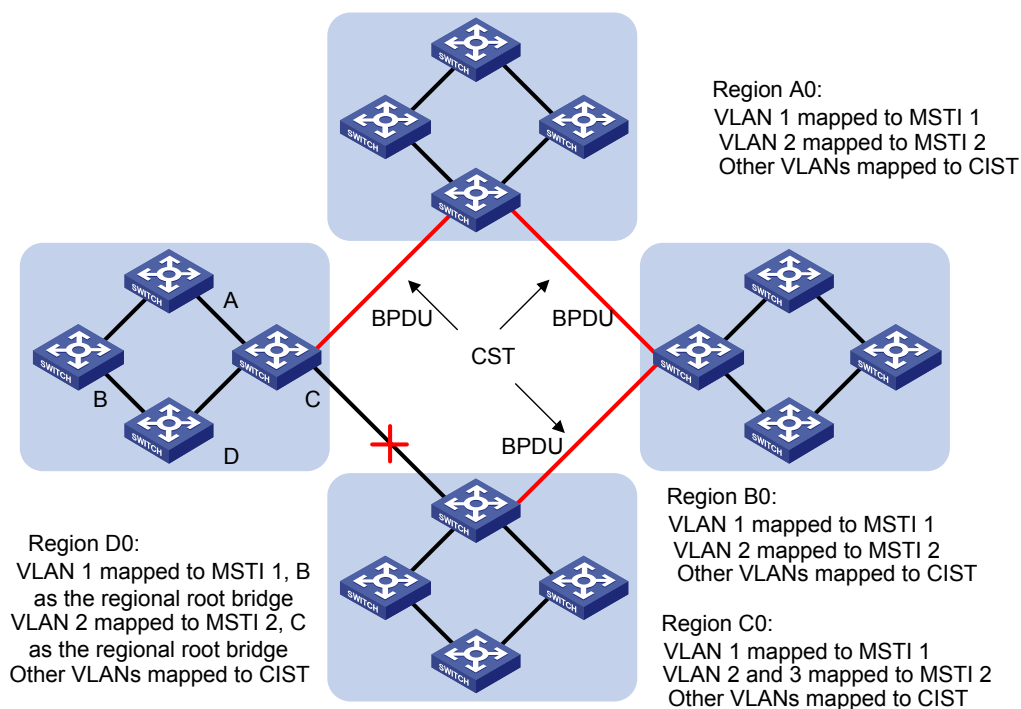
MSTP features the following:

- MSTP supports mapping VLANs to Multiple Spanning Tree (MST) instances (MSTIs) by means of a VLAN-to-instance mapping table. MSTP introduces **instances** (which integrates multiple VLANs into a set) and can bind multiple VLANs to an instance, thus saving communication overhead and improving resource utilization.
- MSTP divides a switched network into multiple regions, each containing multiple spanning trees that are independent of one another.
- MSTP prunes a ring network into a network with tree topology, preventing packets from being duplicated and forwarded in a network endlessly. Furthermore, it offers multiple redundant paths for forwarding data, and thus achieves load balancing for forwarding VLAN data.
- MSTP is compatible with STP and RSTP.

Basic MSTP Terminology

[Figure 1-4](#) illustrates basic MSTP terms (assuming that MSTP is enabled on each switch in this figure).

Figure 1-4 Basic MSTP terminologies



2) 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-instance 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.

As shown in [Figure 1-4](#), all the switches in region A0 are of the same MST region-related configuration, including:

- Region name
- VLAN-to-instance mapping (that is, VLAN 1 is mapped to MSTI 1, VLAN 2 is mapped to MSTI 2, and the other VLANs are mapped to CIST.)
- MSTP revision level (not shown in [Figure 1-4](#))

3) 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 1-4](#) contains multiple spanning trees known as MSTIs. Each of these spanning trees corresponds to a VLAN.

4) VLAN-to-instance mapping table

A VLAN-to-instance mapping table is maintained for each MST region. The table is a collection of mappings between VLANs and MSTIs. For example, in [Figure 1-4](#), the VLAN-to-instance mapping table of region A0 contains these mappings: VLAN 1 to MSTI 1; VLAN 2 to MSTI 2, and other VLANs to CIST. In an MST region, load balancing is implemented according to the VLAN-to-instance mapping table.

5) 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 1-4](#), each MST region has an IST, which is a branch of the CIST.

6) CST

A common spanning tree (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”. For example, the red lines in [Figure 1-4](#) represent the CST.

7) CIST

A common and internal spanning tree (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 1-4](#), the ISTs in the MST regions and the CST connecting the MST regions form the CIST.

8) 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 1-4](#), the region root of MSTI 1 is switch B, and the region root of MSTI 2 is switch C.

9) Common root bridge

The common root bridge is the root of the CIST. The common root bridge of the network shown in [Figure 1-4](#) is a switch in region A0.

10) Port role

MSTP calculation involves the following port roles: root port, designated port, master port, region boundary 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. In the CST, the master port is the root port of the region, which is considered as a node. The master port is a special boundary port. It is a root port in the IST/CIST while a master port in the other MSTIs.

- A region boundary port is located on the boundary 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 secondary port of a root port or master port and is used for rapid transition. With the root port or master port being blocked, the alternate port becomes the new root port or master port.
- A backup port is the secondary port of a designated port and is used for rapid transition. With the designated port being blocked, the backup port becomes the new designated port fast and begins to forward data seamlessly. When two ports of an MSTP-enabled switch are interconnected, the switch blocks one of the two ports to eliminate the loop that occurs. The blocked port is the backup port.

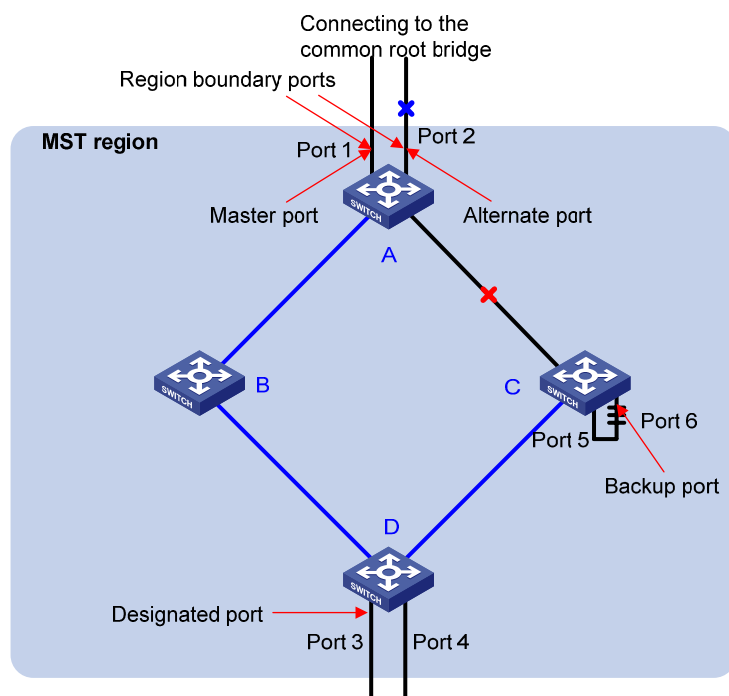
In [Figure 1-5](#), switch A, switch B, switch C, and switch D form an MST region. Port 1 and port 2 on switch A connect upstream to the common root. Port 5 and port 6 on switch C form a loop. Port 3 and port 4 on switch D connect downstream to other MST regions. This figure shows the roles these ports play.



Note

- A port can play different roles in different MSTIs.
- The role a region boundary port plays in an MSTI is consistent with the role it plays in the CIST. The master port, which is a root port in the CIST while a master port in the other MSTIs, is an exception.
- For example, in [Figure 1-5](#), port 1 on switch A is a region boundary port. It is a root port in the CIST while a master port in all the other MSTIs in the region.

Figure 1-5 Port roles



11) Port state

In MSTP, a port 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 but do not forward user packets.
- Discarding state. Ports in this state can only receive BPDU packets.

Port roles and port states are not mutually dependent. [Table 1-6](#) lists possible combinations of port states and port roles.

Table 1-6 Combinations of port states and port roles

Port role Port state	Root/master port	Designated port	Region Boundary port	Alternate port	Backup port
Forwarding	√	√	√	—	—
Learning	√	√	√	—	—
Discarding	√	√	√	√	√

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.

1) 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.

2) Calculate an MSTI

Within an MST region, MSTP generates different MSTIs for different VLANs based on the VLAN-to-instance mappings. MSTP performs a separate calculation process, which is similar to spanning tree calculation in STP, for each spanning tree. For details, refer to [How STP works](#).

In MSTP, a VLAN packet is forwarded along the following paths:

- Within an MST region, the packet is forwarded along the corresponding MSTI.
- Between two MST regions, the packet is forwarded along the CST.

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 their respective spanning tree calculation.

The S3600 series switches support MSTP. After MSTP is enabled on an S3600 series switch, the switch operates in MSTP mode by default. If the network contains switches that run the STP/RSTP protocol, you can use commands to configure the S3600 series switch to operate in STP-compatible mode or RSTP-compatible mode (see [Configuring the MSTP Operation Mode](#) for more information):

- In STP-compatible mode, all ports of the S3600 series switch send out STP BPDUs
- In RSTP mode, all ports of the S3600 series switch send out RSTP BPDUs.

In addition to the basic MSTP functions, H3C series switches also provide the following functions for users to manage their switches.

- Root bridge hold
- Root bridge backup
- Root guard
- BPDU guard
- Loop guard
- TC-BPDU attack guard
- BPDU packet drop

Protocols and Standards

MSTP is documented in:

- IEEE 802.1D: spanning tree protocol
- IEEE 802.1w: rapid spanning tree protocol
- IEEE 802.1s: multiple spanning tree protocol

MSTP Configuration Task List

Before configuring MSTP, you need to know the position of each device in each MSTI: root bridge or leaf node. In each MSTI, one, and only one device acts as the root bridge, while all others as leaf nodes.

Complete these tasks to configure MSTP:

Task		Remarks
Configuring Root Bridge	Enabling MSTP	Required To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after other related configurations are performed.
	Configuring an MST Region	Required
	Specifying the Current Switch as a Root Bridge/Secondary Root Bridge	Required
	Configuring 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.
	Configuring How a Port Recognizes and Sends MSTP Packets	Optional
	Configuring the MSTP Operation Mode	Optional
	Configuring the Maximum Hop Count of an MST Region	Optional
	Configuring the Network Diameter of the Switched Network	Optional The default value is recommended.
	Configuring the MSTP Time-related Parameters	Optional The default values are recommended.

Task		Remarks
	Configuring the Timeout Time Factor	Optional
	Configuring the Maximum Transmitting Rate on the Current Port	Optional The default value is recommended.
	Configuring the Current Port as an Edge Port	Optional
	Setting the Link Type of a Port to P2P	Optional
Configuring Leaf Nodes	Enabling MSTP	Required To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after performing other configurations.
	Configuring an MST Region	Required
	Configuring How a Port Recognizes and Sends MSTP Packets	Optional
	Configuring the Timeout Time Factor	Optional
	Configuring the Maximum Transmitting Rate on the Current Port	Optional The default value is recommended.
	Configuring the Current Port as an Edge Port	Optional
	Configuring the Path Cost for a Port	Optional
	Configuring Port Priority	Optional
	Setting the Link Type of a Port to P2P	Optional
Performing mCheck Operation		Optional
Configuring Guard Functions		Optional
Configuring Digest Snooping		Optional
Configuring Rapid Transition		Optional
Configuring VLAN-VPN Tunnel		Optional
MSTP Maintenance Configuration		Optional
Enabling Trap Messages Conforming to 802.1d Standard		Optional



Note

In a network containing switches with both GVRP and MSTP enabled, GVRP messages travel along the CIST. If you want to advertise a VLAN through GVRP, be sure to map the VLAN to the CIST (MSTI 0) when configuring the VLAN-to-instance mapping table.

Configuring Root Bridge

Configuring an MST Region

Configuration procedure

Follow these steps to configure an MST region:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter MST region view	stp region-configuration	—
Configure the name of the MST region	region-name <i>name</i>	Required The default MST region name of a switch is its MAC address.
Configure the VLAN-to-instance mapping table for the MST region	instance <i>instance-id</i> vlan <i>vlan-list</i>	Required Both commands can be used to configure VLAN-to-instance mapping tables. By default, all VLANs in an MST region are mapped to MSTI 0.
	vlan-mapping modulo <i>modulo</i>	
Configure the MSTP revision level for the MST region	revision-level <i>level</i>	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	Available in any view



Note

Neighbor Topology Discovery Protocol (NTDP) packets sent by devices in a cluster can only be transmitted within the MSTI where the management VLAN of the cluster resides. For more information about clusters and the NTDP protocol, see *Cluster Operation*.

Configuring MST region-related parameters (especially the VLAN-to-instance 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

- MSTP-enabled switches are in the same region only when they have the same format selector (a 802.1s-defined protocol selector, which is 0 by default and cannot be configured), MST region name, VLAN-to-instance mapping table, and revision level.
- The H3C series support only the MST region name, VLAN-to-instance mapping table, and revision level. Switches with the settings of these parameters being the same are assigned to the same MST region.

Configuration example

Configure an MST region named **info**, the MSTP revision level being level 1, VLAN 2 through VLAN 10 being mapped to MSTI 1, and VLAN 20 through VLAN 30 being mapped to MSTI 2.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] region-name info
[Sysname-mst-region] instance 1 vlan 2 to 10
[Sysname-mst-region] instance 2 vlan 20 to 30
[Sysname-mst-region] revision-level 1
[Sysname-mst-region] active region-configuration
```

Verify the above configuration.

```
[Sysname-mst-region] check region-configuration
```

Admin configuration

```
Format selector      :0
Region name          :info
Revision level       :1
```

Instance	Vlans Mapped
0	1, 11 to 19, 31 to 4094
1	2 to 10
2	20 to 30

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.

Specify the current switch as the root bridge of a spanning tree

Follow these steps to specify the current switch as the root bridge of a spanning tree:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify the current switch as the root bridge of a spanning tree	stp [instance <i>instance-id</i>] root primary [bridge-diameter <i>bridgenumber</i> [hello-time <i>centi-seconds</i>]]	Required

Specify the current switch as the secondary root bridge of a spanning tree

Follow these steps to specify the current switch as the secondary root bridge of a spanning tree:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify the current switch as the secondary root bridge of a specified spanning tree	stp [instance <i>instance-id</i>] root secondary [bridge-diameter <i>bridgenumber</i> [hello-time <i>centi-seconds</i>]]	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 MSTI 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 MSTIs. That is, it can be the root bridges in an MSTI and be a secondary root bridge in another MSTI at the same time. But in the same MSTI, 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 an MSTI, 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 [Configuring the Network Diameter of the Switched Network](#) and [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 MSTIs. But you cannot configure two or more root bridges for one MSTI. So, do not configure root bridges for the same MSTI on two or more switches using the **stp root primary** command.
- You can configure multiple secondary root bridges for one MSTI. That is, you can configure secondary root bridges for the same MSTI 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.

Configuration example

Configure the current switch as the root bridge of MSTI 1 and a secondary root bridge of MSTI 2.

```
<Sysname> system-view
[Sysname] stp instance 1 root primary
[Sysname] stp instance 2 root secondary
```

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 MSTIs.

Configuration procedure

Follow these steps to configure the bridge priority of the current switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the bridge priority for the current switch	stp [instance <i>instance-id</i>] priority <i>priority</i>	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.

Configuration example

Set the bridge priority of the current switch to 4,096 in MSTI 1.

```
<Sysname> system-view
```

```
[Sysname] stp instance 1 priority 4096
```

Configuring How a Port Recognizes and Sends MSTP Packets

A port can send/recognize MSTP packets of two formats:

- dot1s**: 802.1s-compliant standard format
- legacy**: Compatible format

By default, the packet format recognition mode of a port is **auto**, namely the port automatically distinguishes the two MSTP packet formats, and determines the format of packets it will send based on the recognized format. You can configure the MSTP packet format to be used by a port. After the configuration, when working in MSTP mode, the port sends and receives only MSTP packets of the format you have configured to communicate with devices that send packets of the same format.

Configuration procedure

Follow these steps to configure how a port recognizes and sends MSTP packets (in system view):

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
Configure how a port recognizes and sends MSTP packets	stp interface <i>interface-list</i> compliance { auto dot1s legacy }	Required By default, a port recognizes and sends MSTP packets in the automatic mode. That is, it determines the format of packets to be sent according to the format of the packets received.

Follow these steps to configure how a port recognizes and sends MSTP packets (in Ethernet port view):

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure how a port recognizes and sends MSTP packets	stp compliance { auto dot1s legacy }	Required By default, a port recognizes and sends MSTP packets in the automatic mode. That is, it determines the format of packets to be sent according to the format of the packets received.

Configuration example

```
# Configure Ethernet 1/0/1 to recognize and send packets in dot1s format.
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp compliance dot1s

# Restore the default mode for Ethernet 1/0/1 to recognize/send MSTP packets.
[Sysname-Ethernet1/0/1] undo stp compliance
```

Configuring the MSTP Operation Mode

To make an MSTP-enabled switch compatible with STP/RSTP, MSTP provides the following three operation modes:

- STP-compatible mode, where the ports of a switch send STP BPDUs to neighboring devices. If STP-enabled switches exist in a switched network, you can use the **stp mode stp** command to configure an MSTP-enabled switch to operate in STP-compatible mode.
- RSTP-compatible mode, where the ports of a switch send RSTP BPDUs to neighboring devices. If RSTP-enabled switches exist in a switched network, you can use the **stp mode rstp** command to configure an MSTP-enabled switch to operate in RSTP-compatible mode.
- MSTP mode, where the ports of a switch send MSTP BPDUs or STP BPDUs (if the switch is connected to STP-enabled switches) to neighboring devices. In this case, the switch is MSTP-capable.

Configuration procedure

Follow these steps to configure the MSTP operation mode:

To do...	Use the command...	Remarks
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.

Configuration example

Specify the MSTP operation mode as STP-compatible.

```
<Sysname> system-view
[Sysname] stp mode stp
```

Configuring the Maximum Hop Count of an MST Region

The maximum hop count configured on the region root is also the maximum hops of the MST region. The value of the maximum hop count 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 hop count from participating in spanning tree calculation, and thus limits the size of an MST region.

With such a mechanism, the maximum hop count 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.

Configuration procedure

Follow these steps to configure the maximum hop count for an MST region:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the maximum hop count of the MST region	stp max-hops <i>hops</i>	Required By default, the maximum hop count of an MST region is 20.

The bigger the maximum hop count, 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.

Configuration example

Configure the maximum hop count of the MST region to be 30.

```
<Sysname> system-view
[Sysname] stp max-hops 30
```

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).

Configuration procedure

Follow these steps to configure the network diameter of the switched network:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the network diameter of the switched network	stp bridge-diameter <i>bridgenumber</i>	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 CIST; it is invalid for MSTIs.

Configuration example

Configure the network diameter of the switched network to 6.

```
<Sysname> system-view
```

```
[Sysname] stp bridge-diameter 6
```

Configuring the MSTP Time-related Parameters

Three MSTP time-related parameters exist: forward delay, hello time, and max age. You can configure the three parameters to control the process of spanning tree calculation.

Configuration procedure

Follow these steps to configure MSTP time-related parameters:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the forward delay parameter	stp timer forward-delay <i>centiseconds</i>	Required The forward delay parameter defaults to 1,500 centiseconds (namely, 15 seconds).
Configure the hello time parameter	stp timer hello <i>centiseconds</i>	Required The hello time parameter defaults to 200 centiseconds (namely, 2 seconds).

To do...	Use the command...	Remarks
Configure the max age parameter	stp timer max-age <i>centiseconds</i>	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.

$2 \times (\text{forward delay} - 1 \text{ second}) \geq \text{max age}$

$\text{Max age} \geq 2 \times (\text{hello time} + 1 \text{ second})$

You are recommended to 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.

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).

```
<Sysname> system-view
[Sysname] stp timer forward-delay 1600
[Sysname] stp timer hello 300
[Sysname] stp timer max-age 2100
```

Configuring the Timeout Time Factor

When the network topology is stable, a non-root-bridge switch regularly forwards BPDUs received from the root bridge to its neighboring devices at the interval specified by the hello time parameter to check for link failures. Normally, a switch regards its upstream switch faulty if the former does not receive any BPDU 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.

Configuration procedure

Follow these steps to configure the timeout time factor:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the timeout time factor for the switch	stp timer-factor <i>number</i>	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.

Configuration example

Configure the timeout time factor to be 6.

```
<Sysname> system-view  
[Sysname] stp timer-factor 6
```

Configuring the Maximum Transmitting Rate on the Current Port

The maximum transmitting rate 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.

Configure the maximum transmitting rate for specified ports in system view

Follow these steps to configure the maximum transmitting rate for specified ports in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the maximum transmitting rate for specified ports	stp interface <i>interface-list</i> transmit-limit <i>packetnum</i>	Required The maximum transmitting rate of all Ethernet ports on a switch defaults to 10.

Configure the maximum transmitting rate in Ethernet port view

Follow these steps to configure the maximum transmitting rate in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the maximum transmitting rate	stp transmit-limit <i>packetnum</i>	Required The maximum transmitting rate of all Ethernet ports on a switch defaults to 10.

As the maximum transmitting rate 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.

Configuration example

Set the maximum transmitting rate of Ethernet 1/0/1 to 15.

- 1) Configure the maximum transmitting rate in system view

```
<Sysname> system-view
[Sysname] stp interface Ethernet 1/0/1 transmit-limit 15
```
- 2) Configure the maximum transmitting rate in Ethernet port view

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp transmit-limit 15
```

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.

Configure a port as an edge port in system view

Follow these steps to configure a port as an edge port in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the specified ports as edge ports	stp interface <i>interface-list</i> edged-port enable	Required By default, all the Ethernet ports of a switch are non-edge ports.

Configure a port as an edge port in Ethernet port view

Follow these steps to configure a port as an edge port in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
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 guard 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 guard function at the same time. This not only enables these ports to turn to the forwarding state rapidly but also secures your network.

Configuration example

Configure Ethernet 1/0/1 as an edge port.

1) Configure Ethernet 1/0/1 as an edge port in system view

```
<Sysname> system-view
```

```
[Sysname] stp interface Ethernet 1/0/1 edged-port enable
```

2) Configure Ethernet 1/0/1 as an edge port in Ethernet port view

```
<Sysname> system-view
```

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] stp edged-port enable
```

Setting the Link Type of a Port to P2P

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.

Setting the Link Type of a Port to P2P in system view

Follow these steps to specify whether the link connected to a port is point-to-point link in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify whether the link connected to a port is point-to-point link	stp interface <i>interface-list</i> point-to-point { force-true force-false auto }	Required The auto keyword is adopted by default.

Setting the Link Type of a Port to P2P in Ethernet port view

Follow these steps to specify whether the link connected to a port is point-to-point link in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
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.



Note

- If you configure the link connected to a port in an aggregation group as a point-to-point link, the configuration will be synchronized to the rest ports in the same aggregation group.
- 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 the MSTIs the port belongs to. 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, loops may occur temporarily.

Configuration example

Configure the link connected to Ethernet 1/0/1 as a point-to-point link.

1) Perform this configuration in system view

```
<Sysname> system-view
```

```
[Sysname] stp interface Ethernet 1/0/1 point-to-point force-true
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
```

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] stp point-to-point force-true
```

Enabling MSTP

Configuration procedure

Follow these steps to enable MSTP in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable MSTP	stp enable	Required MSTP is disabled by default.

To do...	Use the command...	Remarks
Disable MSTP on specified ports	stp interface <i>interface-list</i> 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.

Follow these steps to enable MSTP in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable MSTP	stp enable	Required MSTP is disabled by default.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Disable MSTP 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.

Configuration example

Enable MSTP on the switch and disable MSTP on Ethernet 1/0/1.

1) Perform this configuration in system view

```
<Sysname> system-view
[Sysname] stp enable
[Sysname] stp interface Ethernet 1/0/1 disable
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] stp enable
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp disable
```

Configuring Leaf Nodes

Configuring the MST Region

Refer to [Configuring an MST Region](#).

Configuring How a Port Recognizes and Sends MSTP Packets

Refer to [Configuring How a Port Recognizes and Sends MSTP Packets](#).

Configuring the Timeout Time Factor

Refer to [Configuring the Timeout Time Factor](#).

Configuring the Maximum Transmitting Rate on the Current Port

Refer to [Configuring the Maximum Transmitting Rate on the Current Port](#).

Configuring a Port as an Edge Port

Refer to [Configuring the Current Port as an Edge Port](#).

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 MSTIs. 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.

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.

Follow these steps to specify the standard for calculating path costs:

To do...	Use the command...	Remarks
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 1-7 Transmission rates vs. path costs

Rate	Operation mode (half-/full-duplex)	802.1D-1998	IEEE 802.1t	Latency standard
0	—	65,535	200,000,000	200,000
10 Mbps	Half-duplex/Full-duplex	100	2,000,000	2,000
	Aggregated link 2 ports	95	1,000,000	1,800
	Aggregated link 3 ports	95	666,666	1,600
	Aggregated link 4 ports	95	500,000	1,400

Rate	Operation mode (half-/full-duplex)	802.1D-1998	IEEE 802.1t	Latency standard
100 Mbps	Half-duplex/Full-duplex	19	200,000	200
	Aggregated link 2 ports	15	100,000	180
	Aggregated link 3 ports	15	66,666	160
	Aggregated link 4 ports	15	50,000	140
1,000 Mbps	Full-duplex	4	20,000	20
	Aggregated link 2 ports	3	10,000	18
	Aggregated link 3 ports	3	6,666	16
	Aggregated link 4 ports	3	5,000	14
10 Gbps	Full-duplex	2	2,000	2
	Aggregated link 2 ports	1	1,000	1
	Aggregated link 3 ports	1	666	1
	Aggregated link 4 ports	1	500	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:

$$\text{Path cost} = 200,000,000 / \text{link transmission rate}$$

Where, “link transmission rate” is the sum of the rates of all the unblocked ports on the aggregated link measured in 100 Kbps.

Configure the path cost for specific ports

Follow these steps to configure the path cost for specified ports in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the path cost for specified ports	stp interface <i>interface-list</i> [instance <i>instance-id</i>] cost <i>cost</i>	Required An MSTP-enabled switch can calculate path costs for all its ports automatically.

Follow these steps to configure the path cost for a port in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the path cost for the port	stp [instance <i>instance-id</i>] cost <i>cost</i>	Required An 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.

Configuration example (A)

Configure the path cost of Ethernet 1/0/1 in MSTI 1 to be 2,000.

1) Perform this configuration in system view

```
<Sysname> system-view
```

```
[Sysname] stp interface Ethernet 1/0/1 instance 1 cost 2000
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
```

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] stp instance 1 cost 2000
```

Configuration example (B)

Configure the path cost of Ethernet 1/0/1 in MSTI 1 to be calculated by the MSTP-enabled switch according to the IEEE 802.1D-1998 standard.

1) Perform this configuration in system view

```
<Sysname> system-view
```

```
[Sysname] undo stp interface Ethernet 1/0/1 instance 1 cost
```

```
[Sysname] stp pathcost-standard dot1d-1998
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
```

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] undo stp instance 1 cost
```

```
[Sysname-Ethernet1/0/1] quit
```

```
[Sysname] stp pathcost-standard dot1d-1998
```

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 MSTIs. 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.

Configure port priority in system view

Follow these steps to configure port priority in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure port priority for specified ports	stp interface <i>interface-list</i> instance <i>instance-id</i> port priority <i>priority</i>	Required The default port priority is 128.

Configure port priority in Ethernet port view

Follow these steps to configure port priority in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure port priority for the port	stp [instance <i>instance-id</i>] port priority <i>priority</i>	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.

Configuration example

Configure the port priority of Ethernet 1/0/1 in MSTI 1 to be 16.

1) Perform this configuration in system view

```
<Sysname> system-view
```

```
[Sysname] stp interface Ethernet 1/0/1 instance 1 port priority 16
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
```

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] stp instance 1 port priority 16
```

Setting the Link Type of a Port to P2P

Refer to [Setting the Link Type of a Port to P2P](#).

Enabling MSTP

Refer to [Enabling MSTP](#).

Performing mCheck Operation

Ports on an MSTP-enabled switch can operate in three modes: STP-compatible, RSTP-compatible, and MSTP.

If a port on a device running MSTP (or RSTP) connects to a device running STP, this port will automatically migrate to the STP-compatible mode. However, it will not be able to migrate automatically back to the MSTP (or RSTP) mode, but will remain working in the STP-compatible mode under the following circumstances:

- The device running STP is shut down or removed.
- The device running STP migrates to the MSTP (or RSTP) mode.

By then, you can perform an mCheck operation to force the port to migrate to the MSTP (or RSTP) mode.

Configuration Prerequisites

MSTP runs normally on the switch.

Configuration Procedure

You can perform the mCheck operation in the following two ways.

Perform the mCheck operation in system view

Follow these steps to perform the mCheck operation in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Perform the mCheck operation	stp [interface <i>interface-list</i>] mcheck	Required

Perform the mCheck operation in Ethernet port view

Follow these steps to perform the mCheck operation in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Perform the mCheck operation	stp mcheck	Required

Configuration Example

Perform the mCheck operation on Ethernet 1/0/1.

1) Perform this configuration in system view

```
<Sysname> system-view
```

```
[Sysname] stp interface Ethernet 1/0/1 mcheck
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
```

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] stp mcheck
```

Configuring Guard Functions

The following guard functions are available on an MSTP-enabled switch: BPDU guard, root guard, loop guard, TC-BPDU attack guard, and BPDU drop.

Configuring BPDU Guard

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 guard 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. Ports shut down in this way can only be restored by the administrator.



Note

You are recommended to enable BPDU guard for devices with edge ports configured.

Configuration Prerequisites

MSTP runs normally on the switch.

Configuration procedure

Follow these steps to configure BPDU guard:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the BPDU guard function	stp bpdu-protection	Required The BPDU guard function is disabled by default.

Configuration example

Enable the BPDU guard function.

```
<Sysname> system-view
```

```
[Sysname] stp bpdu-protection
```



Caution

As Gigabit ports of an S3600 Ethernet switch cannot be shut down, the BPDU guard function is not applicable to these ports even if you enable the BPDU guard function and specify these ports to be MSTP edge ports.

Configuring Root Guard

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 guard function. Ports with this function enabled can only be kept as designated ports in all MSTIs. 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.



Note

- You are recommended to enable root guard on the designated ports of a root bridge.
- Loop guard, root guard, and edge port settings are mutually exclusive. With one of these functions enabled on a port, any of the other two functions cannot take effect even if you have configured it on the port.

Configuration Prerequisites

MSTP runs normally on the switch.

Configuration procedure

Follow these steps to configure the root guard function in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the root guard function on specified ports	stp interface <i>interface-list</i> root-protection	Required The root guard function is disabled by default.

Follow these steps to enable the root guard function in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	Interface <i>interface-type</i> <i>interface-number</i>	—
Enable the root guard function on the current port	stp root-protection	Required The root guard function is disabled by default.

Configuration example

Enable the root guard function on Ethernet 1/0/1.

1) Perform this configuration in system view

```
<Sysname> system-view
```

```
[Sysname] stp interface Ethernet 1/0/1 root-protection
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
```

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] stp root-protection
```

Configuring Loop Guard

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 turn to the forwarding state. This may cause loops in the network.

The loop guard 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.



Note

- You are recommended to enable loop guard on the root port and alternate port of a non-root bridge.
- Loop guard, root guard, and edge port settings are mutually exclusive. With one of these functions enabled on a port, any of the other two functions cannot take effect even if you have configured it on the port.

Configuration Prerequisites

MSTP runs normally on the switch.

Configuration procedure

Follow these steps to configure loop guard:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the loop guard function on the current port	stp loop-protection	Required The loop guard function is disabled by default.

Configuration example

```
# Enable the loop guard function on Ethernet 1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] stp loop-protection
```

Configuring TC-BPDU Attack Guard

Normally, a switch removes its MAC address table and ARP entries upon receiving Topology Change BPDUs (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 the MAC address table and ARP entries, which may affect spanning tree calculation, occupy large amount of bandwidth and increase switch CPU utilization.

With the TC-BPDU attack guard function enabled, a switch performs a removing operation upon receiving a TC-BPDU and triggers a timer (set to 10 seconds by default) at the same time. Before the timer expires, the switch only performs the removing operation for limited times (up to six times by default) regardless of the number of the TC-BPDUs it receives. Such a mechanism prevents a switch from being busy in removing the MAC address table and ARP entries.

You can use the **stp tc-protection threshold** command to set the maximum times for a switch to remove the MAC address table and ARP entries in a specific period. When the number of the TC-BPDUs received within a period is less than the maximum times, the switch performs a removing operation upon receiving a TC-BPDU. After the number of the TC-BPDUs received reaches the maximum times, the switch stops performing the removing operation. For example, if you set the maximum times for a switch to remove the MAC address table and ARP entries to 100 and the switch receives 200 TC-BPDUs in the period, the switch removes the MAC address table and ARP entries for only 100 times within the period.

Configuration prerequisites

MSTP runs normally on the switch.

Configuration procedure

Follow these steps to configure the TC-BPDU attack guard function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the TC-BPDU attack guard function	stp tc-protection enable	Required The TC-BPDU attack guard function is disabled by default.
Set the maximum times that a switch can remove the MAC address table and ARP entries within each 10 seconds	stp tc-protection threshold <i>number</i>	Optional

Configuration example

Enable the TC-BPDU attack guard function

```
<Sysname> system-view
```

```
[Sysname] stp tc-protection enable
```

Set the maximum times for the switch to remove the MAC address table and ARP entries within 10 seconds to 5.

```
<Sysname> system-view
```

```
[Sysname] stp tc-protection threshold 5
```

Configuring BPDU Dropping

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 repeatedly, 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 BPDU dropping on Ethernet ports. Once the function is enabled on a port, the port will not receive or forward any BPDU packets. In this way, the switch is protected against the BPDU packet attacks so that the STP calculation is assured to be right.

Configuration Prerequisites

MSTP runs normally on the switch.

Configuration procedure

Follow these steps to configure BPDU dropping:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-name</i>	—
Enable BPDU dropping	bpdu-drop any	Required BPDU dropping is disabled by default.

Configuration example

Enable BPDU dropping on Ethernet 1/0/1.

```
<Sysname>system-view
```

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] bpdu-drop any
```

Configuring Digest Snooping

Introduction

According to IEEE 802.1s, two interconnected switches can communicate 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 communicate 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 communicate with another manufacturer's switches in the same MST region.



Caution

The digest snooping function is not applicable to edge ports.

Configuring Digest Snooping

Configure the digest snooping feature on a switch to enable it to communicate with other switches adopting proprietary protocols to calculate configuration digests in the same MST region through MSTIs.

Configuration prerequisites

The switch to be configured is connected to another manufacturer's switch adopting a proprietary spanning tree protocol. MSTP and the network operate normally.

Configuration procedure

Follow these steps to configure digest snooping:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the digest snooping feature	stp config-digest-snooping	Required The digest snooping feature is disabled on a 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 current configuration	display current-configuration	Available 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-instance mapping).
 - The digest snooping feature must be enabled on all the switch ports that connect 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-instance mapping table cannot be modified.
 - The digest snooping feature is not applicable to boundary ports in an MST region.
 - The digest snooping feature is not applicable to edge ports in an MST region.
-

Configuring Rapid Transition

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 1-6](#) and [Figure 1-7](#) illustrate the rapid transition mechanisms on designated ports in RSTP and MSTP.

Figure 1-6 The RSTP rapid transition mechanism

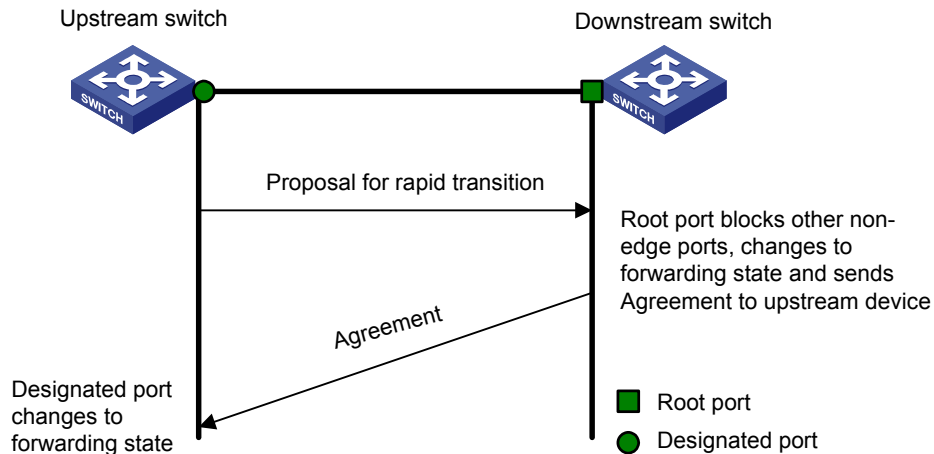
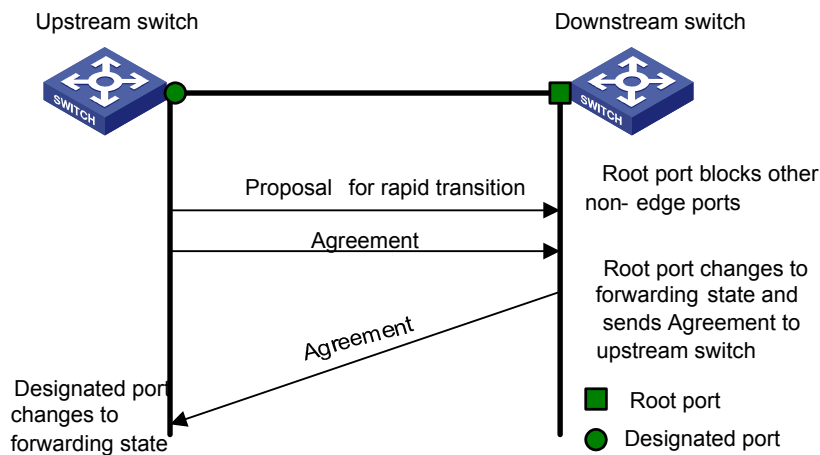


Figure 1-7 The MSTP rapid transition mechanism



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.

Configuring Rapid Transition

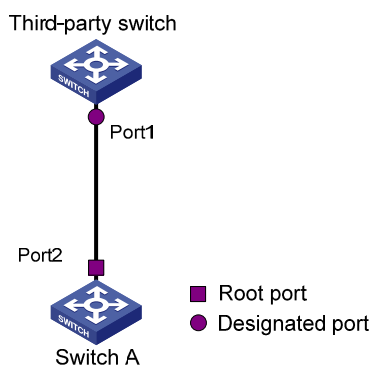
Configuration prerequisites

As shown in [Figure 1-8](#), 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 H3C switch is running MSTP. Port 2 is the root port.

Figure 1-8 Network diagram for rapid transition configuration



Configuration procedure

- 1) Configure the rapid transition feature in system view

Follow these steps to configure the rapid transition feature in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the rapid transition feature	stp interface <i>interface-type</i> <i>interface-number</i> 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

Follow these steps to configure the rapid transition feature in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
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.
-

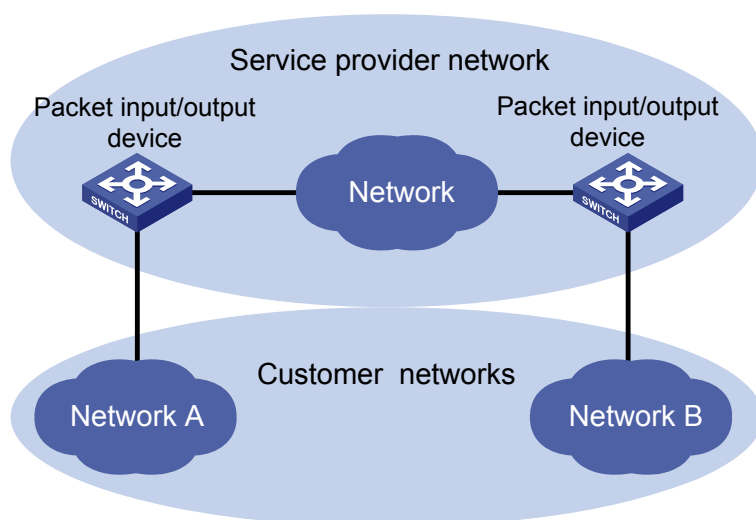
Configuring VLAN-VPN Tunnel

Introduction

The VLAN-VPN Tunnel function enables STP packets to be transparently transmitted between geographically dispersed customer networks through specified VLAN VPNs in service provider networks, through which spanning trees can be generated across these customer networks and are independent of those of the service provider network.

As shown in [Figure 1-9](#), the upper part is the service provider network, and the lower part comprises the customer networks. The service provider network comprises packet input/output devices, and the customer network has networks A and B. On the service provider network, configure the arriving STP packets at the input device to have MAC addresses in a special format, and reconvert them back to their original formats at the output device. This is how transparent transmission is implemented over the service provider network.

Figure 1-9 VLAN-VPN tunnel network hierarchy



Configuring VLAN-VPN tunnel

Follow these steps to configure VLAN-VPN tunnel:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable MSTP globally	stp enable	—

To do...	Use the command...	Remarks
Enable the VLAN-VPN tunnel function globally	vlan-vpn tunnel	Required The VLAN-VPN tunnel function is disabled by default.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	Make sure that you enter the Ethernet port view of the port for which you want to enable the VLAN-VPN tunnel function.
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 STP-enabled devices only.
- To enable the VLAN-VPN tunnel function, make sure the links between service provider 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.

MSTP Maintenance Configuration

Introduction

In a large-scale network with MSTP enabled, there may be many MSTP instances, and so the status of a port may change frequently. In this case, maintenance personnel may expect that log/trap information is output to the log host when particular ports fail, so that they can check the status changes of those ports through alarm information.

Enabling Log/Trap Output for Ports of MSTP Instance

Follow these steps to enable log/trap output for ports of MSTP instance:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable log/trap output for the ports of a specified instance	stp [instance <i>instance-id</i>] portlog	Required By default, log/trap output is disabled for the ports of all instances.
Enable log/trap output for the ports of all instances	stp portlog all	Required By default, log/trap output is disabled for the ports of all instances.

Configuration Example

```
# Enable log/trap output for the ports of instance 1.
```

```

<Sysname> system-view
[Sysname] stp instance 1 portlog

# Enable log/trap output for the ports of all instances.

<Sysname> system-view
[Sysname] stp portlog all

```

Enabling Trap Messages Conforming to 802.1d Standard

A switch sends trap messages conforming to 802.1d standard to the network management device in the following two cases:

- The switch becomes the root bridge of an instance.
- Network topology changes are detected.

Configuration procedure

Follow these steps to enable trap messages conforming to 802.1d standard:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable trap messages conforming to 802.1d standard in an instance	stp [instance <i>instance-id</i>] dot1d-trap [newroot topologychange] enable	Required

Configuration example

Enable a switch to send trap messages conforming to 802.1d standard to the network management device when the switch becomes the root bridge of instance 1.

```

<Sysname> system-view
[Sysname] stp instance 1 dot1d-trap newroot enable

```

Displaying and Maintaining MSTP

To do...	Use the command...	Remarks
Display the state and statistics information about spanning trees of the current device	display stp [instance <i>instance-id</i>] [interface <i>interface-list</i> slot <i>slot-number</i>] [brief]	Available in any view
Display region configuration	display stp region-configuration	
Display information about the ports that are shut down by STP protection	display stp portdown	
Display information about the ports that are blocked by STP protection	display stp abnormalport	
Display information about the root port of the instance where the switch reside	display stp root	
Clear statistics about MSTP	reset stp [interface <i>interface-list</i>]	Available in user view

MSTP Configuration Example

Network requirements

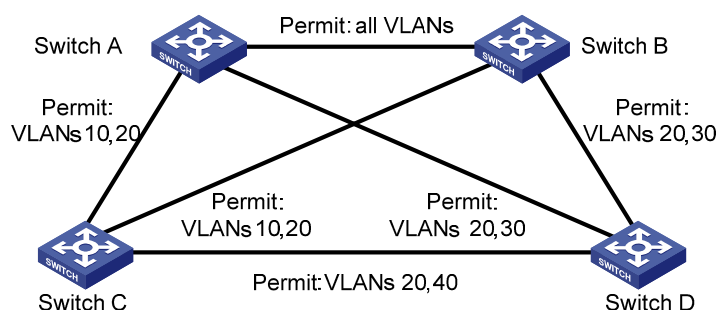
Implement MSTP in the network shown in [Figure 1-10](#) to enable packets of different VLANs to be forwarded along different MSTIs. The detailed configurations are as follows:

- 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 MSTI 1, MSTI 3, MSTI 4, and MSTI 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 MSTI 1 and MSTI 3 respectively. Switch C is configured as the root bridge of MSTI 4.

Network diagram

Figure 1-10 Network diagram for MSTP configuration



Note

The word “permit” shown in [Figure 1-10](#) means the corresponding link permits packets of specific VLANs.

Configuration procedure

1) Configure Switch A

Enter MST region view.

```
<Sysname> system-view
```

```
[Sysname] stp region-configuration
```

Configure the region name, VLAN-to-instance mapping table, and revision level for the MST region.

```
[Sysname-mst-region] region-name example
```

```
[Sysname-mst-region] instance 1 vlan 10
```

```
[Sysname-mst-region] instance 3 vlan 30
```

```
[Sysname-mst-region] instance 4 vlan 40
```

```
[Sysname-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[Sysname-mst-region] active region-configuration
```


Specify Switch A as the root bridge of MSTI 1.

```
[Sysname] stp instance 1 root primary
```

2) Configure Switch B

Enter MST region view.

```
<Sysname> system-view
```

```
[Sysname] stp region-configuration
```

Configure the region name, VLAN-to-instance mapping table, and revision level for the MST region.

```
[Sysname-mst-region] region-name example
```

```
[Sysname-mst-region] instance 1 vlan 10
```

```
[Sysname-mst-region] instance 3 vlan 30
```

```
[Sysname-mst-region] instance 4 vlan 40
```

```
[Sysname-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[Sysname-mst-region] active region-configuration
```

Specify Switch B as the root bridge of MSTI 3.

```
[Sysname] stp instance 3 root primary
```

3) Configure Switch C.

Enter MST region view.

```
<Sysname> system-view
```

```
[Sysname] stp region-configuration
```

Configure the MST region.

```
[Sysname-mst-region] region-name example
```

```
[Sysname-mst-region] instance 1 vlan 10
```

```
[Sysname-mst-region] instance 3 vlan 30
```

```
[Sysname-mst-region] instance 4 vlan 40
```

```
[Sysname-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[Sysname-mst-region] active region-configuration
```

Specify Switch C as the root bridge of MSTI 4.

```
[Sysname] stp instance 4 root primary
```

4) Configure Switch D

Enter MST region view.

```
<Sysname> system-view
```

```
[Sysname] stp region-configuration
```

Configure the MST region.

```
[Sysname-mst-region] region-name example
```

```
[Sysname-mst-region] instance 1 vlan 10
```

```
[Sysname-mst-region] instance 3 vlan 30
```

```
[Sysname-mst-region] instance 4 vlan 40
```

```
[Sysname-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[Sysname-mst-region] active region-configuration
```

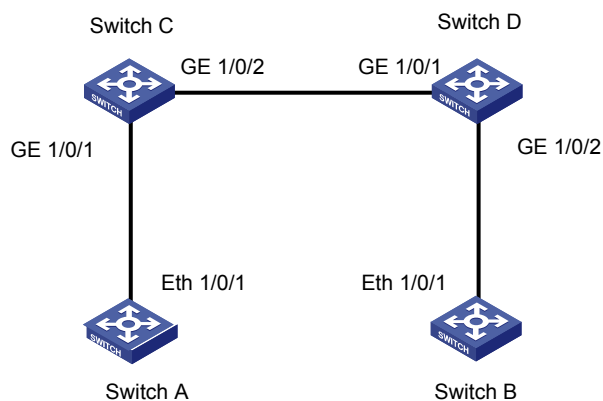
VLAN-VPN Tunnel Configuration Example

Network requirements

- Switch C and Switch D are the access devices for the service provider network.
- S3600 switches operate as the access devices of the customer networks, 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 customer networks and the service provider network.

Network diagram

Figure 1-11 Network diagram for VLAN-VPN tunnel configuration



Configuration procedure

1) Configure Switch A

Enable MSTP.

```
<Sysname> system-view
```

```
[Sysname] stp enable
```

Add Ethernet 1/0/1 to VLAN 10.

```
[Sysname] vlan 10
```

```
[Sysname-Vlan10] port Ethernet 1/0/1
```

2) Configure Switch B

Enable MSTP.

```
<Sysname> system-view
```

```
[Sysname] stp enable
```

Add Ethernet 1/0/1 to VLAN 10.

```
[Sysname] vlan 10
```

```
[Sysname-Vlan10] port Ethernet 1/0/1
```

3) Configure Switch C

Enable MSTP.

```
<Sysname> system-view
```

```
[Sysname] stp enable
```

Enable the VLAN-VPN tunnel function.

```

[Sysname] vlan-vpn tunnel

# Add GigabitEthernet 1/0/1 to VLAN 10.

[Sysname] vlan 10
[Sysname-Vlan10] port GigabitEthernet 1/0/1
[Sysname-Vlan10] quit

# Enable the VLAN VPN function on GigabitEthernet 1/0/1.

[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 10
[Sysname-GigabitEthernet1/0/1] vlan-vpn enable
[Sysname-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 as a trunk port.

[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-type trunk

# Add the trunk port to all VLANs.

[Sysname-GigabitEthernet1/0/2] port trunk permit vlan all
4) Configure Switch D

# Enable MSTP.

<Sysname> system-view
[Sysname] stp enable

# Enable the VLAN-VPN tunnel function.

[Sysname] vlan-vpn tunnel

# Add GigabitEthernet 1/0/2 to VLAN 10.

[Sysname] vlan 10
[Sysname-Vlan10] port GigabitEthernet 1/0/2

# Enable the VLAN VPN function on GigabitEthernet 1/0/2.

[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port access vlan 10
[Sysname-GigabitEthernet1/0/2] vlan-vpn enable
[Sysname-GigabitEthernet1/0/2] quit

# Configure GigabitEthernet 1/0/1 as a trunk port.

[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk

# Add the trunk port to all VLANs.

[Sysname-GigabitEthernet1/0/1] port trunk permit vlan all

```

Table of Contents

1 IP Routing Protocol Overview	1-1
Introduction to IP Route and Routing Table	1-1
IP Route	1-1
Routing Table	1-1
Routing Protocol Overview	1-3
Static Routing and Dynamic Routing	1-3
Classification of Dynamic Routing Protocols	1-3
Routing Protocols and Routing Priority	1-4
Load Sharing and Route Backup	1-4
Routing Information Sharing	1-5
Displaying and Maintaining a Routing Table	1-5
2 Static Route Configuration	2-1
Introduction to Static Route	2-1
Static Route	2-1
Default Route	2-2
Static Route Configuration	2-2
Configuration Prerequisites	2-2
Configuring a Static Route	2-2
Displaying and Maintaining Static Routes	2-3
Static Route Configuration Example	2-3
Troubleshooting a Static Route	2-4
3 RIP Configuration	3-1
RIP Overview	3-1
Basic Concepts	3-1
RIP Startup and Operation	3-2
RIP Configuration Task List	3-2
Basic RIP Configuration	3-3
Configuration Prerequisites	3-3
Configuring Basic RIP Functions	3-3
RIP Route Control	3-4
Configuration Prerequisites	3-5
Configuring RIP Route Control	3-5
RIP Network Adjustment and Optimization	3-8
Configuration Prerequisites	3-8
Configuration Tasks	3-8
Displaying and Maintaining RIP Configuration	3-10
RIP Configuration Example	3-10
Troubleshooting RIP Configuration	3-12
Failed to Receive RIP Updates	3-12
4 OSPF Configuration	4-1
OSPF Overview	4-1
Introduction to OSPF	4-1

OSPF Route Calculation	4-1
Basic OSPF Concepts	4-2
OSPF Area Partition and Route Summarization	4-4
OSPF Network Type	4-8
DR/BDR	4-9
OSPF Features	4-11
OSPF Configuration Task List	4-11
Basic OSPF Configuration	4-12
Configuration Prerequisites	4-12
Basic OSPF Configuration	4-12
OSPF Area Attribute Configuration	4-13
Configuration Prerequisites	4-14
Configuring OSPF Area Attributes	4-14
OSPF Network Type Configuration	4-14
Configuration Prerequisites	4-15
Configuring the Network Type of an OSPF Interface	4-15
Configuring an NBMA/P2MP Neighbor	4-15
Configuring the DR Priority on an OSPF Interface	4-16
OSPF Route Control	4-16
Configuration Prerequisites	4-17
Configuring OSPF Route Summarization	4-17
Configuring OSPF to Filter Received Routes	4-17
Configuring the OSPF Cost on an Interface	4-18
Configuring OSPF Route Priority	4-18
Configuring the Maximum Number of OSPF ECMP Routes	4-19
Configuring OSPF to Redistribute External Routes	4-19
OSPF Network Adjustment and Optimization	4-20
Configuration Prerequisites	4-20
Configuring OSPF Timers	4-20
Configuring the LSA transmission delay	4-21
Configuring the SPF Calculation Interval	4-22
Disabling OSPF Packet Transmission on an Interface	4-22
Configuring OSPF Authentication	4-22
Configuring the MTU Field in DD Packets	4-23
Enabling OSPF Logging of Neighbor State Changes	4-23
Configuring OSPF Network Management	4-24
Displaying and Maintaining OSPF Configuration	4-24
OSPF Configuration Examples	4-25
Configuring DR/BDR Election	4-25
Configuring OSPF Virtual Link	4-27
Troubleshooting OSPF Configuration	4-29
Unable to Establish a Neighbor Relationship between Routers	4-29
Unable to Learn a Complete Network Topology	4-29
5 IP Route Policy Configuration	5-1
IP Route Policy Overview	5-1
Introduction to IP Route Policy	5-1
Filters	5-1
IP Route Policy Configuration Task List	5-2

Route Policy Configuration	5-2
Configuration Prerequisites	5-3
Defining a Route Policy	5-3
Defining if-match Clauses and apply Clauses	5-3
IP-Prefix Configuration	5-5
Configuration Prerequisites	5-5
Configuring an ip-prefix list	5-5
Displaying IP Route Policy	5-5
IP Route Policy Configuration Example	5-6
Configuring to Filter Received Routing Information	5-6
Controlling RIP Packet Cost to Implement Dynamic Route Backup	5-8
Troubleshooting IP Route Policy	5-11
6 Route Capacity Configuration	6-1
Route Capacity Configuration Overview	6-1
Introduction	6-1
Route Capacity Limitation	6-1
Route Capacity Limitation Configuration	6-2
Configuring the Lower Limit and the Safety Value of the Switch Memory	6-2
Enabling/Disabling Automatic Protocol Recovery	6-2
Displaying and Maintaining Route Capacity Limitation Configuration	6-3

1 IP Routing Protocol Overview

Go to these sections for information you are interested in:

- [Introduction to IP Route and Routing Table](#)
- [Routing Protocol Overview](#)
- [Displaying and Maintaining a Routing Table](#)



Note

- The term **router** in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.
 - The S3600-SI series do not support OSPF.
-

Introduction to IP Route and Routing Table

IP Route

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.

Routing Table

Function

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.

Routes in a routing table can be divided into three categories by origin:

- Direct routes: Routes discovered by data link protocols, also known as interface routes.
- Static routes: Routes that are manually configured.
- Dynamic routes: Routes that are discovered dynamically by routing protocols.

Routing entry

Each routing entry in a routing table contains:

- Destination: It identifies the address of the destination host or network of an IP packet.
- Mask: Along with the destination address, it identifies the address of the network segment where the destination host or router resides. By performing a logical AND operation 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.

- Interface: It indicates through which interface IP packets should be forwarded to the destination.
- Nexthop: It indicates the next router that IP packets will pass through to reach the destination.
- Preference: 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.

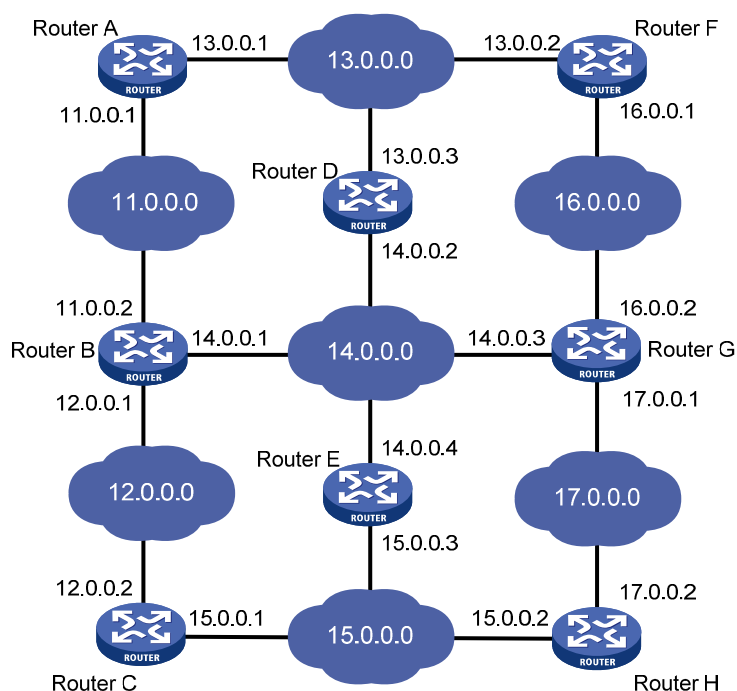
In addition, according to whether the network where the destination resides is directly connected to the router, routes fall into the following categories:

- 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 1-1](#) shows a relatively complicated internet environment, the number in each network cloud indicate the network address. Router G is connected to three networks, and so it has three IP addresses and three physical ports. Its routing table is shown in [Figure 1-1](#).

Figure 1-1 Routing table



Destination Network	Nexthop	Interface
11.0.0.0	14.0.0.1	3
12.0.0.0	14.0.0.1	3
13.0.0.0	16.0.0.1	2
14.0.0.0	14.0.0.3	3
15.0.0.0	17.0.0.2	1

16.0.0.0	16.0.0.2	2
17.0.0.0	17.0.0.1	1

Routing Protocol Overview

Static Routing and Dynamic Routing

Static routing is easy to configure and requires less system resources. It works well in small, stable networks with simple topologies. It cannot adapt itself to any network topology change automatically so that you must perform routing configuration again whenever the network topology changes.

Dynamic routing is based on dynamic routing protocols, which can detect network topology changes and recalculate the routes accordingly. Therefore, dynamic routing is suitable for large networks. It is complicated to configure, and it not only imposes higher requirements on the system than static routing, but also occupies a certain amount of network resources.

Classification of Dynamic Routing Protocols

Dynamic routing protocols can be classified based on the following standards:

Operational scope

- Interior Gateway Protocols (IGPs): Work within an autonomous system, typically including RIP, OSPF, and IS-IS.
- Exterior Gateway Protocols (EGPs): Work between autonomous systems. The most popular one is BGP.



Note

An autonomous system refers to a group of routers that share the same route policy and work under the same administration.

Routing algorithm

- Distance-vector protocols: RIP and BGP. BGP is also considered a path-vector protocol.
- Link-state protocols: OSPF and IS-IS.

The main differences between the above two types of routing algorithms lie in the way routes are discovered and calculated.

Type of the destination address

- Unicast routing protocols: RIP, OSPF, BGP, and IS-IS.
- Multicast routing protocols: PIM-SM and PIM-DM.

This chapter focuses on unicast routing protocols. For information on multicast routing protocols, refer to the part discussing *Multicast*.

Routing Protocols and Routing Priority

Different routing protocols may find different routes (including static routes) to the same destination. However, not all of those routes are optimal. In fact, at a particular moment, only one protocol can uniquely determine the current optimal routing to the destination. For the purpose of route selection, each routing protocol (including static routes) is assigned a priority. The route found by the routing protocol with the highest priority is preferred.

The following table lists some routing protocols and the default priorities for routes found by them:

Table 1-1 Routing protocols and priorities of their default route

Routing approach	Priority
DIRECT	0
OSPF	10
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
UNKNOWN	255



Note

- The smaller the priority value, the higher the priority.
- The priority for a direct route is always 0, which you cannot change. Any other type of routes can have their priorities manually configured.
- Each static route can be configured with a different priority.

Load Sharing and Route Backup

Load sharing

A given routing protocol may find several routes with the same metric to the same destination, and if this protocol has the highest priority among all the active protocols, these routes will be considered valid and are used to forward packets, thus achieving load sharing.

Route backup

You can configure multiple routes to the same destination, expecting the one with the highest priority to be the primary route and all the rest backup routes.

Route backup can help improve network reliability. Automatic switching can happen between the primary route and a backup route.

Under normal circumstances, packets are forwarded through the primary route. When the primary route goes down, the route with the highest priority among the backup routes is selected to forward packets. When the primary route recovers, the route selection process is performed again and the primary route is selected again to forward packets.

Routing Information Sharing

As different routing protocols use different algorithms to calculate routes, they may discover different routes. In a large network with multiple routing protocols, it is required for routing protocols to share their routing information. Each routing protocol shares routing information discovered by other routing protocols through a route redistribution mechanism.

Displaying and Maintaining a Routing Table

To do...	Use the command...	Remarks
Display brief information about a routing table	display ip routing-table [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display detailed information about a routing table	display ip routing-table verbose	
Display information about routes permitted by a basic ACL	display ip routing-table acl <i>acl-number</i> [verbose]	
Display information about routes permitted by a prefix list	display ip routing-table ip-prefix <i>ip-prefix-name</i> [verbose]	
Display routes to a specified destination	display ip routing-table <i>ip-address</i> [<i>mask</i> <i>mask-length</i>] [longer-match] [verbose]	
Display routes to specified destinations	display ip routing-table <i>ip-address1</i> { <i>mask1</i> <i>mask-length1</i> } <i>ip-address2</i> { <i>mask2</i> <i>mask-length2</i> } [verbose]	
Display routes discovered by a routing protocol	display ip routing-table protocol <i>protocol</i> [inactive verbose]	
Display the tree-structured routing table information	display ip routing-table radix	
Display statistics about a routing table	display ip routing-table statistics	
Clear statistics about a routing table	reset ip routing-table statistics protocol { all <i>protocol</i> }	Available in user view

2 Static Route Configuration

When configuring a static route, go to these sections for information you are interested in:

- [Introduction to Static Route](#)
- [Static Route Configuration](#)
- [Displaying and Maintaining Static Routes](#)
- [Static Route Configuration Example](#)
- [Troubleshooting a Static Route](#)



Note

The term **router** in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.

Introduction to Static Route

Static Route

Static routes are special routes. They are manually configured by 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.

When the network topology changes, static routes may become unreachable because they cannot adapt themselves to the change automatically, thus resulting in network interruption. In this case, the network administrator needs to modify the configuration of static routes manually.

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.

Default Route

To avoid too large a routing table, you can configure a default route.

When the destination address of a packet fails to match any entry in the routing table,

- If there is default route in the routing table, the default route will be selected to forward the packet.
- If there is no default route, the packet will be discarded and an ICMP Destination Unreachable or Network Unreachable packet will be returned to the source.

A default route can be manually configured or generated by some dynamic routing protocols, such as OSPF and RIP.

Static Route Configuration

Configuration Prerequisites

Before configuring a static route, perform the following tasks:

- Configuring the physical parameters of related interfaces
- Configuring IP addresses for related interfaces

Configuring a Static Route

Follow these steps to configure a static route:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a static route	ip route-static <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-type</i> <i>interface-number</i> <i>next-hop</i> } [preference <i>preference-value</i>] [reject blackhole] [detect-group <i>group number</i>] [description <i>text</i>]	Required By default, the system can obtain the route to the subnet directly connected to the router.



Note

- Use the **ip route-static** command to configure a default route by setting the destination IP address and the mask to 0.0.0.0.
- Avoid configuring 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 policies.
- For automatic detection information, refer to the part discussing *Auto Detect*.

Displaying and Maintaining Static Routes

To do...	Use the command...	Remarks
Display the current configuration information	display current-configuration	Available in any view
Display the brief information of a routing table	display ip routing-table	
Display the detailed information of a routing table	display ip routing-table verbose	
Display the information of static routes	display ip routing-table protocol static [inactive verbose]	
Delete all static routes	delete static-routes all	Available in system view

Static Route Configuration Example

Network requirements

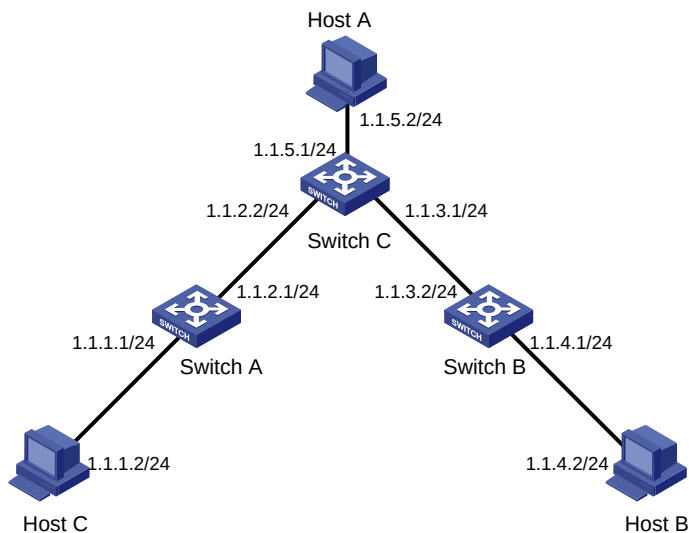
A small company requires that any two nodes in its office network communicate with each other, and that the network structure be simple and stable. The company hopes that the existing devices that do not support any dynamic routing protocol can be fully utilized.

In this case, static routes can implement communication between any two nodes.

Network diagram

According to the network requirements, the network topology is designed as shown in [Figure 2-1](#).

Figure 2-1 Network diagram for static route configuration



Configuration procedure



Note

When only one interface of the device is interconnected with another network segment, you can implement network communication by configuring either a static route or default route.

1) Perform the following configurations on the switch.

Approach 1: Configure static routes on Switch A.

```
<SwitchA> system-view
[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
```

Approach 2: Configure a static route on Switch A.

```
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.2.2
```

Approach 1: Configure static routes on Switch B.

```
<SwitchB> system-view
[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
```

Approach 2: Configure a static route on Switch B.

```
<SwitchB> system-view
[SwitchB] ip route-static 0.0.0.0 0.0.0.0 1.1.3.1
```

Configure static routes on Switch C.

```
<SwitchC> system-view
[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
```

2) Perform the following configurations on the host.

Set the default gateway address of Host A to 1.1.5.1. Detailed configuration procedure is omitted.

Set the default gateway address of Host B to 1.1.4.1. Detailed configuration procedure is omitted.

Set the default gateway address of Host C to 1.1.1.1. Detailed configuration procedure is omitted.

Now, all the hosts and switches in the figure can communicate with each other.

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 forwarded on the interface.

Solution: Perform the following procedure.

- 1) Use the **display ip routing-table protocol static** command to view whether the corresponding static route is correctly configured.
- 2) Use the **display ip routing-table** command to view whether the static route is valid.

3 RIP Configuration

When configuring RIP, go to these sections for information you are interested in:

- [RIP Overview](#)
- [RIP Configuration Task List](#)
- [RIP Configuration Example](#)
- [Troubleshooting RIP Configuration](#)



Note

The term **router** in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.

RIP Overview

Routing information protocol (RIP) is a simple interior gateway protocol (IGP) suitable for small-sized networks. RIP is not recommended in complicated large networks.

Basic Concepts

RIP

RIP is a distance-vector (D-V) algorithm-based protocol. It uses port 520 to exchange 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. This limitation makes RIP not suitable for large networks.

To improve performance and avoid routing loop, RIP supports split horizon. Besides, RIP can import routes discovered by other routing protocols.

RIP routing database

Each RIP router has a routing table containing routing entries of all reachable destinations, and each routing entry contains:

- Destination address: IP address of a host or network.
- Next hop: IP address of an interface on the adjacent router that IP packets should pass through to reach the destination.

- Interface: Outbound interface on this router, through which IP packets should be forwarded to reach the destination.
- Metric: Cost from the local router to the destination.
- Route time: Time elapsed since the routing entry was last updated. The time is reset to 0 every time the routing entry is updated.

RIP timers

As defined in RFC 1058, RIP is controlled by three timers: Period update, Timeout, and Garbage-collection.

- Period update timer: The period update timer defines the interval between routing updates.
- Timeout timer: The timeout timer defines the route aging time. If no update for a route is received after the aging time elapses, the metric of the route is set to 16 in the routing table.
- Garbage-collection timer: The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the Garbage-Collect timer length, RIP advertises the route with the routing metric set to 16. If no update is announced for that route after the Garbage-Collect timer expires, the route will be deleted from the routing table.

Routing loops prevention

RIP is a distance-vector (D-V) based routing protocol. Since a RIP router advertises its own routing table to neighbors, routing loops may occur.

RIP uses the following mechanisms to prevent routing loops.

- Counting to infinity. The metric value of 16 is defined as unreachable. When a routing loop occurs, the metric value of the route will increment to 16.
- Split horizon. A router does not send the routing information learned from a neighbor back to the neighbor to prevent routing loops and save the bandwidth.

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 updates its local routing table and sends a triggered update packet to the neighbors. Upon receiving the triggered update 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 aging mechanism to handle the timeout routes to ensure real-time and valid routes.

RIP Configuration Task List

Complete the following tasks to configure RIP:

Task		Remarks
Configuring Basic RIP Functions	Enabling RIP on the interfaces attached to a specified network segment	Required
	Setting the RIP operating status on an interface	Optional
	Specifying the RIP version on an interface	Optional
Configuring RIP Route Control	Setting the additional routing metrics of an interface	Optional
	Configuring RIP route summarization	Optional
	Disabling the router from receiving host routes	Optional
	Configuring RIP to filter incoming/outgoing routes	Optional
	Setting RIP preference	Optional
	Enabling load sharing among RIP interfaces	Optional
	Configuring RIP to redistribute routes from another protocol	Optional
RIP Network Adjustment and Optimization	Configuring RIP timers	Optional
	Configuring split horizon	Optional
	Configuring RIP-1 packet zero field check	Optional
	Setting RIP-2 packet authentication mode	Optional
	Configuring RIP to unicast RIP packets	Optional

Basic RIP Configuration

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

Configuring Basic RIP Functions

Enabling RIP on the interfaces attached to a specified network segment

Follow these steps to enable RIP on the interfaces attached to a specified network segment:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable RIP and enter RIP view	rip	Required
Enable RIP on the specified interface	network <i>network-address</i>	Required Disabled by default



Note

- Related RIP commands configured in interface view can take effect only after RIP is enabled.
- RIP operates on the interfaces attached to a specified network segment. 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 any interface route. Therefore, after RIP is enabled globally, you must also specify its operating network segments to enable it on the corresponding interfaces.

Setting the RIP operating status on an interface

Follow these steps to set the RIP operating status on an interface:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the interface to receive RIP update packets	rip input	Optional Enabled by default
Enable the interface to send RIP update packets	rip output	
Enable the interface to receive and send RIP update packets	rip work	

Specifying the RIP version on an interface

Follow these steps to specify the RIP version on an interface:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Specify the version of the RIP running on the interface	rip version { 1 2 [broadcast multicast] }	Optional By default, the version of the RIP running on an interface is RIP-1.

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 summarization and disabling the receiving of host routes.
- Filter incoming and outgoing 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.
- Redistribute external routes in an environment with multiple routing protocols.

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

Configuring RIP Route Control

Setting the additional routing metrics of an interface

Additional metric is the metric added to the original metrics of RIP routes on an interface. It does not directly change the metric value of a RIP route in the routing table of a router, but will be added to incoming or outgoing RIP routes on the interface.

Follow these steps to set additional routing metric:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type interface-number</i>	—
Set the additional routing metric to be added for incoming RIP routes on this interface	rip metricin <i>value</i>	Optional 0 by default
Set the additional routing metric to be added for outgoing RIP routes on this interface	rip metricout <i>value</i>	Optional 1 by default



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.

Configuring RIP route summarization

Rip route summarization means that when the router advertises RIP updates, 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 the size of the routing table.

When it is necessary to advertise RIP route updates in a subnet, disable the route summarization for RIP-2.

Follow these steps to configure RIP route summarization:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter RIP view	rip	—
Enable RIP-2 automatic route summarization	summary	Required Enabled by default

Disabling the router from receiving 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 a router is disabled from receiving host routes, it can refuse any incoming host route.

Follow these steps to disable the router from receiving host routes:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter RIP view	rip	—
Disable the router from receiving host routes	undo host-route	Required By default, the router receives host routes.

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, address prefix list, or route policy to make RIP filter incoming/outgoing routes. Besides, you can configure RIP to receive only the RIP packets from a specific neighbor.

Follow these steps to configure RIP to filter incoming/outgoing routes:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter RIP view	rip	—
Configure RIP to filter incoming routes	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> [gateway <i>ip-prefix-name</i>] route-policy <i>route-policy-name</i> } 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 <i>ip-prefix-name</i> import	

To do...	Use the command...	Remarks
Configure RIP to filter outgoing routes	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>protocol</i> [<i>process-id</i>]]	Required By default, RIP does not filter any outgoing route.
	filter-policy route-policy <i>route-policy-name</i> 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 redistributed with the **import-route** command and routes learned from neighbors.
- You can also use the **filter-policy export** command to filter outgoing routes redistributed from a specified routing protocol.

Setting RIP preference

Follow these steps to set RIP preference:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter RIP view	rip	—
Set the RIP preference	preference <i>value</i>	Required 100 by default

Enabling load sharing among RIP interfaces

Follow these steps to enable load sharing among RIP interfaces:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter RIP view	rip	—
Enable load sharing among RIP interfaces	traffic-share-across-interface	Required Disabled by default

Configuring RIP to redistribute routes from another protocol

Follow these steps to configure RIP to import routes from another protocol:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter RIP view	rip	—

To do...	Use the command...	Remarks
Configure a default cost for an incoming route	default cost <i>value</i>	Optional 1 by default
Configure RIP to redistribute routes from another protocol	import-route <i>protocol</i> [<i>process-id</i>] [cost <i>value</i> route-policy <i>route-policy-name</i>]*	Required By default, RIP does not redistribute any route from other protocols.

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 loops by configuring split horizon;
- Packet validation in network environments with high security requirements, and
- Configuring RIP to unicast RIP messages on interfaces with special requirements.

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

Configuration Tasks

Configuring RIP timers

Follow these steps to configure RIP timers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter RIP view	rip	—
Set the RIP timers	timers { update <i>update-timer</i> timeout <i>timeout-timer</i> } *	Required By default, the Update timer is 30 seconds and the Timeout timer 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.

Configuring split horizon

Follow these steps to configure split horizon:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type interface-number</i>	—
Enable split horizon	rip split-horizon	Required Enabled by default



Note

Split horizon cannot be disabled on a point-to-point link.

Configuring RIP-1 packet zero field check

Follow these steps to configure RIP-1 packet zero field check:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter RIP view	rip	—
Enable the check of the must be zero field in RIP-1 packets	checkzero	Required Enabled by default



Note

Some fields in a RIP-1 packet must be 0, and they are known as **must be zero** field. For RIP-1, the **must be zero** field is checked for incoming packets, and those RIP-1 packets with this field being nonzero will not be processed.

Setting RIP-2 packet authentication mode

RIP-2 supports two authentication modes: simple authentication and message digest 5 (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.

Follow these steps to set RIP-2 packet authentication mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type interface-number</i>	—

To do...	Use the command...	Remarks
Set RIP-2 packet authentication mode	rip authentication-mode { simple password md5 { rfc2082 key-string key-id rfc2453 key-string } }	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)

Configuring RIP to unicast RIP packets

Follow these steps to configure RIP to unicast RIP packets:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter RIP view	rip	—
Configure RIP to unicast RIP packets	peer ip-address	Required When RIP runs on the link that does not support broadcast or multicast, you must configure RIP to unicast RIP packets.

Displaying and Maintaining RIP Configuration

To do...	Use the command...	Remarks
Display the current RIP running status and configuration information	display rip	Available 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	Available in RIP view

RIP Configuration Example

Network requirements

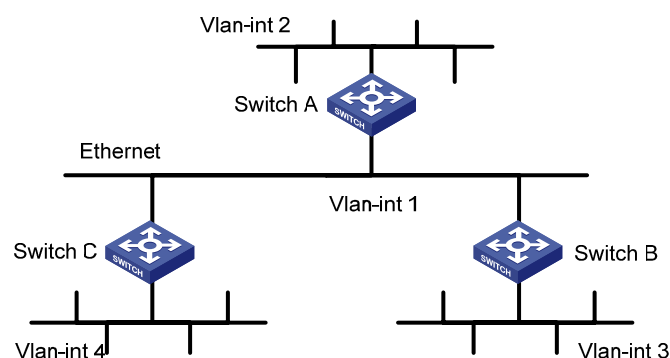
A small-sized company requires that any two nodes in its small office network communicate with each other, and that the network devices automatically adapt themselves to any topology change so as to reduce the work of manual maintenance.

In this case, RIP can implement communication between any two nodes.

Network diagram

According to the network requirements, the network topology is designed as shown in [Figure 3-1](#).

Figure 3-1 Network diagram for RIP configuration



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int1	110.11.2.1/24	Switch B	Vlan-int1	110.11.2.2/24
	Vlan-int2	155.10.1.1/24		Vlan-int3	196.38.165.1/24
Switch C	Vlan-int1	110.11.2.3/24			
	Vlan-int4	117.102.0.1/16			

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 Switch A:

Configure RIP.

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip] network 110.11.2.0
[SwitchA-rip] network 155.10.1.0
```

2) Configure Switch B:

Configure RIP.

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip] network 196.38.165.0
[SwitchB-rip] network 110.11.2.0
```

3) Configure Switch C:

Configure RIP.

```
<SwitchC> system-view
[SwitchC] rip
[SwitchC-rip] network 117.102.0.0
[SwitchC-rip] network 110.11.2.0
```

Troubleshooting RIP Configuration

Failed to Receive RIP Updates

Symptom

The Ethernet switch cannot receive any RIP update when the physical connection between the switch and the peer routing device is normal.

Solution

Check that:

- RIP is enabled by using the **network** command on the corresponding interface.
- The interface is allowed to receive or send RIP packets.
- The interface receives RIP packets in the way the peer device sends them, for example, in the broadcast or multicast mode.

4 OSPF Configuration

When configuring OSPF, go to these sections for information you are interested in:

- [OSPF Overview](#)
- [OSPF Configuration Task List](#)
- [Displaying and Maintaining OSPF Configuration](#)
- [OSPF Configuration Examples](#)
- [Troubleshooting OSPF Configuration](#)



Note

- The term **router** in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.
 - The S3600-SI series do not support OSPF.
-

OSPF Overview

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 various networks in size, and even networks with 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 first algorithm according to the collected link states, it guarantees that no loop routes will be generated.
- 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 summarized 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.

OSPF Route Calculation

Taking no account of area partition, the routing calculation process of the OSPF protocol is as follows:

- Each OSPF-supported 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 transform the LSDB to a weighted, directed graph, which reflects the real topology of the whole network. All routers get exactly the same weighted, directed graph.
- According to the weighted, directed graph, each 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. 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 adjacencies 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 "[DR/BDR introduction](#)".

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).

Basic OSPF Concepts

Autonomous System

A set of routers using the same routing protocol to exchange routing information constitute an Autonomous System (AS).

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 loopback interface 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.

OSPF Packets

OSPF uses five types of packets:

- 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, DR, BDR and known neighbors.

- DD packet:

When two routers synchronize their databases, they use database description (DD) packets to describe their own LSDBs, including the summary of each LSA. The summary refers to the header of an LSA

which uniquely identifies the LSA. This reduces the size of traffic transmitted between the routers because the header of an LSA only occupies a small portion of the LSA. With the header, the peer router can judge whether it has the LSA or not.

- 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.

- 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).

- LSAck packet

Link state acknowledgment (LSAck) packets are used to acknowledge received LSU packets. An LSAck contains the header(s) of LSA(s) to be acknowledged (One LSAck packet can acknowledge multiple LSAs).

LSA Types

1) 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 originating area.
- Network-LSA: Type-2 LSAs, generated by the DRs on a broadcast or NBMA network to describe the link states of the current network segment, and are advertised only in the originating area.
- 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 and NSSA areas). The default AS route can also be described by AS-external-LSAs.

2) 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).

Neighbor and Adjacency

In OSPF, **neighbor** and **adjacency** are two different concepts.

Neighbor: Two routers that have interfaces to a common network. Neighbor relationships are maintained by, and usually dynamically discovered by, OSPF's hello packets. When a router starts, it

sends a hello packet through the OSPF interface, and the router that receives the hello packet checks parameters carried in the packet. If parameters of the two routers match, they become neighbors.

Adjacency: A relationship formed between selected neighboring routers for the purpose of exchanging routing information. Not every pair of neighboring routers become adjacent, which depends on network types. Only by synchronizing the LSDB via exchanging DD packets and LSAs can two routers become adjacent.

OSPF Area Partition and Route Summarization

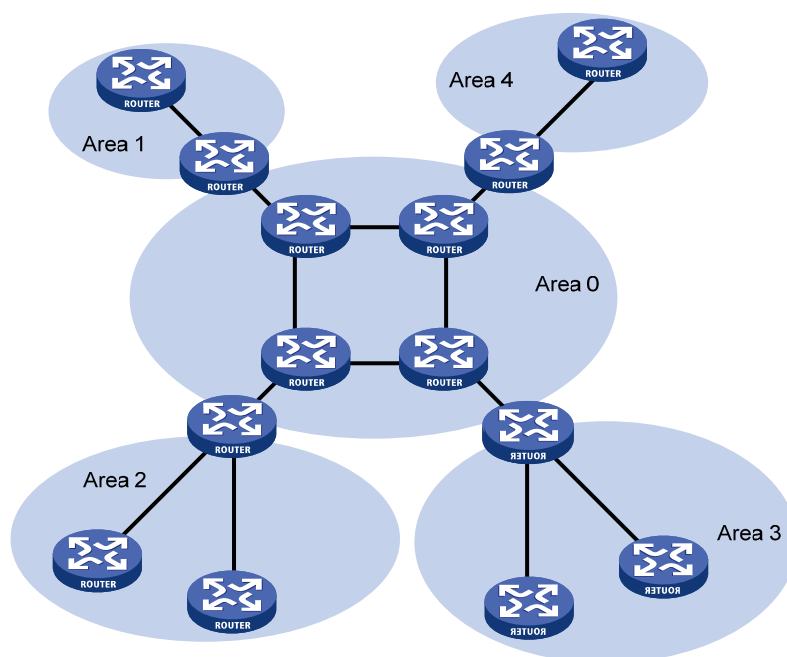
Area partition

If all the routers on an ever-growing large 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 likely to have changes in the network topology. Hence, the network will often be “flapping”, and a great number of OSPF packets will be generated and transmitted in the network. This will lower the network bandwidth utilization. Even worse, any change of the topology will cause all the routers on the network to re-perform route calculation.

OSPF solves the above-mentioned problem by dividing an AS into multiple areas. Areas refer to groups into which routers are logically divided. Each group is identified by an Area ID, as shown in [Figure 4-1](#).

Figure 4-1 OSPF area partition



On the border of an area is a router, which belongs to different areas. After area partition, area border routers perform route summarization to reduce the number of LSAs advertised to other areas and minimize the effect of topology changes.

Classification of routers

The OSPF router falls into four types according to the position in the AS:

- 1) Internal router

All interfaces on an internal router belong to one OSPF area.

2) Area border router (ABR)

An area border router belongs to more than two areas, one of which must be the backbone area. It connects the backbone area to a non-backbone area. The connection between an area border router and the backbone area can be physical or logical.

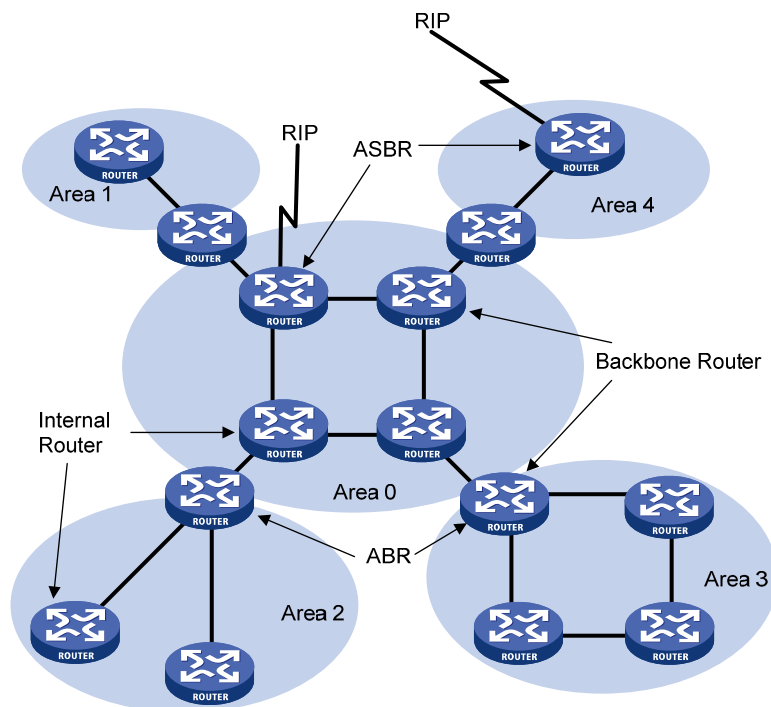
3) Backbone router

At least one interface of a backbone router must be attached to the backbone area. Therefore, all ABRs and internal routers in area 0 are backbone routers.

4) Autonomous system border router (ASBR)

The router exchanging routing information with another AS is an ASBR, which may not reside on the boundary of the AS. It can be an internal router or area border router.

Figure 4-2 OSPF router types



5) Type-7 LSAs translator

A Type-7 LSAs translator takes effect on an ABR. The state of the Type-7 LSAs translator determines whether the ABR needs to translate Type-7 LSAs into Type-5 LSAs.

- When the Type-7 LSAs translator state is **Enabled** or **Elected**, the ABR translates Type-7 LSAs into Type-5 LSAs.
- When the Type-7 LSAs translator state is **Disabled**, the ABR does not translate Type-7 LSAs into Type-5 LSAs.

Backbone area and virtual link

1) 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. Routing information between non-backbone areas must be forwarded by the backbone area. Therefore, OSPF requires:

- All non-backbone areas must maintain connectivity to the backbone area.
- The backbone area itself must maintain connectivity.

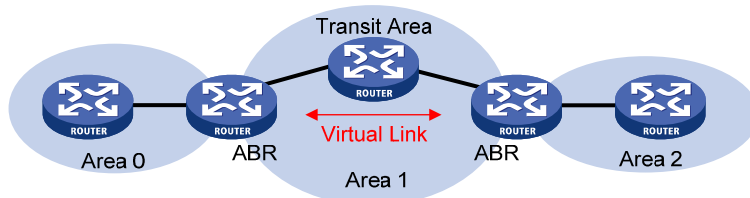
In practice, due to physical limitations, the requirements may not be satisfied. In this case, configuring OSPF virtual links is a solution.

2) Virtual link

A virtual link is established between two area border routers through a non-backbone area and is configured on both ABRs to take effect. The area that provides the non-backbone area internal route for the virtual link is a “transit area”.

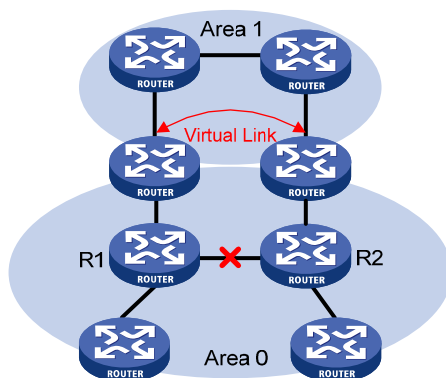
In the following figure, Area 2 has no direct physical link to the backbone area 0. Configuring a virtual link between ABRs can connect Area 2 to the backbone area.

Figure 4-3 Virtual link application 1



Another application of virtual links is to provide redundant links. If the backbone area cannot maintain internal connectivity due to a physical link failure, configuring a virtual link can guarantee logical connectivity in the backbone area, as shown below.

Figure 4-4 Virtual link application 2



The virtual link between the two ABRs acts as a point-to-point connection. Therefore, you can configure interface parameters such as hello packet interval on the virtual link as they are configured on physical interfaces.

The two ABRs on the virtual link exchange OSPF packets with each other directly, the OSPF routers in between simply convey these OSPF packets as normal IP packets.

(Totally) Stub area

The ABR in a stub area does not distribute Type-5 LSAs into the area, so the routing table scale and amount of routing information in this area are reduced significantly.

You can also configure the stub area as a Totally Stub area, where the ABR advertises neither the routes of other areas nor the external routes.

Stub area configuration is optional, and not every area is qualified to be a stub area. In general, a stub area resides on the border of the AS.

The ABR in a stub area generates a default route into the area.

Note the following when configuring a (totally) stub area:

- The backbone area cannot be a (totally) stub area
- The **stub** command must be configured on routers in a (totally) stub area
- A (totally) stub area cannot have an ASBR because AS external routes cannot be distributed into the stub area.
- Virtual links cannot transit (totally) stub areas.

NSSA area

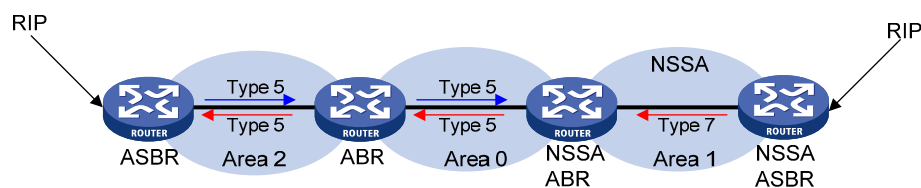
Similar to a stub area, an NSSA area imports no AS external LSA (Type-5 LSA) but can import Type-7 LSAs that are generated by the ASBR and distributed throughout the NSSA area. When reaching the NSSA ABR, Type-7 LSAs are translated into Type-5 LSAs by the ABR (the Type-7 LSAs translator state must be **enabled/elected**) before being advertised to other areas.

In the following figure, the OSPF AS contains three areas: Area 1, Area 2 and Area 0. The other two ASs employ the RIP protocol. Area 1 is an NSSA area, and the ASBR in it translates RIP routes into Type-7 LSAs and advertises them throughout Area 1. When these LSAs reach the NSSA ABR with the Type-7 LSAs translator state as **Enabled** or **Elected**, the ABR translates Type-7 LSAs to Type-5 LSAs for advertisement to Area 0 and Area 2.

On the left of the figure, RIP routes are translated into Type-5 LSAs by the ASBR of Area 2 and distributed into the OSPF AS. However, Area 1 is an NSSA area, so these Type-5 LSAs cannot travel to Area 1.

Similar to stub areas, virtual links cannot transit NSSA areas.

Figure 4-5 NSSA area



Route summarization

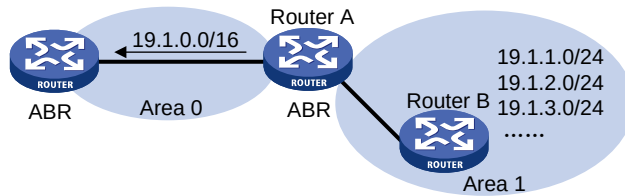
Route summarization: An ABR or ASBR summarizes routes with the same prefix with a single route and distribute it to other areas.

After an AS is divided into different areas that are interconnected through OSPF ABRs, The routing information between areas can be reduced through route summarization. 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 summarization configuration) and sends the LSA outside the area.

For example, as shown in the following figure, in Area 1 are three internal routes 19.1.1.0/24, 19.1.2.0/24, and 19.1.3.0/24. By configuring route summarization on Router A, the three routes are summarized with the route 19.1.0.0/16 that is advertised into Area 0.

Figure 4-6 Route summarization



OSPF has two types of route summarization:

2) ABR route summarization

To distribute routing information to other areas, an ABR generates Type-3 LSAs on a per network segment basis for an attached non-backbone area. If contiguous network segments are available in the area, you can summarize them with a single network segment. The ABR in the area distributes only the summary LSA to reduce the scale of LSDBs on routers in other areas.

3) ASBR route summarization

If summarization for redistributed routes is configured on an ASBR, it will summarize redistributed Type-5 LSAs that fall into the specified address range. If in an NSSA area, it also summarizes Type-7 LSAs that fall into the specified address range.

If this feature is configured on an ABR, the ABR will summarize Type-5 LSAs translated from Type-7 LSAs.

Route types

OSPF prioritizes routes into four levels:

- Intra-area route
- Inter-area route
- type1 external route
- type2 external route

The intra-area and inter-area routes describe the network topology of the AS, while external routes describe routes to destinations outside the AS. OSPF classifies external routes into two types: type1 and type2.

A type1 external route is an IGP route, such as a RIP or static route, which has high credibility and whose cost is comparable with the cost of an OSPF internal route. The cost from a router to the destination of the type1 external route = the cost from the router to the corresponding ASBR + the cost from the ASBR to the destination of the external route.

A type2 external route is an EGP route, which has low credibility, so OSPF considers the cost from the ASBR to the destination of the type2 external route is much bigger than the cost from the ASBR to an OSPF internal router. Therefore, the cost from the internal router to the destination of the type2 external route = the cost from the ASBR to the destination of the type2 external route. If two routes to the same destination have the same cost, then take the cost from the router to the ASBR into consideration.

OSPF Network Type

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 to the multicast address (224.0.0.5) by default, but protocol packets can be sent in the unicast address as needed.
- 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).

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 neighbor, 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.
- Since NBMA interfaces send packets to unicast addresses, you need to configure neighbors manually. By default, P2MP sends protocol packets to multicast addresses.

DR/BDR

DR/BDR introduction

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, $n \times (n-1)/2$ 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.

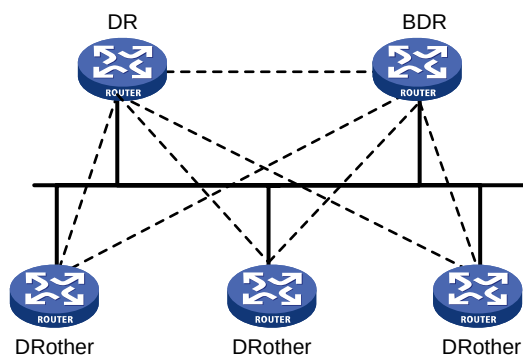
A BDR provides backup for a DR. DR and BDR are elected at the same time. Adjacencies are also established between the BDR and all the other routers on the segment, and routing information is also

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.

On an OSPF network, a router which is neither DR nor BDR is called DR Other. It establishes adjacencies with the DR and BDR, but not with other DR Others. This reduces not only the number of adjacencies among routers, but also the network traffic and occupied bandwidth resources on the broadcast or NBMA network.

In [Figure 4-7](#), 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 4-7 DR/BDR



DR/BDR election

The DR and BDR in a network are elected by all routers rather than configured manually. The DR priority of an interface determines its qualification for DR/BDR election. Interfaces attached to the network and having priorities higher than '0' are election candidates.

The election votes are hello packets. Each router sends the DR elected by itself in a hello packet to all the other routers. If two routers on the network declare themselves as the DR, the router with the higher DR priority wins. If DR priorities are the same, the router with the higher Router ID wins. In addition, a router with the priority 0 cannot become the DR/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.
- The priority of a router affects the DR and BDR election. However, it has no effect on the election after the DR and BDR election ends. A new priority assigned to the router takes effect at the time of next DR and BDR election.
- 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 unnecessarily the router with the highest priority. Likewise, the BDR is unnecessarily the router with the second highest priority.

OSPF Features

The switches 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: NSSA 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.
- Packet authentication: OSPF supports the authentication of the packets between neighboring routers in the same area by using one of the two methods: plain text authentication and MD5 authentication.
- 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.

OSPF Configuration Task List

Complete the following tasks to configure OSPF:

Task		Remarks
Basic OSPF Configuration		Required
OSPF Area Attribute Configuration		Optional
OSPF Network Type Configuration	Configuring the Network Type of an OSPF Interface	Optional
	Configuring an NBMA/P2MP Neighbor	Optional
	Configuring the DR Priority on an OSPF Interface	Optional
OSPF Route Control	Configuring OSPF Route Summarization	Optional
	Configuring OSPF to Filter Received Routes	Optional
	Configuring the OSPF Cost on an Interface	Optional
	Configuring OSPF Route Priority	Optional
	Configuring the Maximum Number of OSPF ECMP Routes	Optional
	Configuring OSPF to Redistribute External Routes	Optional

Task		Remarks
OSPF Network Adjustment and Optimization	Configuring OSPF Timers	Optional
	Configuring the LSA transmission delay	Optional
	Configuring the SPF Calculation Interval	Optional
	Disabling OSPF Packet Transmission on an Interface	Optional
	Configuring OSPF Authentication	Optional
	Configuring the MTU Field in DD Packets	Optional
	Enabling OSPF Logging of Neighbor State Changes	Optional
	Configuring OSPF Network Management	Optional

Basic OSPF Configuration

Before you can configure other OSPF features, you must first enable OSPF and specify the interface and area ID.

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

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 IP address of an interface on the router to the router ID.

- Enabling OSPF

The switches support 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.

Follow these steps to perform basic OSPF configurations:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the router ID	router id <i>router-id</i>	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 [<i>process-id</i> [router-id <i>router-id</i>]]	Required Enter OSPF view.
Enter OSPF area view	area <i>area-id</i>	—
Configure the network segments in the area	network <i>ip-address wildcard-mask</i>	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.
- An OSPF process ID on a router must be unique.
- One segment can belong to only one area and you must specify each OSPF interface to belong to a particular area.

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 redistribute any external route. For this reason the concept of NSSA is introduced. Type-7 LSAs can be advertised in an NSSA. Type-7 LSAs are generated by ASBRs in the NSSA, and will be transformed into Type-5 LSAs (AS-external LSAs) when 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.

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

Configuring OSPF Area Attributes

Follow these steps to configure OSPF area attributes:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i>]]	—
Enter OSPF area view	area <i>area-id</i>	—
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 translate-always] *	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 <i>cost</i>	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 <i>router-id</i> [hello <i>seconds</i> retransmit <i>seconds</i> trans-delay <i>seconds</i> dead <i>seconds</i> simple <i>password</i> md5 <i>keyid</i> <i>key</i>] *	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.

OSPF Network Type Configuration

OSPF divides networks into four types by link layer protocol. See section "[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 network type of an interface as P2MP if not all the routers are directly accessible on an NBMA network. You can also configure the network type of an interface 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 election priority for each interface of a router to control the DR/BDR election in the network. Thus, the router with higher performance and reliability can be selected as a DR or BDR.

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

Configuring the Network Type of an OSPF Interface

Follow these steps to configure the network type of an OSPF interface:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the network type of the OSPF interface	ospf network-type { broadcast nbma p2mp [unicast] p2p }	Required 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.
- An adjacency can be established between two interfaces configured as broadcast, NBMA, or P2MP only if the interfaces are on the same network segment.
- If the network type of an interface is NBMA or is changed to NBMA, you must use the **peer** command to specify the peer.
- If the network type of an interface is P2MP and the **unicast** keyword is specified, an interface sends packets in the unicast mode. In this case, you must use the **peer** command to specify the peer.

Configuring an NBMA/P2MP Neighbor

When the network type of an interface on the router is one of the following types, you need to specify the IP address of the neighbor router:

- NBMA

- P2MP (required only when the interface sends packets in the unicast mode)

Since the neighbor routers cannot be discovered by broadcasting Hello packets, you must manually specify the IP address of the neighbor router. For an NBMA network, you can determine whether the neighbor has the DR election right.

Follow these steps to configure NBMA/P2MP neighbor:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i>]]	Required
Configure an NBMA/P2MP neighbor	peer <i>ip-address</i> [dr-priority <i>dr-priority</i>]	Required By default, the priority for the neighbor of an NBMA interface is 1.

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.

Follow these steps to configure the DR priority on an OSPF interface:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the DR priority on the OSPF interface	ospf dr-priority <i>priority</i>	Optional 1 by default



Note

The DR priorities configured by the **ospf dr-priority** command and the **peer** command have different purposes:

- 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 adjacencies.

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.

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 matching rules for routing information

Configuring OSPF Route Summarization

The configuration of OSPF route summarization includes:

- Configuring ABR route summarization,
- Configuring ASBR route summarization for imported routes.

Follow these steps to configure ABR route summarization:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i>]]	—
Enter area view	area <i>area-id</i>	—
Enable ABR route summarization	abr-summary <i>ip-address mask</i> [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.

Follow these steps to configure ASBR route summarization:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i>]]	—
Enable ASBR route summarization	asbr-summary <i>ip-address mask</i> [not-advertise tag <i>value</i>]	Required By default, summarization of imported routes is disabled.

Configuring OSPF to Filter Received Routes

Follow these steps to configure OSPF to filter received routes:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i>]]	—

To do...	Use the command...	Remarks
Configure to filter the received routes	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> gateway <i>ip-prefix-name</i> } 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 SPF algorithm (namely, routes in the OSPF routing table); only the routes passing the filter can be added to the routing table.

Configuring the OSPF Cost on an Interface

Follow these steps to configure the OSPF cost on an interface:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the OSPF cost on the interface	ospf cost <i>value</i>	Required By default, a VLAN interface on the switch, a fixed value of 10 is used.

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 system add the route discovered by the protocol with the highest priority to the routing table.

Follow these steps to configure OSPF route priority:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i>]]	—
Configure OSPF route priority	preference [ase] <i>value</i>	Required By default, the OSPF route priority is 10 and the priority of OSPF ASE is 150.

Configuring the Maximum Number of OSPF ECMP Routes

Follow these steps to configure the maximum number of OSPF ECMP routes:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i>]]	—
Configure the maximum number of OSPF ECMP routes	multi-path-number <i>value</i>	Optional 3 by default

Configuring OSPF to Redistribute External Routes

Follow these steps to configure OSPF to redistribute external routes:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i>]]	—
Configure OSPF to redistribute routes from another protocol	import-route <i>protocol</i> [<i>process-id</i>] [cost <i>value</i> type <i>value</i> tag <i>value</i> route-policy <i>route-policy-name</i>] *	Required By default, OSPF does not import the routing information of other protocols.
Configure OSPF to filter outgoing routes	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>protocol</i>]	Optional By default, OSPF does not filter advertised routes.
Enable OSPF to import the default route	default-route-advertise [always cost <i>value</i> type <i>type-value</i> route-policy <i>route-policy-name</i>] *	Optional By default, OSPF does not import the default route.
Configure the default parameters for redistributed routes, including cost, interval, limit, tag, and type	default { cost <i>value</i> interval <i>seconds</i> limit <i>routes</i> tag <i>tag</i> type <i>type</i> } *	Optional These parameters respectively default to: • Cost: 1 • Interval: 1 (second) • Limit: 1000 • Tag: 1 • 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, limit, tag, and type. A route tag can be used to identify protocol-related information.

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.

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

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.

Follow these steps to configure OSPF timers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—

To do...	Use the command...	Remarks
Configure the hello interval on the interface	ospf timer hello <i>seconds</i>	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 <i>seconds</i>	Optional 40 seconds by default
Configure the dead time of the neighboring router on the interface	ospf timer dead <i>seconds</i>	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 for retransmitting an LSA on an interface	ospf timer retransmit <i>interval</i>	Optional 5 seconds by default



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.

Configuring the LSA transmission delay

Follow these steps to configure the LSA transmission delay:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the LSA transmission delay	ospf trans-delay <i>seconds</i>	Required 1 second by default



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.

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 affect caused by frequent network changes.

Follow these steps to configure the SPF calculation interval:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i>]]	—
Configure the SPF calculation interval	spf-schedule-interval <i>interval</i>	Required 5 seconds by default

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.

Follow these steps to disable OSPF packet transmission on an interface:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i>]]	—
Disable OSPF packet transmission on a specified interface	silent-interface <i>silent-interface-type</i> <i>silent-interface-number</i>	Required 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 on which 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 adjacencies can be established on the interface. This enhances OSPF networking adaptability, thus reducing the consumption of system resources.

Configuring OSPF Authentication

Follow these steps to configure OSPF authentication:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i>]]	—
Enter OSPF area view	area <i>area-id</i>	—
Configure the authentication mode of the OSPF area	authentication-mode { simple md5 }	Required Not configured by default
Return to OSPF view	quit	—
Return to system view	quit	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the authentication mode of the OSPF interface	ospf authentication-mode { simple <i>password</i> md5 <i>key-id</i> <i>key</i> }	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 adjacencies 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.

Configuring the MTU Field in 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 interface MTU is filled in the MTU field in DD packets.

Follow these steps to configure to fill the MTU field when an interface transmits DD packets:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the interface to fill in the MTU field when transmitting DD packets	ospf mtu-enable	Required 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.

Enabling OSPF Logging of Neighbor State Changes

Follow these steps to enable OSPF logging of neighbor state changes:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter OSPF view	ospf [<i>process-id</i> [router-id <i>router-id</i>]]	—
Enable the OSPF logging of neighbor state changes	log-peer-change	Required Disabled by default

Configuring OSPF Network Management

Follow these steps to configure OSPF network management (NM):

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure OSPF MIB binding	ospf mib-binding <i>process-id</i>	Optional By default, OSPF MIB is bound to the first enabled OSPF process.
Enable OSPF Trap sending	snmp-agent trap enable ospf [<i>process-id</i>] [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.

Displaying and Maintaining OSPF Configuration

To do...	Use the command...	Remarks
Display the router ID	display router id	Available in any view
Display brief information about one or all OSPF processes	display ospf [<i>process-id</i>] brief	
Display OSPF statistics	display ospf [<i>process-id</i>] cumulative	
Display OSPF LSDB information	display ospf <i>process-id</i> <i>area-id</i> lsdb [brief [asbr network nssa router summary] [<i>ip-address</i>]] [originate-router <i>ip-address</i> self-originate]] display ospf [<i>process-id</i>] lsdb [brief [asbr ase network nssa router summary] [<i>ip-address</i>]] [originate-router <i>ip-address</i> self-originate]]	
Display OSPF peer information	display ospf [<i>process-id</i>] peer [brief statistics]	
Display OSPF next hop information	display ospf [<i>process-id</i>] nexthop	
Display OSPF routing table	display ospf [<i>process-id</i>] routing	

To do...	Use the command...	Remarks
Display OSPF virtual links	display ospf [<i>process-id</i>] vlink	
Display OSPF request list	display ospf [<i>process-id</i>] request-queue	
Display OSPF retransmission list	display ospf [<i>process-id</i>] retrans-queue	
Display the information about OSPF ABR and ASBR	display ospf [<i>process-id</i>] abr-asbr	
Display OSPF interface information	display ospf [<i>process-id</i>] interface <i>interface-type interface-number</i>	
Display OSPF errors	display ospf [<i>process-id</i>] error	
Display OSPF ASBR summarization information	display ospf [<i>process-id</i>] asbr-summary [<i>ip-address mask</i>]	
Reset OSPF process(es)	reset ospf { all <i>process-id</i> }	Available in user view
Clear the statistics of one or all OSPF processes	reset ospf statistics { all <i>process-id</i> }	

OSPF Configuration Examples

Configuring DR/BDR Election

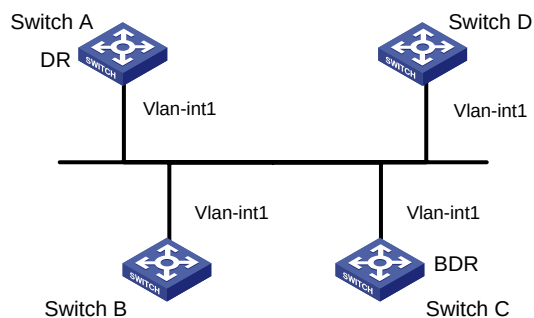
Network requirements

Use OSPF to realize interconnection between devices in a broadcast network. Devices with higher performance should become the DR and BDR to improve network performance. Devices with lower performance are forbidden to take part in DB/BDR election.

Based on the customer requirements and networking environment, assign proper priorities to interfaces.

Network diagram

Figure 4-8 Network diagram for DR/BDR election



Device	Interface	IP address	Router ID	Interface priority
Switch A	Vlan-int1	196.1.1.1/24	1.1.1.1	100
Switch B	Vlan-int1	196.1.1.2/24	2.2.2.2	0
Switch C	Vlan-int1	196.1.1.3/24	3.3.3.3	2
Switch D	Vlan-int1	196.1.1.4/24	4.4.4.4	1

Configuration procedure

Configure Switch A.

```

<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 Switch B.

```

<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 Switch C.

```

<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 Switch D.

```

<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 Switch A, run the **display ospf peer** command to display its OSPF peers. Note that Switch A has three peers.

The state of each peer is full, which means that adjacency is established between Switch A and each peer. Switch A and Switch C must establish adjacencies with all the switches on the network so that they can serve as the DR and BDR respectively on the network. Switch A is DR, while Switch C 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 Switch B to 200.

```

<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ospf dr-priority 200

```

On Switch A, use the **display ospf peer** command to display its OSPF neighbors. Note that the priority of Switch B has been changed to 200, but it is still not a DR.

The current DR is changed only when it is offline. Shut down Switch A, and use the **display ospf peer** command on Switch D to display its neighbors. Note that the original BDR (Switch C) becomes the DR and Switch B becomes BDR now.

If all Ethernet Switches on the network are removed from and then added to the network again, Switch B will be elected as the DR (with a priority of 200), and Switch A will be the BDR (with a priority of 100). Shutting down and restarting all the switches will bring about a new round of DR/BDR election on the network.

Configuring OSPF Virtual Link

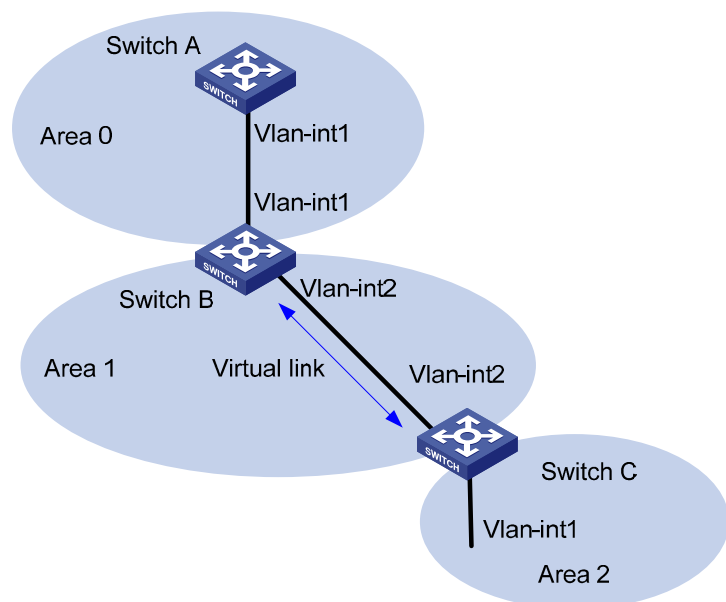
Network requirements

Devices in the network run OSPF to realize interconnection. The network is split into three areas: one backbone area and two non-backbone areas (Area 1 and Area 2). Area 2 has no direct connection to the backbone, and it has to reach the backbone through Area 1. The customer hopes that Area 2 can interconnect with other two areas.

Based on the customer requirements and networking environment, use a virtual link to connect Area 2 to the backbone area.

Network diagram

Figure 4-9 Network diagram for OSPF virtual link configuration



Device	Interface	IP interface	Router ID
Switch A	Vlan-int1	196.1.1.1/24	1.1.1.1
Switch B	Vlan-int1	196.1.1.2/24	2.2.2.2
	Vlan-int2	197.1.1.2/24	
Switch C	Vlan-int1	152.1.1.1/24	3.3.3.3
	Vlan-int2	197.1.1.1/24	

Configuration procedure

Configure Switch A.

```
<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 Switch B.

```
<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 Switch C.

```
<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
```

Troubleshooting OSPF Configuration

Unable to Establish a Neighbor Relationship between Routers

Symptom

No neighbor relationship can be established between neighboring routers.

Analysis

- 1) Verify that the routers work normally at the link layer.
- 2) Verify that the conditions for establishing a neighbor relationship are satisfied.
 - OSPF parameters on the interconnected interfaces must be consistent.
 - Area IDs on the interconnected interfaces must be the same.
 - Network ID and subnet masks of the interconnected interfaces must be consistent. (P2P networks and virtual link are excluded.)
 - The interconnected interfaces have the same type of network.
 - If the network type of the interface on the local router is NBMA, a neighbor must be specified by using the **peer** command.

Solution

Perform the following procedure.

- 1) Use the **display ip interface brief** command to verify that the link layer works normally.
- 2) Use the **ping** command to check network layer connectivity.
- 3) Use the **display ospf interface** command to view the OSPF interface configuration.
- 4) If the network type of an interface is NBMA, use the **display current-configuration configuration ospf** command to verify that a neighbor is specified for the router.
- 5) Use the **display ospf brief** command to check that the OSPF timers are consistent with those on the neighbor and that the dead time of the neighbor is four times the Hello interval.
- 6) Use the **display ospf peer** command to view neighbors.

Unable to Learn a Complete Network Topology

Symptom

The router running OSPF is unable to learn a complete network topology.

Analysis

Perform the following procedure to make analyses:

- 1) If multiple areas are configured on the router, check that one is specified as the backbone area.
- 2) Check that the backbone area is fully meshed.
- 3) Check that the backbone area is not configured as a Stub area or NSSA area.
- 4) Check that no virtual links are configured for the backbone area.
- 5) For a Stub area, check that the Stub attributes are configured for all routers in the area.
- 6) For an NSSA area, check that the NSSA attributes are configured for all routers in the area.
- 7) Check that Stub or NSSA areas are not a transit area of any virtual link. Virtual links cannot pass through a Stub or NSSA area.

Solution

Perform the following procedure:

- 1) Use the **display ospf peer** command to view the OSPF neighbor status.
- 2) Use the **display ospf interface** command to view the OSPF configuration on an interface.
- 3) Use the **display ospf lsdb** command to view the LSDB information.
- 4) Use the **display current-configuration configuration ospf** command to view area configurations.
- 5) If a virtual link is configured, use the **display ospf vlink** command to check that the OSPF virtual link is normal.

5 IP Route Policy Configuration

When configuring an IP route policy, go to these sections for information you are interested in:

- [IP Route Policy Overview](#)
- [IP Route Policy Configuration Task List](#)
- [Displaying IP Route Policy](#)
- [IP Route Policy Configuration Example](#)
- [Troubleshooting IP Route Policy](#)



Note

The term **router** in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.

IP Route Policy Overview

Introduction to IP Route Policy

Route policy is technology used to modify routing information to control the forwarding path of data packets. Route policy is implemented by changing the route attributes such as reachability.

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 control some attributes of the imported routes to make the routes meet the requirements of this protocol.

For the implementation of a route 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.

Filters

A routing protocol can reference an ACL, IP-prefix, or route policy to filter routing information. The following sections describe these filters.

ACL

You can specify a range of IP addresses or subnets when defining an ACL so as to match the destination network addresses or next-hop addresses in routing information. You can reference an ACL into a route policy to filter routing information.

For ACL configuration, refer to the part discussing ACL.

IP-prefix list

IP-prefix list plays a role similar to ACL. But it is more flexible than ACL and easier to understand. When IP-prefix list is applied to filter routing information, its matching object is the destination address field in routing information. Moreover, with IP-prefix list, you can use the **gateway** option to specify that only routing information advertised by certain routers will be received.

An IP-prefix list is identified by its IP-prefix name. Each IP-prefix list can contain multiple entries, and each entry, identified by an index-number, can independently specify the match range in the network prefix form. An index-number specifies the matching sequence in the IP-prefix list.

There is an OR relationship between entries. During the matching, the router checks entries identified by index-number in ascending order. Once an entry is matched, the IP-prefix list filtering is passed and no other entries will be checked.

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 ascending 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.

There is an OR relationship between different nodes in a route policy. As a result, the system examines the nodes in the route policy in sequence, and once the route matches a node in the route policy, it will pass the matching test of the route policy without entering the test of the next node.

IP Route Policy Configuration Task List

Complete the following tasks to configure an IP route policy:

Task		Remarks
Route Policy Configuration	Defining a Route Policy	Required
	Defining if-match Clauses and apply Clauses	Required
IP-Prefix Configuration		Required

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.

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

Defining a Route Policy

Follow these steps to define a route policy:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Define a route policy and enter the route policy view	route-policy <i>route-policy-name</i> { permit deny } node <i>node-number</i>	Required Not defined by default



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.

Defining if-match Clauses and apply Clauses

Follow these steps to define if-match clauses and apply clauses:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter the route-policy view	route-policy <i>route-policy-name</i> { permit deny } node <i>node-number</i>	Required
Define a rule to match the IP address of routing information	if-match { acl <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> }	Optional By default, no matching is performed on the address of routing information.
Define a rule to match the cost of routes	if-match cost <i>value</i>	Optional By default, no matching is performed against the cost of routes.
Define a rule to match the next-hop interface of routing information	if-match interface <i>interface-type</i> <i>interface-number</i>	Optional By default, no matching is performed on the next-hop interface of routing information.
Define a rule to match the next-hop address of routing information	if-match ip next-hop { acl <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> }	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 <i>value</i>	Optional By default, no matching is performed on the tag field of OSPF routing information.
Apply a cost to routes satisfying matching rules	apply cost <i>value</i>	Optional By default, no cost is applied to routes satisfying matching rules.
Define an action to set the tag field of routing information	apply tag <i>value</i>	Optional By default, no action is defined to set the tag field of OSPF routing information.



Note

- A route policy comprises multiple nodes. There is an OR relationship between the nodes in a route policy. As a result, the system examines the nodes in sequence, and once the route matches 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, there is an AND relationship between the **if-match** clauses for a route policy node. 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.

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.

Configuration Prerequisites

Before configuring a filter list, prepare the following data:

- IP-prefix name
- Range of addresses to be matched

Configuring an ip-prefix list

An IP-prefix list is identified by its IP-prefix list name. Each IP-prefix list can comprise multiple entries. Each entry 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 entries in ascending order of index-number. Once the route matches an entry, the route passes the filtering of the IP-prefix list and no other entry will be matched.

Follow these steps to configure an IPv4 IP-prefix list:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure an IPv4 IP-prefix list	ip ip-prefix <i>ip-prefix-name</i> [index <i>index-number</i>] { permit deny } <i>network len</i> [greater-equal <i>greater-equal</i> less-equal <i>less-equal</i>]	Required Not configured by default



Note

If all the entries of the IP prefix list are in the **deny** mode, all routing information will be denied by the filter. In this case, you are recommended to define an entry in the **permit** mode with the **ip ip-prefix** *ip-prefix-name* **index** *index-number* **permit** 0.0.0.0 0 **less-equal** 32 command following multiple entries in the **deny** mode to permit all the other IP routes.

Displaying IP Route Policy

To do...	Use the command...	Remarks
Display route policy information	display route-policy [<i>route-policy-name</i>]	Available in any view
Display IP-prefix information	display ip ip-prefix [<i>ip-prefix-name</i>]	

IP Route Policy Configuration Example

Configuring to Filter Received Routing Information

Network requirements

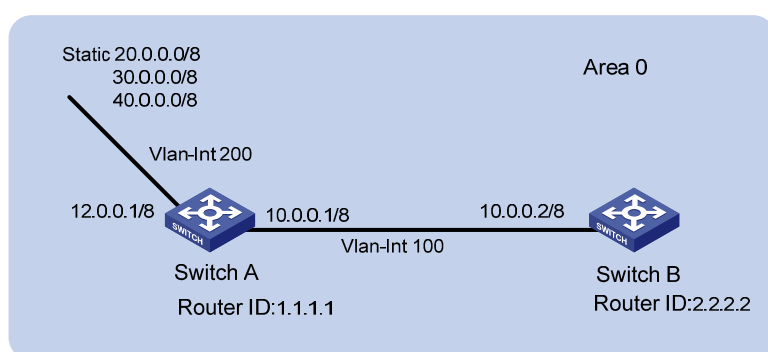
Switch A communicates with Switch B. OSPF protocol is enabled on both switches. The router ID of Switch A is 1.1.1.1 and that of Switch B is 2.2.2.2.

Configure three static routes and enable OSPF on Switch A.

By configuring route filtering rules on Switch A 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.

Network diagram

Figure 5-1 Filter received routing information



Configuration procedure

- Configure Switch A:

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 20.0.0.0 255.0.0.0 12.0.0.2
[SwitchA] ip route-static 30.0.0.0 255.0.0.0 12.0.0.2
[SwitchA] ip route-static 40.0.0.0 255.0.0.0 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 Switch B:

```
# 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 Switch B 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

Controlling RIP Packet Cost to Implement Dynamic Route Backup

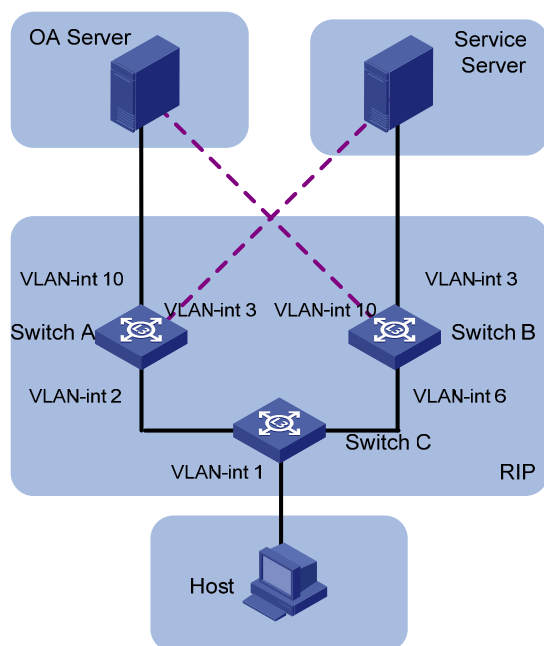
Network requirements

The required speed of convergence in the small network of a company is not high. The network provides two services. Main and backup links are provided for each service for the purpose of reliability. The main link of one service serves as the backup link of the other. The two services are distinguished by IP addresses. If a fault occurs to the main link of one service, dynamic backup can prevent service interruption.

Network diagram

According to the network requirements, the network topology is designed as shown in [Figure 5-2](#).

Figure 5-2 Network diagram



Device	Interface	IP address
Switch A	Vlan-int 2	2.2.2.1/8
	Vlan-int 3	3.3.3.254/8
	Vlan-int 10	1.1.1.254/8
Switch B	Vlan-int 3	3.3.3.253/8
	Vlan-int 6	6.6.6.5/8
	Vlan-int 10	1.1.1.253/8
Switch C	Vlan-int 1	192.168.0.39/24
	Vlan-int 2	2.2.2.2/8
	Vlan-int 6	6.6.6.6/8
OA Server		1.1.1.1/32
Service Server		3.3.3.3/32
Host		192.168.0.9/24

Configuration considerations

- According to the network requirements, select RIP.
- For the OA server, the main link is between Switch A and Switch C, while the backup link is between Switch B and Switch C.
- For the service server, the main link is between Switch B and Switch C, while the backup link is between Switch A and Switch C.

- Apply a route policy to control the cost of routes received by Switch C to provide main and backup links for the services of the OA server and service server.

Configuration procedure

1) Configure Switch A.

Create VLANs and configure IP addresses for the VLAN interfaces. The configuration procedure is omitted.

Configure RIP.

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip] network 1.0.0.0
[SwitchA-rip] network 2.0.0.0
[SwitchA-rip] network 3.0.0.0
```

2) Configure Switch B.

Create VLANs and configure IP addresses for the VLAN interfaces. The configuration procedure is omitted.

Configure RIP.

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip] network 1.0.0.0
[SwitchB-rip] network 3.0.0.0
[SwitchB-rip] network 6.0.0.0
```

3) Configure Switch C.

Create VLANs and configure IP addresses for the VLAN interfaces. The configuration procedure is omitted.

Define IP-prefix 1 containing the IP address prefix 1.0.0.0/8, and IP-prefix 2 containing the IP address prefix 3.0.0.0/8.

```
<SwitchC> system-view
[SwitchC] ip ip-prefix 1 index 10 permit 1.0.0.0 8
[SwitchC] ip ip-prefix 2 index 10 permit 3.0.0.0 8
```

Create a route policy named **in** and node 10 with the matching mode being **permit**. Define if-match clauses. Apply the cost 5 to routes matching the outgoing interface VLAN-interface 2 and prefix list 1.

```
[SwitchC] route-policy in permit node 10
[SwitchC-route-policy] if-match interface Vlan-interface2
[SwitchC-route-policy] if-match ip-prefix 1
[SwitchC-route-policy] apply cost 5
[SwitchC-route-policy] quit
```

Create node 20 with the matching mode being **permit** in the route policy. Define if-match clauses. Apply the cost 6 to routes matching the outgoing interface VLAN-interface 2 and prefix list 2.

```
[SwitchC] route-policy in permit node 20
[SwitchC-route-policy] if-match interface Vlan-interface2
[SwitchC-route-policy] if-match ip-prefix 2
[SwitchC-route-policy] apply cost 6
[SwitchC-route-policy] quit
```

Create node 30 with the matching mode being **permit** in the route policy. Define if-match clauses. Apply the cost 6 to routes matching the outgoing interface VLAN-interface 6 and prefix list 1.

```
[SwitchC] route-policy in permit node 30
[SwitchC-route-policy] if-match interface Vlan-interface6
[SwitchC-route-policy] if-match ip-prefix 1
[SwitchC-route-policy] apply cost 6
[SwitchC-route-policy] quit
```

Create node 40 with the matching mode being **permit** in the route policy. Define if-match clauses. Apply the cost 5 to routes matching the outgoing interface VLAN-interface 6 and prefix list 2.

```
[SwitchC] route-policy in permit node 40
[SwitchC-route-policy] if-match interface Vlan-interface6
[SwitchC-route-policy] if-match ip-prefix 2
[SwitchC-route-policy] apply cost 5
[SwitchC-route-policy] quit
```

Create node 50 with the matching mode being **permit**, to allow all routing information to pass.

```
[SwitchC] route-policy in permit node 50
[SwitchC-route-policy] quit
```

Configure RIP and apply the route policy **in** to the incoming routing information.

```
[SwitchC] rip
[SwitchC-rip] network 1.0.0.0
[SwitchC-rip] network 3.0.0.0
[SwitchC-rip] network 6.0.0.0
[SwitchC-rip] filter-policy route-policy in import
```

Configuration verification

- 1) Display data forwarding paths when the main link of the OA server between Switch A and Switch C works normally.

```
<SwitchC> display ip routing-table
```

```
Routing Table: public net
```

Destination/Mask	Protocol	Pre	Cost	Nexthop	Interface
1.0.0.0/8	RIP	100	5	2.2.2.1	Vlan-interface2
2.0.0.0/8	DIRECT	0	0	2.2.2.2	Vlan-interface2
2.2.2.2/32	DIRECT	0	0	127.0.0.1	InLoopBack0
3.0.0.0/8	RIP	100	5	6.6.6.5	Vlan-interface6
6.0.0.0/8	DIRECT	0	0	6.6.6.6	Vlan-interface6
6.6.6.6/32	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.0/8	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
192.168.0.0/24	DIRECT	0	0	192.168.0.39	Vlan-interface1
192.168.0.39/32	DIRECT	0	0	127.0.0.1	InLoopBack0

- 2) Display data forwarding paths when the main link of the OA server between Switch A and Switch C is down.

```
<SwitchC> display ip routing-table
```

```
Routing Table: public net
```

Destination/Mask	Protocol	Pre	Cost	Nexthop	Interface
1.0.0.0/8	RIP	100	6	6.6.6.5	Vlan-interface2

3.0.0.0/8	RIP	100	5	6.6.6.5	Vlan-interface6
6.0.0.0/8	DIRECT	0	0	6.6.6.6	Vlan-interface6
6.6.6.6/32	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.0/8	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
192.168.0.0/24	DIRECT	0	0	192.168.0.39	Vlan-interface1
192.168.0.39/32	DIRECT	0	0	127.0.0.1	InLoopBack0

Precautions

- 1) When you configure the **apply cost** command in a route policy:
 - The new cost should be greater than the original one to prevent RIP from generating routing loop in the case that a loop exists in the topology.
 - The cost will become 16 if you try to set it to a value greater than 16.
 - The cost will become the original one if you try to set it to 0.
 - The cost will still be 16 if you try to set it to 16.
- 2) Using the **if-match interface** command will match the routes whose outgoing interface to the next hop is the specified interface.
- 3) You are recommended to configure a node to match all routes not passing the preceding nodes in a route policy.
- 4) If the cost of a received RIP route is equal to 16, the cost specified by the **apply cost** command in a route policy will not be applied to the route, that is, the cost of the route is equal to 16.
- 5) Using the **filter-policy** command does not filter redistributed routes.

Troubleshooting IP Route Policy

Symptom

The route policy cannot filter routing information correctly when the routing protocol runs normally.

Analysis

The route policy cannot filter routing information correctly in the following two cases:

- All nodes in the route policy are in the **deny** mode.
- All entries in the IP-prefix list are in the **deny** mode.

Solution

- 1) Use the **display ip ip-prefix** command to display the configuration of the IP-prefix list.
- 2) Use the **display route-policy** command to display the configuration of the route policy.

6 Route Capacity Configuration

When configuring route capacity, go to these sections for information you are interested in:

- [Route Capacity Configuration Overview](#)
- [Route Capacity Limitation Configuration](#)
- [Displaying and Maintaining Route Capacity Limitation Configuration](#)



Note

- The term **router** in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.
 - The S3600-SI series do not support route capacity configuration.
-

Route Capacity Configuration Overview

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 switches 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

Normally, the default configuration of the system can meet the requirements. To avoid decreasing system stability and availability due to improper configuration, it is not recommended to modify the configuration.

Route Capacity Limitation

Huge routing tables are usually caused by OSPF route entries. Therefore, the route capacity limitation of a switch applies only to OSPF routes, instead of static routes and RIP routes. The route capacity limitation is implemented by controlling the size of the free memory of the switch.

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.

Route Capacity Limitation Configuration

Route capacity limitation configuration includes:

- Configuring the lower limit and the safety value of switch memory,
- Enabling/disabling the switch to recover the disconnected routing protocol automatically.

Configuring the Lower Limit and the Safety Value of the Switch Memory

Follow these steps to set the lower limit and the safety value of switch memory:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the lower limit and the safety value of switch memory	memory { <i>safety</i> <i>safety-value</i> <i>limit</i> <i>limit-value</i> }*	Optional By default • <i>safety-value</i> is 5 • <i>limit-value</i> is 4



Note

The *safety-value* must be greater than the lower *limit-value*.

Enabling/Disabling Automatic Protocol Recovery

Follow these steps to enable automatic protocol recovery:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable automatic protocol recovery	memory auto-establish enable	Optional Enabled by default

Follow these steps to disable automatic protocol recovery:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Disable automatic protocol recovery	memory auto-establish disable	Optional Enabled by default.



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.

Displaying and Maintaining Route Capacity Limitation Configuration

Follow these steps to display route capacity configuration:

To do...	Use the command...	Remarks
Display memory occupancy of a switch	display memory [unit <i>unit-id</i>]	Available in any view
Display the route capacity related memory setting and state information	display memory limit	

Table of Contents

1 Multicast Overview	1-1
Multicast Overview	1-1
Information Transmission in the Unicast Mode	1-1
Information Transmission in the Broadcast Mode	1-2
Information Transmission in the Multicast Mode	1-3
Roles in Multicast	1-4
Common Notations in Multicast	1-5
Advantages and Applications of Multicast	1-5
Multicast Models	1-6
Multicast Architecture	1-6
Multicast Address	1-7
Multicast Protocols	1-9
Multicast Packet Forwarding Mechanism	1-11
Implementation of the RPF Mechanism	1-12
RPF Check	1-12
2 Common Multicast Configuration	2-1
Common Multicast Configuration	2-1
Enabling Multicast Packet Buffering	2-1
Enabling Multicast Routing	2-2
Configuring Limit on the Number of Route Entries	2-2
Configuring Suppression on the Multicast Source Port	2-3
Clearing Multicast Forwarding and Routing Entries	2-3
Configuring a Multicast MAC Address Entry	2-4
Configuring Dropping Unknown Multicast Packets	2-5
Tracing a Multicast Path	2-5
Displaying and Maintaining Common Multicast Configuration	2-5
3 IGMP Configuration	3-1
IGMP Overview	3-1
IGMP Versions	3-1
Work Mechanism of IGMPv1	3-1
Enhancements Provided by IGMPv2	3-3
Enhancements Provided by IGMPv3	3-3
IGMP Proxy	3-5
Configuring IGMP	3-6
IGMP Configuration Task List	3-6
Enabling IGMP	3-6
Configuring IGMP Version	3-7
Configuring Options Related to IGMP Query Messages	3-7
Configuring the Maximum Allowed Number of Multicast Groups	3-9
Configuring a Multicast Group Filter	3-9
Configuring Simulated Joining	3-10
Configuring IGMP Proxy	3-11
Removing Joined IGMP Groups from an Interface	3-12

Displaying and Maintaining IGMP	3-12
4 PIM Configuration	4-1
PIM Overview	4-1
Introduction to PIM-DM	4-2
How PIM-DM Works	4-2
Introduction to PIM-SM	4-4
How PIM-SM Works	4-5
Configuring PIM-DM	4-10
Enabling PIM-DM	4-10
Configuring PIM-SM	4-10
Enabling PIM-SM	4-10
Configuring an RP	4-11
Configuring a BSR	4-12
Filtering the Registration Packets from DR to RP	4-14
Disabling RPT-to-SPT Switchover	4-14
Configuring Common PIM Parameters	4-15
Configuring a Multicast Data Filter	4-15
Configuring the Hello Interval	4-16
Configuring PIM Neighbors	4-16
Configuring Multicast Source Lifetime	4-17
Configuring PIM Prune Delay	4-17
Clearing the Related PIM Entries	4-18
Displaying and Maintaining PIM	4-18
PIM Configuration Examples	4-19
PIM-DM Configuration Example	4-19
PIM-SM Configuration Example	4-22
Troubleshooting PIM	4-26
5 MSDP Configuration	5-1
MSDP Overview	5-1
Introduction to MSDP	5-1
How MSDP Works	5-2
Protocols and Standards	5-7
Configuring MSDP Basic Functions	5-7
Configuration Prerequisites	5-8
Configuring MSDP Basic Functions	5-8
Configuring Connection Between MSDP Peers	5-8
Configuration Prerequisites	5-9
Configuring Description Information for MSDP Peers	5-9
Configuring an MSDP Mesh Group	5-9
Configuring MSDP Peer Connection Control	5-10
Configuring SA Message Transmission	5-10
Configuration Prerequisites	5-11
Configuring RP Address in SA Messages	5-11
Configuring SA Message Cache	5-12
Configuring the Transmission and Filtering of SA Request Messages	5-12
Configuring a Rule for Filtering the Multicast Sources of SA Messages	5-13
Configuring a Rule for Filtering Received and Forwarded SA Messages	5-13

Displaying and Maintaining MSDP	5-14
MSDP Configuration Example	5-15
Anycast RP Configuration	5-15
Troubleshooting MSDP Configuration	5-18
MSDP Peer Always in the Down State	5-18
No SA Entry in the SA Cache of the Router	5-18
6 IGMP Snooping Configuration	6-1
IGMP Snooping Overview	6-1
Principle of IGMP Snooping	6-1
Basic Concepts in IGMP Snooping	6-2
Work Mechanism of IGMP Snooping	6-3
Configuring IGMP Snooping	6-5
Enabling IGMP Snooping	6-5
Configuring the Version of IGMP Snooping	6-6
Configuring Timers	6-6
Configuring Fast Leave Processing	6-7
Configuring a Multicast Group Filter	6-8
Configuring the Maximum Number of Multicast Groups on a Port	6-9
Configuring IGMP Snooping Querier	6-10
Suppressing Flooding of Unknown Multicast Traffic in a VLAN	6-11
Configuring Static Member Port for a Multicast Group	6-11
Configuring a Static Router Port	6-12
Disabling a Port from Becoming a Router Port	6-13
Configuring a Port as a Simulated Group Member	6-13
Configuring a VLAN Tag for Query Messages	6-14
Configuring Multicast VLAN	6-15
Displaying and Maintaining IGMP Snooping	6-16
IGMP Snooping Configuration Examples	6-17
Configuring IGMP Snooping	6-17
Configuring Multicast VLAN	6-19
Troubleshooting IGMP Snooping	6-21

1 Multicast Overview



Note

In this manual, the term “router” refers to a router in the generic sense or a Layer 3 Ethernet switch running an IP multicast protocol.

The following features are added in this version:

- [Configuring PIM Prune Delay](#)
 - [Configuring the source address to be carried in IGMP queries](#)
 - [Disabling a Port from Becoming a Router Port](#)
-

Multicast Overview

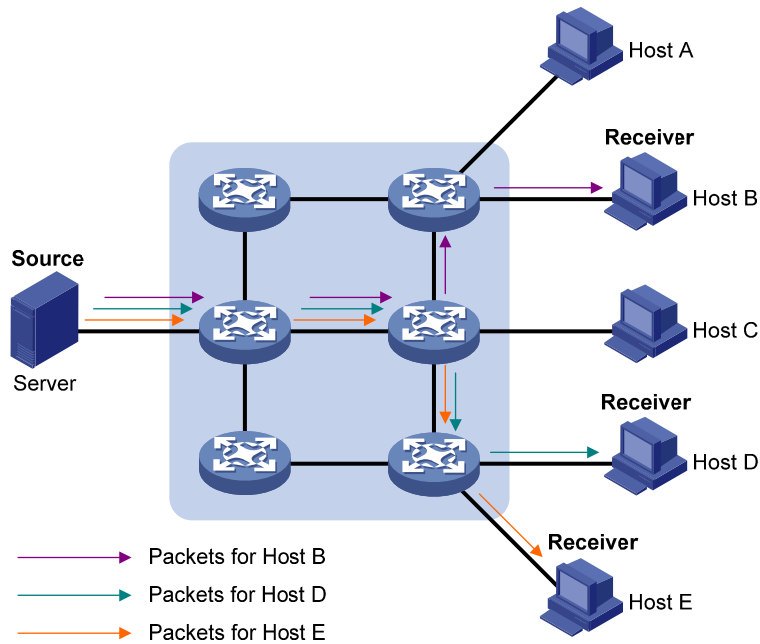
With the development of the Internet, more and more interaction services such as data, voice, and video services are running on the network. In addition, highly bandwidth- and time-critical services, such as e-commerce, Web conferencing, online auctions, video on demand (VoD), and tele-education have 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 for unicast, broadcast, and multicast traffic.

Information Transmission in the Unicast Mode

In unicast, the system establishes a separate data transmission channel for each user requiring this information, and sends a separate copy of the information to the user, as shown in [Figure 1-1](#):

Figure 1-1 Information transmission in the unicast mode

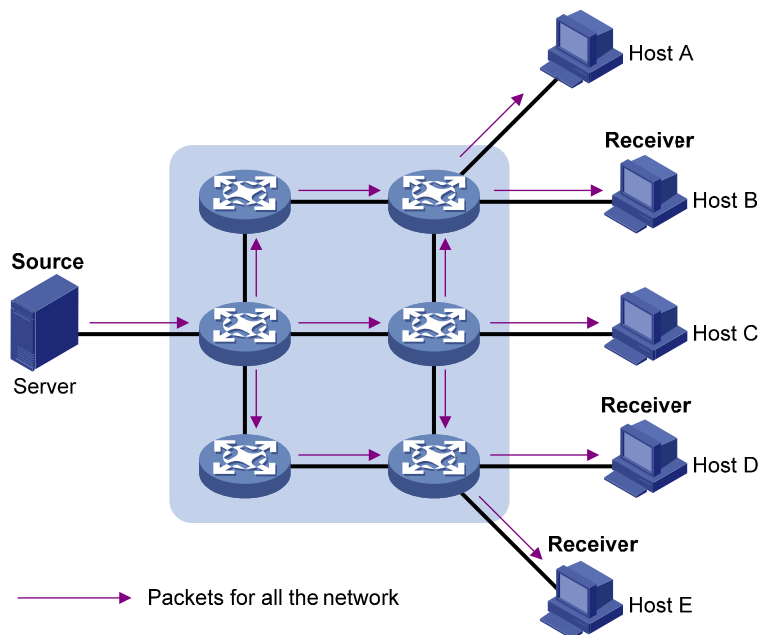


Assume that Hosts B, D and E need this information. The source server establishes transmission channels for the devices of these users respectively. As the transmitted traffic over the network is in direct proportion to the number of users that receive this information, when a large number of users need the same information, the server must send many packets of information with the same content to the users. While suitable for networks with small numbers of users, or where information transmitted to users is significantly different, in other cases this is an inefficient use of the network, and when there is limited bandwidth, bottlenecks can develop in information transmission. In general, unicast is not good for the transmission of a great deal of the same information to multiple recipients.

Information Transmission in the Broadcast Mode

When you broadcast traffic, the system transmits information to all users on a network. Any user on the network can receive the information, no matter if 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 Hosts B, D, and E need the information. The source server broadcasts this information through the routers, reaching the targets, but also Hosts A and C on the network receive this information.

This is an efficient way to send the same content to densely distributed users. However, as we can see from the information transmission process, security and restricted use of paid services 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.

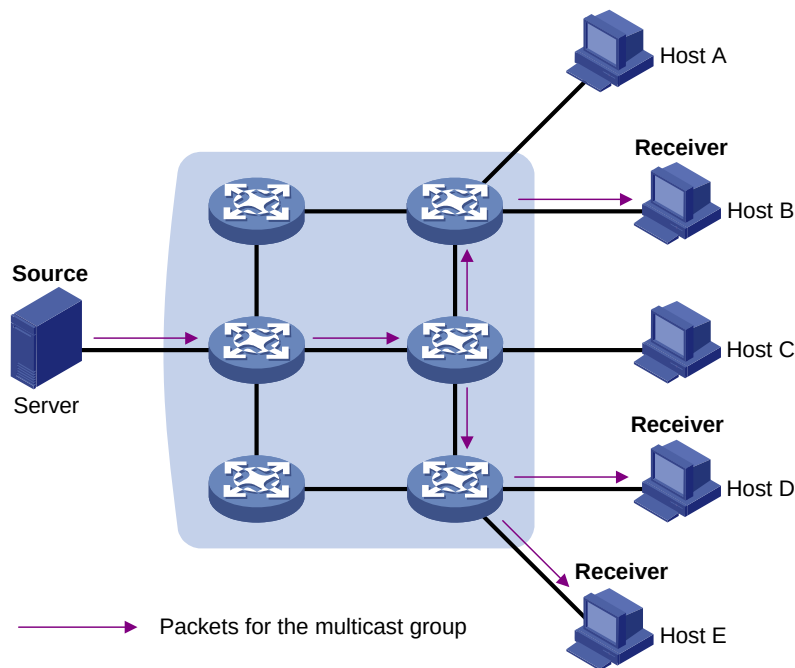
Therefore, broadcast is disadvantageous in transmitting data to specific users, and is more bandwidth intensive.

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 are not efficient.

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 multicast distribution trees established for multicast data packets through multicast routing protocols, 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 Hosts B, D and E need the information. To transmit the information to the right users, it is necessary to group Hosts 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 Hosts 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.

Roles in Multicast

The following roles are involved in multicast transmission:

- An information sender is referred to as a multicast source ("Source" in [Figure 1-3](#)).
- Each receiver is a multicast group member ("Receiver" in [Figure 1-3](#)).
- All receivers interested in the same information form a multicast group. Multicast groups are not subject to geographic restrictions.
- A router that supports Layer 3 multicast is called multicast router or Layer 3 multicast device. In addition to providing multicast routing, a multicast router can also manage multicast group members.

For a better understanding of the multicast concept, you can use the analogy of a transmission of TV programs, as shown in [Table 1-1](#).

Table 1-1 An analogy between TV transmission and multicast transmission

Step	TV transmission	Multicast transmission
1	A TV station transmits a TV program through a television channel.	A multicast source sends multicast data to a multicast group.
2	A user tunes the TV set to the channel.	A receiver joins the multicast group.
3	The user starts to watch the TV program transmitted by the TV station via the channel.	The receiver starts to receive the multicast data that the source sends to the multicast group.
4	The user turns off the TV set.	The receiver leaves the multicast group.



Note

- A multicast source does not necessarily belong to a multicast group. Namely, a multicast source is not necessarily a multicast data receiver.
- A multicast source can send data to multiple multicast groups at the same time, and multiple multicast sources can send data to the same multicast group at the same time.

Common Notations in Multicast

Two notations are commonly used in multicast:

- (*, G): Indicates a rendezvous point tree (RPT), or a multicast packet that any multicast source sends to multicast group G. Here “*” represents any multicast source, while “G” represents a specific multicast group.
- (S, G): Indicates a shortest path tree (SPT), or a multicast packet that multicast source S sends to multicast group G. Here “S” represents a specific multicast source, while “G” represents a specific multicast group.



Note

For details about the concepts RPT and SPT, see [“PIM Configuration”](#).

Advantages and Applications of Multicast

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.

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 supports 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.

Multicast Models

Based on the multicast source processing modes, there are three multicast models:

- Any-source multicast (ASM)
- Source-filtered multicast (SFM)
- Source-specific multicast (SSM)

ASM model

In the ASM model, any sender can become a multicast source and send information to a multicast group; numbers of receivers can join a multicast group identified by a group address and obtain multicast information addressed to that multicast group. In this model, receivers are not aware of the position of a multicast source in advance. However, they can join or leave the multicast group at any time.

SFM model

The SFM model is derived from the ASM model. From the view of a sender, the two models have the same multicast group membership architecture.

Functionally, the SFM model is an extension of the ASM model. In the SFM model, the upper layer software checks the source address of received multicast packets so as to permit or deny multicast traffic from specific sources. Therefore, receivers can receive the multicast data from only part of the multicast sources. From the view of a receiver, multicast sources are not all valid: they are filtered.

SSM model

In the practical life, users may be interested in the multicast data from only certain multicast sources. The SSM model provides a transmission service that allows users to specify the multicast sources they are interested in at the client side.

The radical difference between the SSM model and the ASM model is that in the SSM model, receivers already know the locations of the multicast sources by some means. In addition, the SSM model uses a multicast address range that is different from that of the ASM model, and dedicated multicast forwarding paths are established between receivers and the specified multicast sources.

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 transport 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:

- 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 using the membership registration mechanism.
- Multicast routing: A router or switch transports packets from a multicast source to receivers by building a multicast distribution tree with multicast routes.
- 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.

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?

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:

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, there are a group of destination addresses (called group address), rather than one address. 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 1-2](#).

Table 1-2 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	Administratively scoped 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 1-3 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)
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

Class D address range	Description
224.0.0.18	Virtual Router Redundancy Protocol (VRRP)
224.0.0.19 to 224.0.0.255	Other protocols



Note

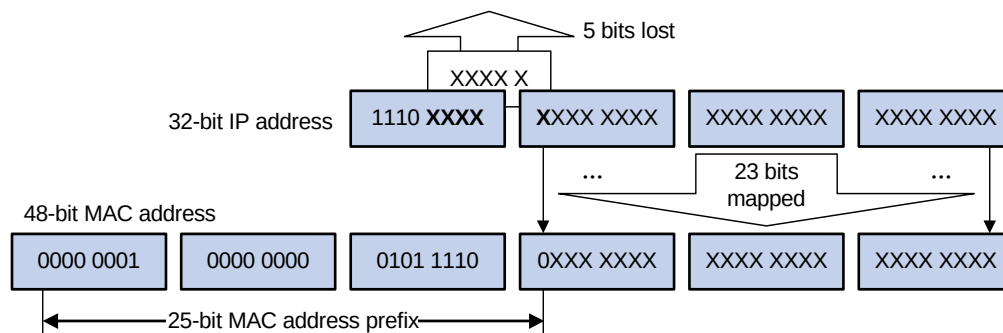
Like having reserved the private network segment 10.0.0.0/8 for unicast, IANA has also reserved the network segment 239.0.0.0/8 for multicast. These are administratively scoped addresses. With the administratively scoped addresses, you can define the range of multicast domains flexibly to isolate IP addresses between different multicast domains, so that the same multicast address can be used in different multicast domains without causing collisions.

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 1-4](#) describes the mapping relationship:

Figure 1-4 Multicast address mapping



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.

Multicast Protocols

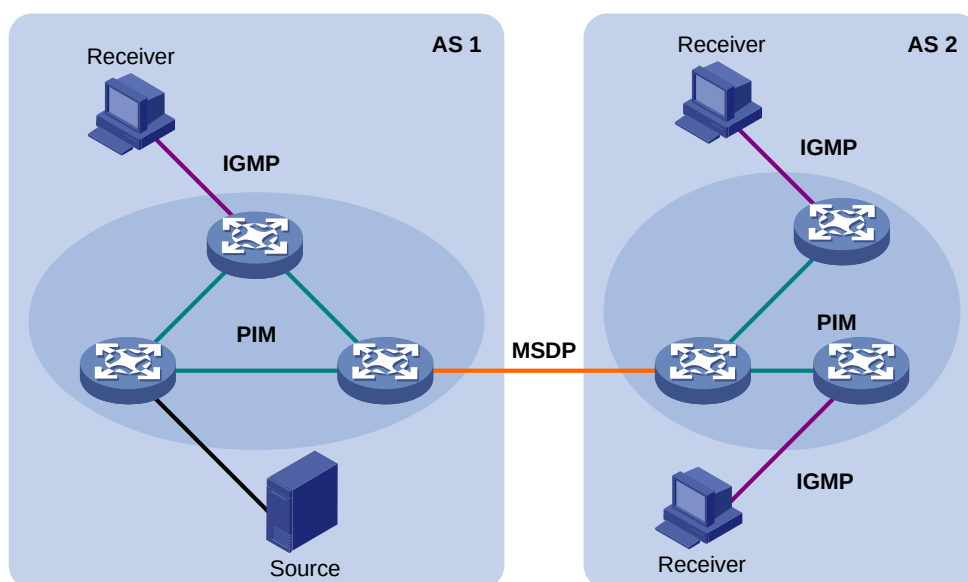
Note

- Generally, we refer to IP multicast working at the network layer as Layer 3 multicast and the corresponding multicast protocols as Layer 3 multicast protocols, which include IGMP, PIM, and MSDP; we refer to IP multicast working at the data link layer as Layer 2 multicast and the corresponding multicast protocols as Layer 2 multicast protocols, which include IGMP Snooping.
 - This section provides only general descriptions about applications and functions of the Layer 2 and Layer 3 multicast protocols in a network. For details about these protocols, refer to the related chapters of this manual.
-

Layer 3 multicast protocols

Layer 3 multicast protocols include multicast group management protocols and multicast routing protocols. [Figure 1-5](#) describes where these multicast protocols are in a network.

Figure 1-5 Positions of Layer 3 multicast protocols



2) Multicast management protocols

Typically, the Internet Group Management Protocol (IGMP) is used between hosts and Layer 3 multicast devices directly connected with the hosts. These protocols define the mechanism of establishing and maintaining group memberships between hosts and Layer 3 multicast devices.

3) Multicast routing protocols

A multicast routing protocol runs on Layer 3 multicast devices to establish and maintain multicast routes and forward multicast packets correctly and efficiently. Multicast routes constitute a loop-free data transmission path from a data source to multiple receivers, namely a multicast distribution tree.

In the ASM model, multicast routes come in intra-domain routes and inter-domain routes.

- An intra-domain multicast routing protocol is used to discover multicast sources and build multicast distribution trees within an autonomous system (AS) so as to deliver multicast data to receivers. Among a variety of mature intra-domain multicast routing protocols, Protocol Independent Multicast (PIM) is a popular one. Based on the forwarding mechanism, PIM comes in two modes – dense mode (often referred to as PIM-DM) and sparse mode (often referred to as PIM-SM).

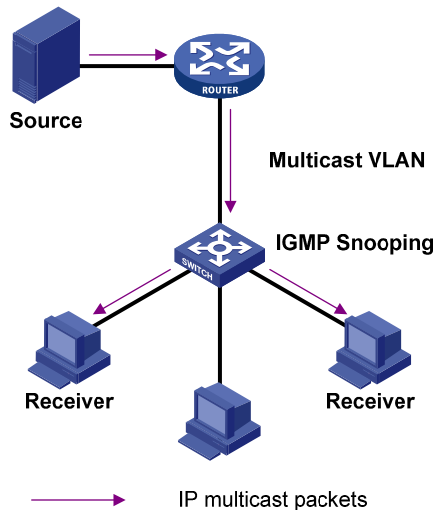
- An inter-domain multicast routing protocol is used for delivery of multicast information between two ASs. So far, mature solutions include Multicast Source Discovery Protocol (MSDP).

For the SSM model, multicast routes are not divided into inter-domain routes and intra-domain routes. Since receivers know the position of the multicast source, channels established through PIM-SM are sufficient for multicast information transport.

Layer 2 multicast protocols

Layer 2 multicast protocols include IGMP Snooping and multicast VLAN. [Figure 1-6](#) shows where these protocols are in the network.

Figure 1-6 Positions of Layer 2 multicast protocols



1) IGMP Snooping

Running on Layer 2 devices, Internet Group Management Protocol Snooping (IGMP Snooping) are multicast constraining mechanisms that manage and control multicast groups by listening to and analyzing IGMP messages exchanged between the hosts and Layer 3 multicast devices, thus effectively controlling and limiting the flooding of multicast data in a Layer 2 network.

2) Multicast VLAN

In the traditional multicast-on-demand mode, when users in different VLANs on a Layer 2 device need multicast information, the upstream Layer 3 device needs to forward a separate copy of the multicast data to each VLAN of the Layer 2 device. With the multicast VLAN feature enabled on the Layer 2 device, the Layer 3 multicast device needs to send only one copy of multicast to the multicast VLAN on the Layer 2 device. This avoids waste of network bandwidth and extra burden on the Layer 3 device.

Multicast Packet Forwarding Mechanism

In a multicast model, a multicast source sends information to the host group identified by the multicast group address in the destination address field of the IP packets. Therefore, to deliver multicast packets to receivers located in different parts of the network, multicast routers on the forwarding path usually need to forward multicast packets received on one incoming interface to multiple outgoing interfaces. Compared with a unicast model, a multicast model is more complex in the following aspects.

- In the network, multicast packet transmission is based on the guidance of the multicast forwarding table derived from the unicast routing table or the multicast routing table specially provided for multicast.
- To process the same multicast information from different peers received on different interfaces of the same device, every multicast packet is subject to a Reverse Path Forwarding (RPF) check on the incoming interface. The result of the RPF check determines whether the packet will be forwarded or discarded. The RPF check mechanism is the basis for most multicast routing protocols to implement multicast forwarding.

The RPF mechanism enables multicast devices to forward multicast packets correctly based on the multicast route configuration. In addition, the RPF mechanism also helps avoid data loops caused by various reasons.

Implementation of the RPF Mechanism

Upon receiving a multicast packet that a multicast source S sends to a multicast group G, the multicast device first searches its multicast forwarding table:

- 1) If the corresponding (S, G) entry exists, and the interface on which the packet actually arrived is the incoming interface in the multicast forwarding table, the router forwards the packet to all the outgoing interfaces.
- 2) If the corresponding (S, G) entry exists, but the interface on which the packet actually arrived is not the incoming interface in the multicast forwarding table, the multicast packet is subject to an RPF check.
 - If the result of the RPF check shows that the RPF interface is the incoming interface of the existing (S, G) entry, this means that the (S, G) entry is correct but the packet arrived from a wrong path and is to be discarded.
 - If the result of the RPF check shows that the RPF interface is not the incoming interface of the existing (S, G) entry, this means that the (S, G) entry is no longer valid. The router replaces the incoming interface of the (S, G) entry with the interface on which the packet actually arrived and forwards the packet to all the outgoing interfaces.
- 3) If no corresponding (S, G) entry exists in the multicast forwarding table, the packet is also subject to an RPF check. The router creates an (S, G) entry based on the relevant routing information and using the RPF interface as the incoming interface, and installs the entry into the multicast forwarding table.
 - If the interface on which the packet actually arrived is the RPF interface, the RPF check is successful and the router forwards the packet to all the outgoing interfaces.
 - If the interface on which the packet actually arrived is not the RPF interface, the RPF check fails and the router discards the packet.

RPF Check

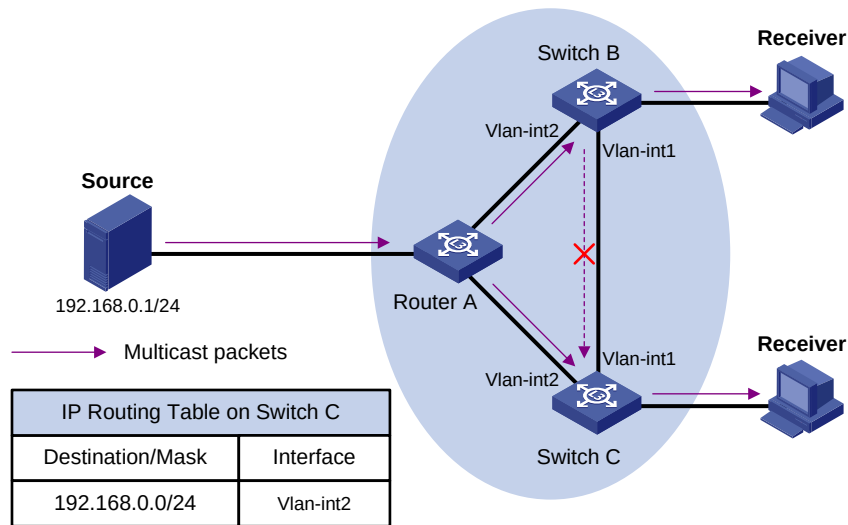
The basis for an RPF check is a unicast route. A unicast routing table contains the shortest path to each destination subnet. A multicast routing protocol does not independently maintain any type of unicast route; instead, it relies on the existing unicast routing information in creating multicast routing entries.

When performing an RPF check, a router searches its unicast routing table. The specific process is as follows: The router automatically chooses an optimal unicast route by searching its unicast routing table, using the IP address of the “packet source” as the destination address. The outgoing interface in the corresponding routing entry is the RPF interface and the next hop is the RPF neighbor. The router

considers the path along which the packet from the RPF neighbor arrived on the RPF interface to be the shortest path that leads back to the source.

Assume that unicast routes exist in the network, as shown in [Figure 1-7](#). Multicast packets travel along the SPT from the multicast source to the receivers.

Figure 1-7 RPF check process



- A multicast packet from Source arrives to VLAN-interface 1 of Switch C, and the corresponding forwarding entry does not exist in the multicast forwarding table of Switch C. Switch C performs an RPF check, and finds in its unicast routing table that the outgoing interface to 192.168.0.0/24 is VLAN-interface 2. This means that the interface on which the packet actually arrived is not the RPF interface. The RPF check fails and the packet is discarded.
- A multicast packet from Source arrives to VLAN-interface 2 of Switch C, and the corresponding forwarding entry does not exist in the multicast forwarding table of Switch C. The router performs an RPF check, and finds in its unicast routing table that the outgoing interface to 192.168.0.0/24 is the interface on which the packet actually arrived. The RPF check succeeds and the packet is forwarded.

2 Common Multicast Configuration



Note

- In this manual, the term “router” refers to a router in the generic sense or a Layer 3 Ethernet switch running an IP multicast protocol.
- S3600-SI series Ethernet switches support only [Configuring Suppression on the Multicast Source Port](#), [Configuring a Multicast MAC Address Entry](#), and [Configuring Dropping Unknown Multicast Packets](#), while S3600-EI series Ethernet switches support all multicast features.

Common Multicast Configuration

Table 2-1 Complete the following tasks to perform common multicast configurations:

Task	Remarks
Enabling Multicast Packet Buffering	Optional
Enabling Multicast Routing	Required
Configuring Limit on the Number of Route Entries	Optional
Configuring Suppression on the Multicast Source Port	Optional
Clearing Multicast Forwarding and Routing Entries	Optional
Configuring a Multicast MAC Address Entry	Optional
Configuring Dropping Unknown Multicast Packets	Optional
Tracing a Multicast Path	Optional

Enabling Multicast Packet Buffering

With the multicast packet buffering feature enabled, multicast packets delivered to the CPU are buffered while the corresponding multicast forwarding entries are being created and then forwarded out according to the multicast forwarding entries after entry creation.

This mechanism buffers multicast packets at the price of impact to the CPU and extra memory usage.

Follow these steps to enable multicast packet buffering:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable multicast packet buffering	multicast storing-enable	Optional By default, this function is disabled.

To do...	Use the command...	Remarks
Configure the maximum number of packets that can be buffered per multicast forwarding entry	multicast storing-packet <i>packet-number</i>	Optional The system default is 100.



Caution

The multicast packet buffering feature should be enabled before multicast routing is enabled.

Enabling Multicast Routing

Follow these steps to enable multicast routing:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable multicast routing	multicast routing-enable	Required Disabled by default.



Note

To guard against attacks on any socket not in use, S3600 series provide the following functions to achieve enhanced security:

- The system opens the RAW Socket used for multicast routing only if multicast routing is enabled.
- When you disable multicast routing, the RAW Socket used for multicast routing is also closed.



Caution

IGMP, PIM and MSDP configurations can be performed or can take effect only if multicast routing has been enabled.

Configuring Limit on the Number of Route Entries

Multicast routing entries specify the interfaces through which multicast packets are sent to multicast group members. Too many multicast routing entries can exhaust the router's memory and thus result in lower router performance. Therefore, the number of multicast routing entries should be limited.

Follow these steps to configure limit on the number of route entries:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
Configure the maximum number of multicast route entries	multicast route-limit <i>limit</i>	Optional By default, the maximum number of multicast route entries is 256

Configuring Suppression on the Multicast Source Port

Some users may deploy unauthorized multicast servers on the network. This affects the use of network bandwidth and transmission of multicast data of authorized users by taking network resources. You can configure multicast source port suppression on certain ports to prevent unauthorized multicast servers attached to these ports from sending multicast traffic to the network.

Configuring multicast source port suppression in system view

Follow these steps to configure multicast source port suppression in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure multicast source port suppression	multicast-source-deny [interface <i>interface-list</i>]	Optional Multicast source port suppression is disabled by default.

Configuring multicast source port suppression in Ethernet port view

Follow these steps to configure multicast source port suppression in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure multicast source port suppression	multicast-source-deny	Optional Multicast source port suppression is disabled by default.

Clearing Multicast Forwarding and Routing Entries

To release system memory, you can use **reset** commands to clear multicast routing entries, multicast forwarding entries, and related statistics information stored in the device.

Follow these steps to clear the multicast-related entries and statistics:

To do...	Use the command...	Remarks
Clear multicast forwarding entries and, with statistics specified, the corresponding statistics information	reset multicast forwarding-table [statistics] { all { <i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }] <i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }] incoming-interface <i>interface-type</i> <i>interface-number</i> } * }	Use the reset commands in user view.
Clear routing entries in the core multicast routing table	reset multicast routing-table { all { <i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }] <i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }] { incoming-interface <i>interface-type</i> <i>interface-number</i> } } * }	

Configuring a Multicast MAC Address Entry

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 MAC address entry by configuring a multicast MAC address entry manually.

Generally, when receiving a multicast packet for a multicast group not yet registered on the switch, the switch will flood the packet within the VLAN to which the port belongs. You can configure a static multicast MAC address entry to avoid this.

Follow these steps to configure a multicast MAC address entry in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a multicast MAC address entry	mac-address multicast <i>mac-address</i> interface <i>interface-list</i> vlan <i>vlan-id</i>	Required The <i>mac-address</i> argument must be a multicast MAC address.

Follow these steps to configure a multicast MAC address entry in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Create a multicast MAC address entry.	mac-address multicast <i>mac-address</i> vlan <i>vlan-id</i>	Required The <i>mac-address</i> argument must be a multicast MAC address.



Caution

- 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.
- You cannot configure a multicast MAC address starting with 01005e on a device with IRF Fabric enabled.
- 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.
- You cannot configure a multicast MAC address starting with 01005e in an IGMP-Snooping-enabled VLAN. You can do that if IGMP Snooping is not enabled in the VLAN.

Configuring Dropping Unknown Multicast Packets

Generally, if the multicast address of the multicast packet received on the switch is not registered on the local switch, the packet will be flooded in the VLAN which the multicast packet belongs to. When the function of dropping unknown multicast packets is enabled, the switch will drop any multicast packets whose multicast address is not registered. Thus, the bandwidth is saved and the processing efficiency of the system is improved.

Follow these steps to configure dropping unknown multicast packet:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure dropping unknown multicast packets	unknown-multicast drop enable	Required By default, the function of dropping unknown multicast packets is disabled.

Tracing a Multicast Path

You can run the **mtracert** command to trace the path down which the multicast traffic flows from a given first-hop router to the last-hop router.

To do...	Use the command...	Remarks
Trace a multicast path	mtracert <i>source-address</i> [[<i>last-hop-router-address</i>] <i>group-address</i>]	Required Available in any view

Displaying and Maintaining Common Multicast Configuration

The information about the multicast forwarding table is mainly used for debugging. Generally, you can get the required information by checking the core multicast routing table.

Three kinds of tables affect multicast data transmission. Their correlations are as follows:

- Each multicast routing protocol has its own multicast routing table, such as PIM routing table.
- The information of different multicast routing protocols forms a general multicast routing table.
- Consistent with the multicast routing table, the multicast forwarding table is the table that guide multicast forwarding.

Follow these commands to display common multicast configuration:

To do...	Use the command...	Remarks
Display the statistics information about multicast source port suppression	display multicast-source-deny [<i>interface interface-type</i> [<i>interface-number</i>]]	Available in any view
Display the information about the multicast routing table	display multicast routing-table [<i>group-address</i> [mask { <i>mask</i> <i>length</i> }]] <i>source-address</i> [mask { <i>mask</i> <i>length</i> }]] incoming-interface { <i>interface-type interface-number</i> register }]*	Available in any view
Display the information about the multicast forwarding table	display multicast forwarding-table [<i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }]] <i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }]] incoming-interface { <i>interface-type interface-number</i> register }]*	Available in any view
Display multicast forward table information containing port information	display mpm forwarding-table [<i>group-address</i>]	Available in any view
Display the information about the IP multicast groups and MAC multicast groups in a VLAN or all VLANs	display mpm group [<i>vlan vlan-id</i>]	Available in any view
Display the created multicast MAC table entries	display mac-address multicast [static { { { <i>mac-address</i> <i>vlan vlan-id</i> <i>vlan vlan-id</i> } [count] } count }]	Available in any view

3 IGMP Configuration



Note

- In this manual, the term “router” refers to a router in the generic sense or a Layer 3 Ethernet switch running an IP multicast protocol.
 - S3600-SI series Ethernet switches do not support IGMP.
-

When configuring IGMP, go to these sections for information you are interested in:

- [IGMP Overview](#)
- [Configuring IGMP](#)
- [Displaying and Maintaining IGMP](#)

IGMP Overview

As a TCP/IP protocol responsible for IP multicast group member management, the Internet Group Management Protocol (IGMP) is used by IP hosts to establish and maintain their multicast group memberships to immediately neighboring multicast routers.

IGMP Versions

So far, there are three IGMP versions:

- IGMPv1 (documented in RFC 1112)
- IGMPv2 (documented in RFC 2236)
- IGMPv3 (documented in RFC 3376)

All IGMP versions support the any-source multicast (ASM) model. In addition, IGMPv3 provides strong support to the source-specific multicast (SSM) model.

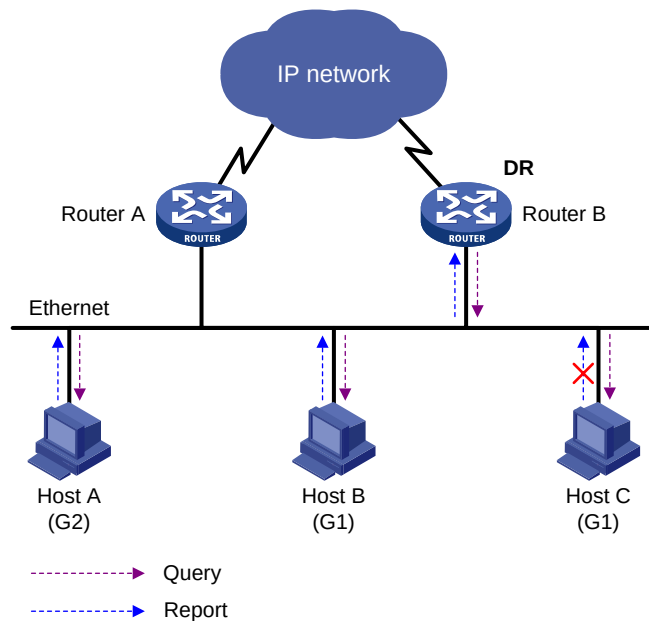
Work Mechanism of IGMPv1

IGMPv1 manages multicast group memberships mainly based on the query and response mechanism. Of multiple multicast routers on the same subnet, all the routers can hear IGMP membership report messages (often referred to as reports) from hosts, but only one router is needed for sending IGMP query messages (often referred to as queries). 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 a multicast routing protocol (such as PIM) serves as the IGMP querier.

For more information about a DR, refer to [DR election](#).

Figure 3-1 Joining multicast groups



Assume that Host B and Host C are expected to receive multicast data addressed to multicast group G1, while Host A is expected to receive multicast data addressed to G2, as shown in [Figure 3-1](#). The basic process that the hosts join the multicast groups is as follows:

- 1) The IGMP querier (Router B in the figure) periodically multicasts IGMP queries (with the destination address of 224.0.0.1) to all hosts and routers on the local subnet.
- 2) Upon receiving a query message, Host B or Host C (the delay timer of whichever expires first) sends an IGMP report to the multicast group address of G1, to announce its interest in G1. Assume it is Host B that sends the report message.
- 3) Host C, which is on the same subnet, hears the report from Host B for joining G1. Upon hearing the report, Host C will suppress itself from sending a report message for the same multicast group, because the IGMP routers (Router A and Router B) already know that at least one host on the local subnet is interested in G1. This mechanism, known as IGMP report suppression, helps reduce traffic over the local subnet.
- 4) At the same time, because Host A is interested in G2, it sends a report to the multicast group address of G2.
- 5) Through the above-mentioned query/report process, the IGMP routers learn that members of G1 and G2 are attached to the local subnet, and generate (*, G1) and (*, G2) multicast forwarding entries, which will be the basis for subsequent multicast forwarding, 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 router forwards the multicast data to the local subnet, and then the receivers on the subnet 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 group, so the routers will delete the multicast forwarding entries corresponding to that multicast group after a period of time.

Enhancements Provided by IGMPv2

Compared with IGMPv1, IGMPv2 provides the querier election mechanism and Leave Group mechanism.

Querier election mechanism

In IGMPv1, the DR elected by the Layer 3 multicast routing protocol (such as PIM) serves as the querier among multiple routers on the same subnet.

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 query messages (often referred to as general queries) to all hosts and routers on the local subnet (the destination address is 224.0.0.1).
- 2) Upon hearing a general query, every IGMPv2 router compares the source IP address of the query message with its own interface address. After comparison, the router with the lowest IP address wins the querier election and all other IGMPv2 routers become non-queriers.
- 3) All the non-queriers start a timer, known as “other querier present timer”. If a router receives an IGMP query from the querier before the timer expires, it resets this timer; otherwise, it assumes the querier to have timed out and initiates a new querier election process.

“Leave group” mechanism

In IGMPv1, when a host leaves a multicast group, it does not send any notification to the multicast router. The multicast router relies on IGMP query response timeout to know whether a group no longer has members. This adds to the leave latency.

In IGMPv2, on the other hand, when a host leaves a multicast group:

- 1) This host sends a Leave Group message (often referred to as leave message) to all routers (the destination address is 224.0.0.2) on the local subnet.
- 2) Upon receiving the leave message, the querier sends a configurable number of group-specific queries to the group being left. The destination address field and group address field of message are both filled with the address of the multicast group being queried.
- 3) One of the remaining members, if any on the subnet, of the group being queried should send a membership report within the maximum response time set in the query messages.
- 4) If the querier receives a membership report for the group within the maximum response time, it will maintain the memberships of the group; otherwise, the querier will assume that no hosts on the subnet are still interested in multicast traffic to that group and will stop maintaining the memberships of the group.

Enhancements Provided by IGMPv3

Built upon and being compatible with IGMPv1 and IGMPv2, IGMPv3 provides hosts with enhanced control capabilities and provides enhancements of query and report messages.

Enhancements in control capability of hosts

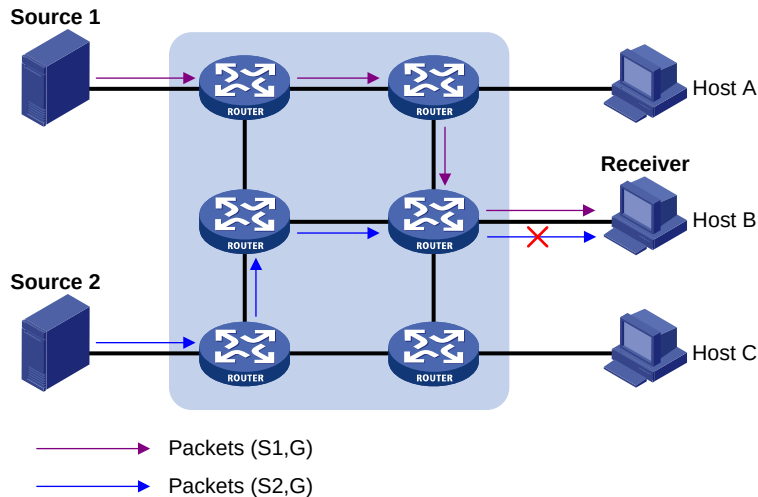
IGMPv3 has introduced source filtering modes (Include and Exclude), so that a host can specify a list of sources it expect or does not expect multicast data from when it joins a multicast group:

- If it expects multicast data from specific sources like S1, S2, ..., it sends a report with the Filter-Mode denoted as “Include Sources (S1, S2, ...)”.

- If it does not expect multicast data from specific sources like S1, S2, ..., it sends a report with the Filter-Mode denoted as “Exclude Sources (S1, S2, ...)”.

As shown in [Figure 3-2](#), the network comprises two multicast sources, Source 1 (S1) and Source 2 (S2), both of which can send multicast data to multicast group G. Host B is interested only in the multicast data that Source 1 sends to G but not in the data from Source 2.

Figure 3-2 Flow paths of source-and-group-specific multicast traffic



In the case of IGMPv1 or IGMPv2, Host B cannot select multicast sources when it joins multicast group G. Therefore, multicast streams from both Source 1 and Source 2 will flow to Host B whether it needs them or not.

When IGMPv3 is running between the hosts and routers, Host B can explicitly express its interest in the multicast data Source 1 sends to multicast group G (denoted as (S1, G)), rather than the multicast data Source 2 sends to multicast group G (denoted as (S2, G)). Thus, only multicast data from Source 1 will be delivered to Host B.

Enhancements in query and report capabilities

1) Query message carrying the source addresses

IGMPv3 supports not only general queries (feature of IGMPv1) and group-specific queries (feature of IGMPv2), but also group-and-source-specific queries.

- A general query does not carry a group address, nor a source address;
- A group-specific query carries a group address, but no source address;
- A group-and-source-specific query carries a group address and one or more source addresses.

2) Reports containing multiple group records

Unlike an IGMPv1 or IGMPv2 report message, an IGMPv3 report message is destined to 224.0.0.22 and contains one or more group records. Each group record contains a multicast group address and a multicast source address list.

Group record types include:

- IS_IN: The source filtering mode is Include, namely, the report sender requests the multicast data from only the sources defined in the specified multicast source list.
- IS_EX: The source filtering mode is Exclude, namely, the report sender requests the multicast data from any sources but those defined in the specified multicast source list.

- TO_IN: The filtering mode has changed from Exclude to Include.
- TO_EX: The filtering mode has changed from Include to Exclude.
- ALLOW: The Source Address fields in this Group Record contain a list of the additional sources that the system wishes to hear from, for packets sent to the specified multicast address. If the change was to an Include source list, these are the addresses that were added to the list; if the change was to an Exclude source list, these are the addresses that were deleted from the list.
- BLOCK: indicates that the Source Address fields in this Group Record contain a list of the sources that the system no longer wishes to hear from, for packets sent to the specified multicast address. If the change was to an Include source list, these are the addresses that were deleted from the list; if the change was to an Exclude source list, these are the addresses that were added to the list.



Note

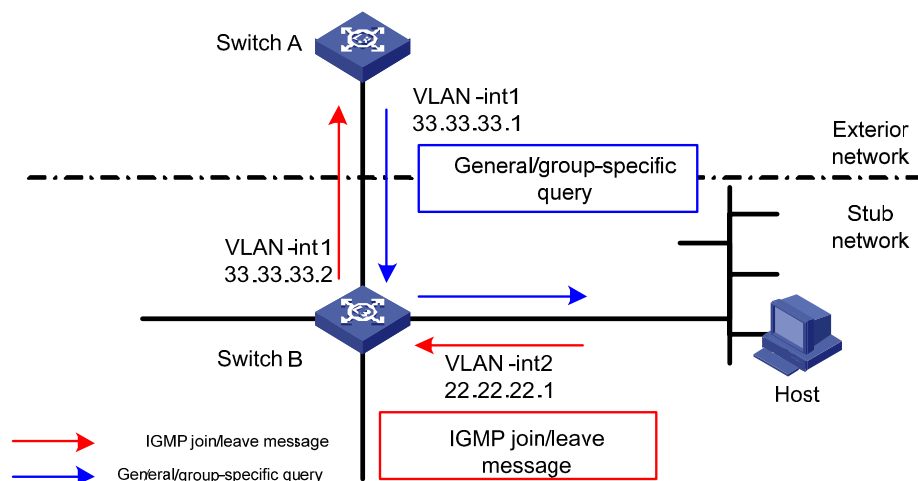
Currently, only the IGMPv1 and IGMPv2 are supported on S3600 series Ethernet switches.

IGMP Proxy

A lot of stub networks (stub 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 stub 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 stub network (Switch B shown in [Figure 3-3](#)). The Layer 3 switch will then forward IGMP join or IGMP leave messages sent by the connected hosts. After IGMP Proxy is configured, the stub switch is no longer a PIM neighbor but a host for the exterior network. The Layer 3 switch receives the multicast data of corresponding groups only when it has directly attached multicast members.

Figure 3-3 Diagram for IGMP proxy



[Figure 3-3](#) shows an IGMP Proxy diagram for a stub network. The upstream interface, VLAN-interface 1 of Switch B is the proxy interface for the downstream interface VLAN-interface 2.

Configure Switch B as follows:

Enable multicast routing, and then enable PIM and IGMP on VLAN-interface 1 and VLAN-interface 2. Run the **igmp proxy** command on VLAN-interface 1 to configure it as the proxy interface for VLAN-interface 2.

Configure Switch A as follows:

- Enable multicast routing, enable IGMP and PIM on VLAN-interface 1.
- 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 the stub network receives from VLAN-interface 2 an IGMP join or IGMP leave message sent by the host, it changes the source address of the IGMP information to the address of VLAN-interface 1, 33.33.33.2, and sends the information to VLAN-interface 1 of Switch A. For Switch A, this works as if there is a host directly connected to VLAN-interface 1.

Similarly, when Switch B receives the IGMP general or group-specific query message from the Layer 3 Switch A, Switch B also changes the source address of the query message to the IP address of VLAN-interface 2, 22.22.22.1, and send the message from VLAN-interface 2.

Configuring IGMP

IGMP Configuration Task List

Complete the following tasks to configure IGMP:

Task	Remarks
Enabling IGMP	Required
Configuring IGMP Version	Optional
Configuring Options Related to IGMP Query Messages	Optional
Configuring the Maximum Allowed Number of Multicast Groups	Optional
Configuring a Multicast Group Filter	Optional
Configuring Simulated Joining	Optional
Configuring IGMP Proxy	Optional
Removing Joined IGMP Groups from an Interface	Optional

Enabling IGMP

First, IGMP must be enabled on the interface on which the multicast group memberships are to be established and maintained.

Follow these steps to enable IGMP:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable IP multicast routing	multicast routing-enable	Required
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable IGMP	igmp enable	Required Disabled by default



Caution

Before performing the following configurations described in this chapter, you must enable multicast routing and enable IGMP on the specific interfaces.

Configuring IGMP Version

Follow these steps to configure IGMP version:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the IGMP version	igmp version { 1 2 }	Optional The system default is IGMP version 2.



Caution

IGMP versions cannot be switched to one another automatically. Therefore, all the interfaces on a subnet must be configured to use the same IGMP version.

Configuring Options Related to IGMP Query Messages

IGMP general query

An IGMP router sends IGMP general query messages to the local subnet periodically, and multicast receiver hosts send IGMP reports in response to IGMP queries. Thus the router learns which multicast groups on the subnet have active members.

IGMP group-specific query

On a multi-access network, the query router (querier for short) maintains group memberships. After the related features are configured, the IGMP querier sends a configurable number of IGMP group-specific queries at a configurable interval when it receives an IGMP leave message 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 message.
- When the IGMP querier receives the message, it sends *robust-value* IGMP group-specific query messages at the interval of *lastmember-queryinterval*.
- If other hosts are interested in the group after receiving the IGMP group-specific query message from the querier, they must send IGMP report messages within the maximum response time specified in the query messages.

- If the IGMP querier receives IGMP report messages 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 report messages from other hosts after the period of *robust-value* x *lastmember-queryinterval*, it considers that the group has no members on the local subnet and removes the forwarding table entry for the group.



Note

You can use the **igmp max-response-time** command to set the maximum response time for general IGMP query messages, while that of an IGMP group-specific query message is determined by *robust-value* x *lastmember-queryinterval*.

The procedure is only fit for the occasion where IGMP queriers run IGMP version 2.

IGMP querier election

On a subnet containing multiple IGMP-enabled interfaces, the one with the lowest IP address becomes the IGMP querier. If non-querier interfaces receive no query message within the period configured in the **igmp timer other-querier-present** command, the current IGMP querier is considered to be down. In this case, a new IGMP querier election process takes place.

The maximum response time of IGMP general query messages

When the host receives a general 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.

Follow these steps to configure options related to IGMP query messages:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the query interval (interval of sending general queries)	igmp timer query <i>seconds</i>	Optional 60 seconds by default.
Configure the interval of sending IGMP group-specific query messages	igmp lastmember-queryinterval <i>seconds</i>	Optional 1 second by default
Configure the number of times of sending IGMP group-specific query messages	igmp robust-count <i>robust-value</i>	Optional 2 by default.
Configure the other querier present timer	igmp timer other-querier-present <i>seconds</i>	Optional The system default is 120 seconds, namely twice the query interval.

To do...	Use the command...	Remarks
Configure the maximum response time of IGMP general queries	igmp max-response-time <i>seconds</i>	Optional 10 seconds by default.

Configuring the Maximum Allowed Number of Multicast Groups

By configuring the maximum number of IGMP multicast groups allowed to be joined on an interface of the switch, you can control the number of programs on demand available for users attached to the interface, thus to control the bandwidth usage on the interface.

Follow these steps to configure the maximum number of multicast groups allowed on an interface:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the maximum number of multicast groups allowed on the interface	igmp group-limit <i>limit</i>	Required The default is 256.



Caution

- After the maximum number of multicast groups is reached, the interface will not join any new multicast group.
- If you configure the maximum number of multicast groups allowed on the interface to 1, a new group registered on the interface supersedes the existing one automatically.
- If the number of existing multicast groups is larger than the configured limit on the number of joined multicast groups on the interface, the device will remove the oldest entries automatically until the number of multicast groups on the interface conforms to the configured limit.

Configuring a Multicast Group Filter

A multicast router determines the group memberships in the specified subnet by analyzing the received IGMP reports. To restrict the hosts on the network attached to an interface from joining certain multicast groups, you can apply an ACL rule on the interface as a group filter that limits the range of multicast groups that the interface serves.

You can:

- Configure the range of multicast groups that the current interface will work for in interface view.
- Configure the range of multicast groups that the interface corresponding to the VLAN where the current port resides will work for in Ethernet port view.

Configuring a multicast group filter in interface view

Follow these steps to configure a multicast group filter in VLAN interface view:

To do...	Use the command...		Remarks
Enter system view	system-view		—
Enter interface view	interface <i>interface-type interface-number</i>		—
Configuring a multicast group filter	In VLAN interface view	igmp group-policy <i>acl-number [1 2 port interface-list]</i>	Optional No multicast group filter is configured by default
	In LoopBack interface view	igmp group-policy <i>acl-number [1 2]</i>	

Configuring a multicast group filter in Ethernet port view

Follow these steps to configure a multicast group filter in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type interface-number</i>	—
Configuring a multicast group filter	igmp group-policy <i>acl-number vlan vlan-id</i>	Optional No multicast group filter is configured by default. The port must belong to the specified VLAN.

Configuring Simulated Joining

Generally, hosts running IGMP respond to the IGMP query messages of the IGMP querier. If hosts fail to respond for some reason, the multicast router may consider that there is no member of the multicast group on the local subnet and remove the corresponding path.

To avoid this situation from happening, you can enable simulated joining on a port of the switch, namely configure the port as a simulated member host for a multicast group. When the port receives IGMP query messages, the simulated member host will respond. As a result, the subnet attached to the Layer 3 interface can continue to receive multicast traffic.

Through this configuration, the following functions can be implemented:

- When an Ethernet port is configured as a simulated member host, the switch sends an IGMP report through this port. Meanwhile, the simulated host sends the same IGMP report to itself and establishes a corresponding IGMP entry based on this report.
- When receiving an IGMP general query, the simulated host responds with an IGMP report. Meanwhile, the simulated host sends the same IGMP report to itself to ensure that the IGMP entry does not age out.
- When the simulated joining function is disabled on an Ethernet port, the simulated host sends an IGMP leave message.

Therefore, to ensure that IGMP entries will not age out, the port must receive IGMP general queries periodically.

Configuring simulated joining in interface view

Follow these steps to configure simulated joining in interface view:

To do...	Use the command...		Remarks
Enter system view	system-view		—
Enter interface view	interface <i>interface-type interface-number</i>		—
Configure one or more ports in the VLAN as simulated member host(s) of the specified multicast group	VLAN interface view	igmp host-join <i>group-address port interface-list</i>	Required Disabled by default
	LoopBack interface view	igmp host-join <i>group-address</i>	

Configuring simulated joining in Ethernet port view

Follow these steps to configure simulated joining in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type interface-number</i>	—
Configure the port in the specified VLAN as a simulated member host of the specified multicast group	igmp host-join <i>group-address</i> vlan <i>vlan-id</i>	Required Disabled by default



Caution

- Before configuring simulated joining, you must enable IGMP in interface view first.
- If you configure simulated joining in Ethernet port view, the Ethernet port must belong to the specified VLAN; otherwise the configuration does not take effect.

Configuring IGMP Proxy

Follow these steps to configure IGMP proxy:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface <i>Vlan-interface interface-number</i>	—
Configure IGMP proxy	igmp proxy <i>Vlan-interface interface-number</i>	Required Disabled by default



Caution

- 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 for two or more interfaces.
- Generally, an interface serving as an IGMP querier cannot act as an IGMP proxy interface. If it is necessary to configure an IGMP querier interface as an IGMP proxy interface, you must configure the port that belongs to the proxy interface and connects to the upstream multicast device as a static router port. For details, see [Configuring a Static Router Port](#).

Removing Joined IGMP Groups from an Interface

You can remove all the joined multicast groups from a particular interface or all interfaces of the switch, or remove a particular multicast group address or group address range from a particular interface or all interfaces.

Follow these steps to remove joined multicast groups from one or all interfaces:

To do...	Use the command...	Remarks
Remove the specified group or all groups from the specified interface or all interfaces	reset igmp group { all interface <i>interface-type</i> <i>interface-number</i> } { all <i>group-address</i> [<i>group-mask</i>] }	This command is available in user view.



Caution

After a multicast group is removed from an interface, the multicast group can join the group again.

Displaying and Maintaining IGMP

To do...	Use the command...	Remarks
Display the membership information of the IGMP multicast group	display igmp group [<i>group-address</i> interface <i>interface-type</i> <i>interface-number</i>]	Available in any view
Display the IGMP configuration and running information of the interface	display igmp interface [<i>interface-type</i> <i>interface-number</i>]	Available in any view

4 PIM Configuration

When configuring PIM, go to these sections for information you are interested in:

- [PIM Overview](#)
- [Configuring PIM-DM](#)
- [Configuring PIM-SM](#)
- [Configuring Common PIM Parameters](#)
- [Displaying and Maintaining PIM](#)
- [PIM Configuration Examples](#)
- [Troubleshooting PIM](#)



Note

- In this manual, the term “router” refers to a router in the generic sense or a Layer 3 Ethernet switch running an IP multicast protocol.
 - S3600-SI series Ethernet switches do not support PIM.
-

PIM Overview

Protocol Independent Multicast (PIM) provides IP multicast forwarding by leveraging static routes or unicast routing tables generated by any unicast routing protocol, such as Routing Information Protocol (RIP), open shortest path first (OSPF), Intermediate System to Intermediate System (IS-IS), or Border Gateway Protocol (BGP). Independent of the unicast routing protocols running on the device, multicast routing can be implemented as long as the corresponding multicast routing entries are created through unicast routes. PIM uses the Reverse Path Forwarding (RPF) mechanism to implement multicast forwarding. When a multicast packet arrives on an interface of the device, it is subject to an RPF check. If the RPF check succeeds, the device creates the corresponding routing entry and forwards the packet; if the RPF check fails, the device discards the packet.

Based on the forwarding mechanism, PIM falls into two modes:

- Protocol Independent Multicast–Dense Mode (PIM-DM), and
- Protocol Independent Multicast–Sparse Mode (PIM-SM).



Note

To facilitate description, a network comprising PIM-capable routers is referred to as a “PIM domain” in this document.

Introduction to PIM-DM

PIM-DM is a type of dense mode multicast protocol. It uses the “push mode” for multicast forwarding, and is suitable for small-sized networks with densely distributed multicast members.

The basic implementation of PIM-DM is as follows:

- PIM-DM assumes that at least one multicast group member exists on each subnet of a network, and therefore multicast data is flooded to all nodes on the network. Then, branches without multicast forwarding are pruned from the forwarding tree, leaving only those branches that contain receivers. This “flood and prune” process takes place periodically, that is, pruned branches resume multicast forwarding when the pruned state times out and then data is re-flooded down these branches, and then are pruned again.
- When a new receiver on a previously pruned branch joins a multicast group, to reduce the join latency, PIM-DM uses a graft mechanism to resume data forwarding to that branch.

Generally speaking, the multicast forwarding path is a source tree, namely a forwarding tree with the multicast source as its “root” and multicast group members as its “leaves”. Because the source tree is the shortest path from the multicast source to the receivers, it is also called shortest path tree (SPT).

How PIM-DM Works

The working mechanism of PIM-DM is summarized as follows:

- Neighbor discovery
- SPT building
- Graft
- Assert

Neighbor discovery

In a PIM domain, a PIM router discovers PIM neighbors, maintains PIM neighboring relationships with other routers, and builds and maintains SPTs by periodically multicasting hello messages to all other PIM routers (224.0.0.13).



Note

Every activated interface on a router sends hello messages periodically, and thus learns the PIM neighboring information pertinent to the interface.

SPT building

The process of building an SPT is the process of “flood and prune”.

- 1) In a PIM-DM domain, when a multicast source S sends multicast data to a multicast group G, the multicast packet is first flooded throughout the domain: The router first performs RPF check on the multicast packet. If the packet passes the RPF check, the router creates an (S, G) entry and forwards the data to all downstream nodes in the network. In the flooding process, an (S, G) entry is created on all the routers in the PIM-DM domain.
- 2) Then, nodes without receivers downstream are pruned: A router having no receivers downstream sends a prune message to the upstream node to “tell” the upstream node to delete the

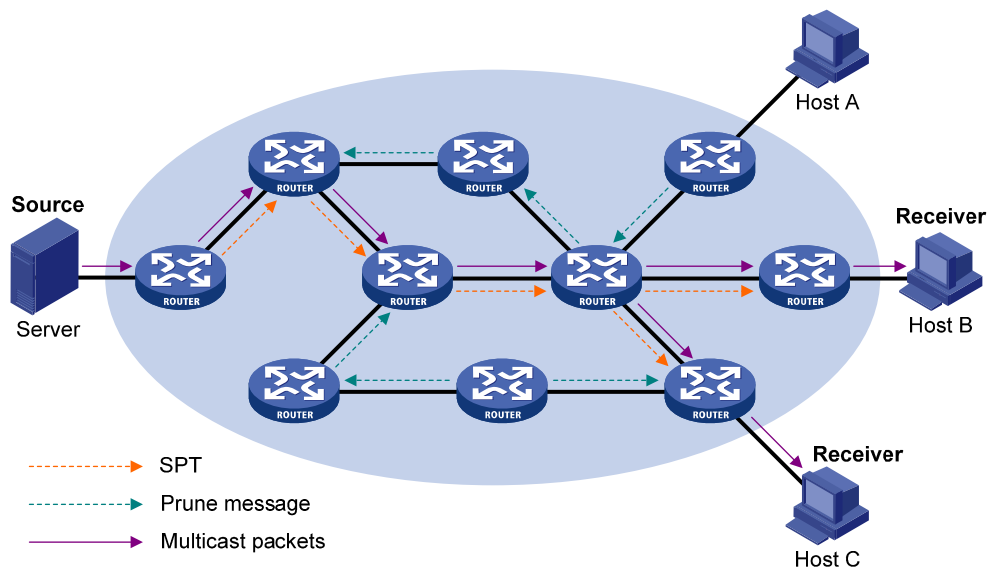
corresponding interface from the outgoing interface list in the (S, G) entry and stop forwarding subsequent packets addressed to that multicast group down to this node.

 Note

- An (S, G) entry contains the multicast source address S, multicast group address G, outgoing interface list, and incoming interface.
 - For a given multicast stream, the interface that receives the multicast stream is referred to as “upstream”, and the interfaces that forward the multicast stream are referred to as “downstream”.
-

A prune process is first initiated by a leaf router. As shown in [Figure 4-1](#), a router without any receiver attached to it (the router connected with Host A, for example) sends a prune message, and this prune process goes on until only necessary branches are left in the PIM-DM domain. These branches constitute the SPT.

Figure 4-1 SPT building



The “flood and prune” process takes place periodically. A pruned state timeout mechanism is provided. A pruned branch restarts multicast forwarding when the pruned state times out and then is pruned again when it no longer has any multicast receiver.

 Note

Pruning has a similar implementation in PIM-SM.

Graft

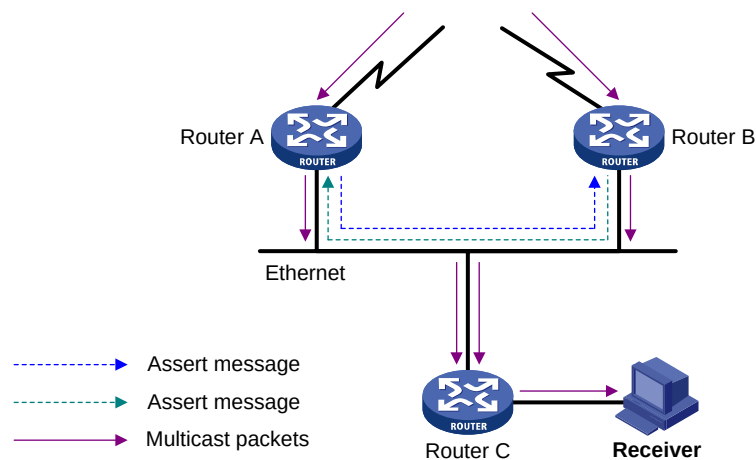
When a host attached to a pruned node joins a multicast group, to reduce the join latency, PIM-DM uses a graft mechanism to resume data forwarding to that branch. The process is as follows:

- 1) The node that need to receive multicast data sends a graft message hop by hop toward the source, as a request to join the SPT again.
- 2) Upon receiving this graft message, the upstream node puts the interface on which the graft was received into the forwarding state and responds with a graft-ack message to the graft sender.
- 3) If the node that sent a graft message does not receive a graft-ack message from its upstream node, it will keep sending graft messages at a configurable interval until it receives an acknowledgment from its upstream node.

Assert

If multiple multicast routers exist on a multi-access subnet, duplicate packets may flow to the same subnet. To shutoff duplicate flows, the assert mechanism is used for election of a single multicast forwarder on a multi-access network.

Figure 4-2 Assert mechanism



As shown in [Figure 4-2](#), after Router A and Router B receive an (S, G) packet from the upstream node, they both forward the packet to the local subnet. As a result, the downstream node Router C receives two identical multicast packets, and both Router A and Router B, on their own local interface, receive a duplicate packet forwarded by the other. Upon detecting this condition, both routers send an assert message to all PIM routers (224.0.0.13) through the interface on which the packet was received. The assert message contains the following information: the multicast source address (S), the multicast group address (G), and the preference and metric of the unicast route to the source. By comparing these parameters, either Router A or Router B becomes the unique forwarder of the subsequent (S, G) packets on the multi-access subnet. The comparison process is as follows:

- 1) The router with a higher unicast route preference to the source wins;
- 2) If both routers have the same unicast route preference to the source, the router with a smaller metric to the source wins;
- 3) If there is a tie in route metric to the source, the router with a higher IP address of the local interface wins.

Introduction to PIM-SM

PIM-DM uses the “flood and prune” principle to build SPTs for multicast data distribution. Although an SPT has the shortest path, it is built with a low efficiency. Therefore the PIM-DM mod is not suitable for large- and medium-sized networks.

PIM-SM is a type of sparse mode multicast protocol. It uses the “pull mode” for multicast forwarding, and is suitable for large- and medium-sized networks with sparsely and widely distributed multicast group members.

The basic implementation of PIM-SM is as follows:

- PIM-SM assumes that no hosts need to receive multicast data. In the PIM-SM mode, routers must specifically request a particular multicast stream before the data is forwarded to them. The core task for PIM-SM to implement multicast forwarding is to build and maintain rendezvous point trees (RPTs). An RPT is rooted at a router in the PIM domain as the common node, or rendezvous point (RP), through which the multicast data travels along the RPT and reaches the receivers.
- When a receiver is interested in the multicast data addressed to a specific multicast group, the router connected to this receiver sends a join message to the RP corresponding to that multicast group. The path along which the message goes hop by hop to the RP forms a branch of the RPT.
- When a multicast source sends a multicast packet to a multicast group, the router directly connected with the multicast source first registers the multicast source with the RP by sending a register message to the RP by unicast. The arrival of this message at the RP triggers the establishment of an SPT. Then, the multicast source sends subsequent multicast packets along the SPT to the RP. Upon reaching the RP, the multicast packet is duplicated and delivered to the receivers along the RPT.



Note

Multicast traffic is duplicated only where the distribution tree branches, and this process automatically repeats until the multicast traffic reaches the receivers.

How PIM-SM Works

The working mechanism of PIM-SM is summarized as follows:

- Neighbor discovery
- DR election
- RP discovery
- RPT building
- Multicast source registration
- Switchover from RPT to SPT
- Assert

Neighbor discovery

PIM-SM uses exactly the same neighbor discovery mechanism as PIM-DM does. Refer to [Neighbor discovery](#).

DR election

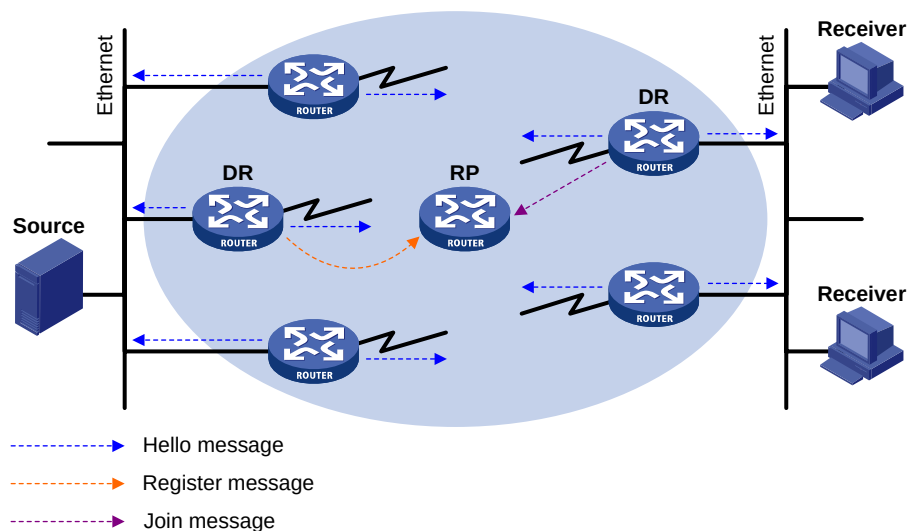
PIM-SM also uses hello messages to elect a designated router (DR) for a multi-access network. The elected DR will be the only multicast forwarder on this multi-access network.

A DR must be elected in a multi-access network, no matter this network connects to multicast sources or to receivers. The DR at the receiver side sends join messages to the RP; the DR at the multicast source side sends register messages to the RP.

 Note

- A DR is elected on a multi-access subnet by means of comparison of the priorities and IP addresses carried in hello messages. An elected DR is substantially meaningful to PIM-SM. PIM-DM itself does not require a DR. However, if IGMPv1 runs on any multi-access network in a PIM-DM domain, a DR must be elected to act as the IGMPv1 querier on that multi-access network.
 - IGMP must be enabled on a device that acts as a DR before receivers attached to this device can join multicast groups through this DR.
-

Figure 4-3 DR election



As shown in [Figure 4-3](#), the DR election process is as follows:

- 1) Routers on the multi-access network send hello messages to one another. The hello messages contain the router priority for DR election. The router with the highest DR priority will become the DR.
- 2) In the case of a tie in the router priority, or if any router in the network does not support carrying the DR-election priority in hello messages, the router with the highest IP address will win the DR election.

When the DR fails, a timeout in receiving hello message triggers a new DR election process among the other routers.



Note

- S3600 series Ethernet switches do not support DR priority. DR election is based on IP addresses.
- In a PIM-DM domain, a DR serves as an IGMPv1 querier.

RP discovery

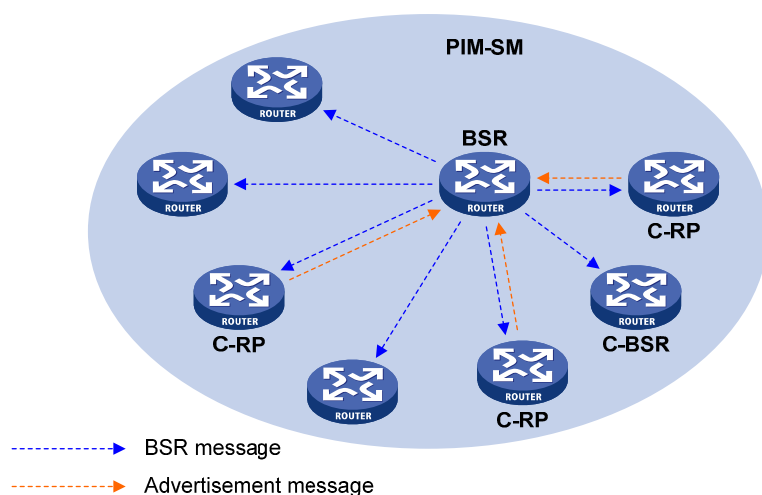
The RP is the core of a PIM-SM domain. For a small-sized, simple network, one RP is enough for forwarding information throughout the network, and the position of the RP can be statically specified on each router in the PIM-SM domain. In most cases, however, a PIM-SM network covers a wide area and a huge amount of multicast traffic needs to be forwarded through the RP. To lessen the RP burden and optimize the topological structure of the RPT, each multicast group should have its own RP. Therefore, a bootstrap mechanism is needed for dynamic RP election. For this purpose, a bootstrap router (BSR) should be configured.

As the administrative core of a PIM-SM domain, the BSR collects advertisement messages (C-RP-Adv messages) from candidate-RPs (C-RPs) and chooses the appropriate C-RP information for each multicast group to form an RP-Set, which is a database of mappings between multicast groups and RPs. The BSR then floods the RP-Set to the entire PIM-SM domain. Based on the information in these RP-Sets, all routers (including the DRs) in the network can calculate the location of the corresponding RPs.

A PIM-SM domain (or an administratively scoped region) can have only one BSR, but can have multiple candidate-BSRs (C-BSRs). Once the BSR fails, a new BSR is automatically elected from the C-BSRs through the bootstrap mechanism to avoid service interruption. Similarly, multiple C-RPs can be configured in a PIM-SM domain, and the position of the RP corresponding to each multicast group is calculated through the BSR mechanism.

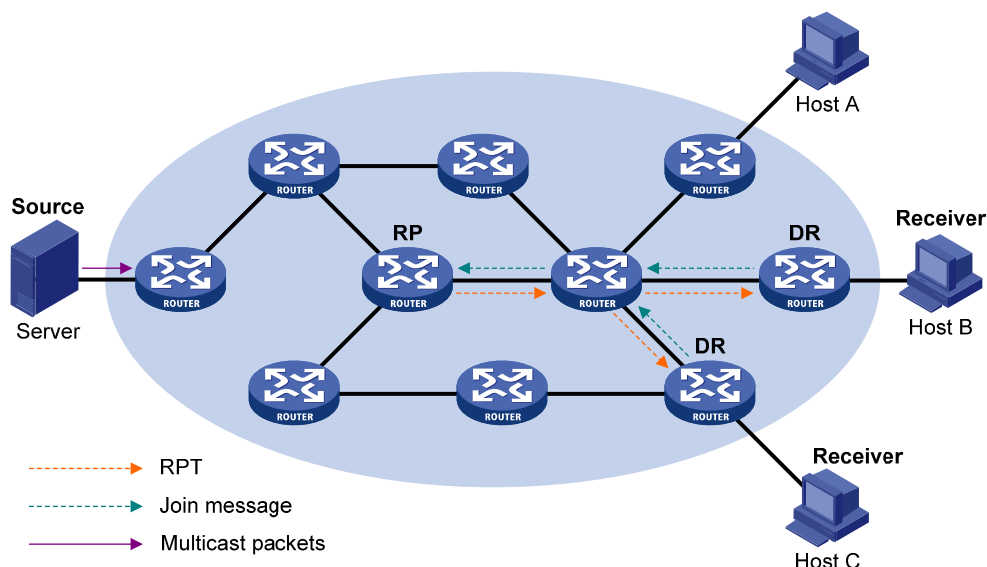
[Figure 4-4](#) shows the positions of C-RPs and the BSR in the network.

Figure 4-4 BSR and C-RPs



RPT building

Figure 4-5 Building an RPT in PIM-SM



As shown in [Figure 4-5](#), the process of building an RPT is as follows:

- 1) When a receiver joins a multicast group G, it uses an IGMP message to inform the directly connected DR.
- 2) Upon getting the receiver information, the DR sends a join message, which is hop by hop forwarded to the RP corresponding to the multicast group.
- 3) The routers along the path from the DR to the RP form an RPT branch. Each router on this branch generates a (*, G) entry in its forwarding table. The * means any multicast source. The RP is the root, while the DRs are the leaves, of the RPT.

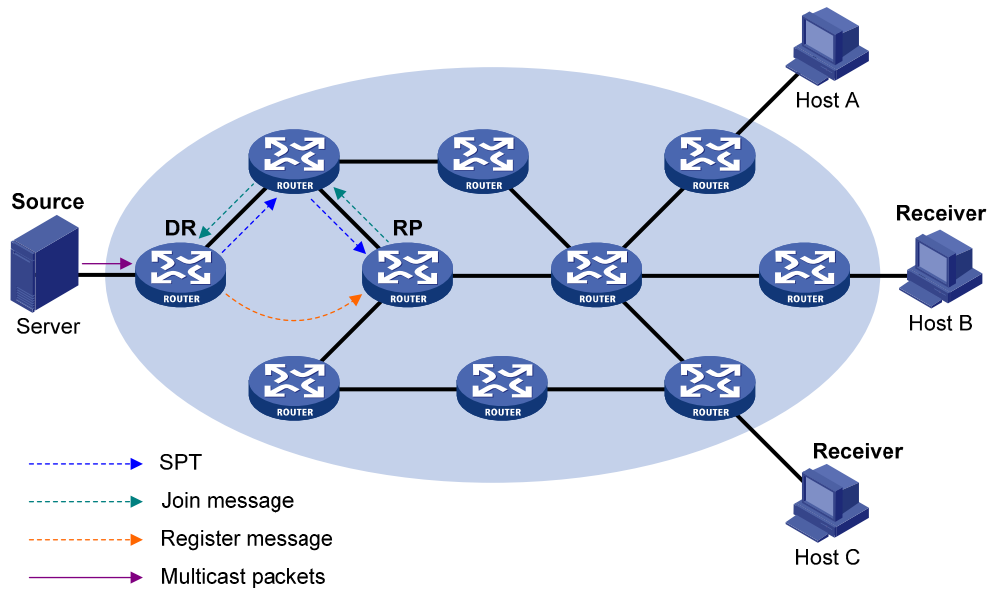
The multicast data addressed to the multicast group G flows through the RP, reaches the corresponding DR along the established RPT, and finally is delivered to the receiver.

When a receiver is no longer interested in the multicast data addressed to a multicast group G , the directly connected DR sends a prune message, which goes hop by hop along the RPT to the RP. Upon receiving the prune message, the upstream node deletes its link with this downstream node from the outgoing interface list and checks whether it itself has receivers for that multicast group. If not, the router continues to forward the prune message to its upstream router.

Multicast source registration

The purpose of multicast source registration is to inform the RP about the existence of the multicast source.

Figure 4-6 Multicast registration



As shown in [Figure 4-6](#), the multicast source registers with the RP as follows:

- 1) When the multicast source S sends the first multicast packet to a multicast group G, the DR directly connected with the multicast source, upon receiving the multicast packet, encapsulates the packet in a PIM register message, and sends the message to the corresponding RP by unicast.
- 2) When the RP receives the register message, on one hand, it extracts the multicast packet from the register message and forwards the multicast packet down the RPT, and, on the other hand, it sends an (S, G) join message hop by hop toward the multicast source. Thus, the routers along the path from the RP to the multicast source constitute an SPT branch. Each router on this branch generates a (S, G) entry in its forwarding table. The multicast source is the root, while the RP is the leaf, of the SPT.
- 3) The subsequent multicast data from the multicast source travels along the established SPT to the RP, and then the RP forwards the data along the RPT to the receivers. When the multicast traffic arrives at the RP along the SPT, the RP sends a register-stop message to the source-side DR by unicast to stop the source registration process.

Switchover from RPT to SPT

Initially, multicast traffic flows along an RPT from the RP to the receivers. Because the RPT is not necessarily the tree that has the shortest path, upon receiving the first multicast packet along the RPT, the receiver-side DR initiates an RPT-to-SPT switchover process, as follows:

- 1) First, the receiver-side DR sends an (S, G) join message hop by hop to the multicast source. When the join message reaches the source-side DR, all the routers on the path have installed the (S, G) entry in their forwarding table, and thus an SPT branch is established.
- 2) Subsequently, the receiver-side DR sends a prune message hop by hop to the RP. Upon receiving this prune message, the RP forwards it towards the multicast source, thus to implement RPT-to-SPT switchover.

After the RPT-to-SPT switchover, multicast data can be directly sent from the source to the receivers. PIM-SM builds SPTs through RPT-to-SPT switchover more economically than PIM-DM does through the “flood and prune” mechanism.

Assert

PIM-SM uses exactly the same assert mechanism as PIM-DM does. Refer to [Assert](#).

Configuring PIM-DM

Enabling PIM-DM

With PIM-DM enabled, a router sends hello messages periodically to discover PIM neighbors and processes messages from PIM neighbors. When deploying a PIM-DM domain, you are recommended to enable PIM-DM on all interfaces of non-border routers.

Follow these steps to enable PIM-DM:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable multicast routing	multicast routing-enable	Required Disabled by default
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable PIM-DM	pim dm	Required Disabled by default

Configuring PIM-SM

Complete the following tasks to configure PIM-SM:

Task	Remarks
Enabling PIM-SM	Required
Configuring an RP	Required
Configuring a BSR	Optional
Filtering the Registration Packets from DR to RP	Optional
Disabling RPT-to-SPT Switchover	Optional

Enabling PIM-SM

With PIM-SM enabled, a router sends hello messages periodically to discover PIM neighbors and processes messages from PIM neighbors. When deploying a PIM-SM domain, you are recommended to enable PIM-SM on all interfaces of non-border routers (border routers are PIM-enabled routers located on the boundary of BSR admin-scope regions).

Follow these steps to enable PIM-SM:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable multicast routing	multicast routing-enable	Required Disabled by default

To do...	Use the command...	Remarks
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable PIM-SM	pim sm	Required Disabled by default

Configuring an RP

An RP can be manually configured or dynamically elected through the BSR mechanism. For a large PIM network, static RP configuration is a tedious job. Generally, static RP configuration is just a backup means for the dynamic RP election mechanism to enhance the robustness and operation manageability of a multicast network.

Configuring a static RP

If there is only one dynamic RP in a network, manually configuring a static RP can avoid communication interruption due to single-point failures and avoid frequent message exchange between C-RPs and the BSR. To enable a static RP to work normally, you must perform this configuration on all the routers in the PIM-SM domain and specify the same RP address.

Follow these steps to configure a static RP:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter PIM view	pim	—
Configure a static RP	static-rp <i>rp-address</i> [<i>acl-number</i>]	Optional No static RP by default

Configuring a C-RP

In a PIM-SM domain, you can configure routers that intend to become the RP as C-RPs. The BSR collects the C-RP information by receiving the C-RP-Adv messages from C-RPs or auto-RP announcements from other routers and organizes the information into an RP-set, which is flooded throughout the entire network. Then, the other routers in the network calculate the mappings between specific group ranges and the corresponding RPs based on the RP-set. We recommend that you configure C-RPs on backbone routers.

To guard against C-RP spoofing, you need to configure a legal C-RP address range and the range of multicast groups to be served on the BSR. In addition, because every C-BSR has a chance to become the BSR, you need to configure the same filtering policy on all C-BSRs in the PIM-SM domain.

Follow these steps to configure a C-RP:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter PIM view	pim	—

To do...	Use the command...	Remarks
Configure candidate RPs	c-rp <i>interface-type</i> <i>interface-number</i> [group-policy <i>acl-number</i> priority <i>priority</i>]*	Optional By default, candidate RPs are not set for the switch and the value of priority is 0.
Limit the range of valid C-RPs	crp-policy <i>acl-number</i>	Optional By default, the range of valid C-RPs is not set for the switch.



Note

- If the range of multicast groups that an RP serves is not specified when the RP is configured, the RP serves all multicast groups.
- If the configured static RP address is the address of an UP interface on the local switch, the switch will serve as an RP.
- Static RPs do not take effect when the RP generated by the BSR mechanism takes effect.

Configuring a BSR

A PIM-SM domain can have only one BSR, but must have at least one C-BSR. Any router can be configured as a C-BSR. Elected from C-BSRs, the BSR is responsible for collecting and advertising RP information in the PIM-SM domain.

Configuring a C-BSR

C-BSRs should be configured on routers in the backbone network. When configuring a router as a C-BSR, be sure to specify a PIM-SM-enabled interface on the router. The BSR election process is summarized as follows:

- Initially, every C-BSR assumes itself to be the BSR of this PIM-SM domain, and uses its interface IP address as the BSR address to send bootstrap messages.
- When a C-BSR receives the bootstrap message of another C-BSR, it first compares its own priority with the other C-BSR's priority carried in message. The C-BSR with a higher priority wins. If there is a tie in the priority, the C-BSR with a higher IP address wins. The loser uses the winner's BSR address to replace its own BSR address and no longer assumes itself to be the BSR, while the winner retains its own BSR address and continues assuming itself to be the BSR.

Configuring a legal range of BSR addresses enables filtering of bootstrap messages based on the address range, thus to prevent a maliciously configured host from masquerading as a BSR. The same configuration needs to be made on all routers in the PIM-SM domain. The following are typical BSR spoofing cases and the corresponding preventive measures:

- 1) Some maliciously configured hosts can forge bootstrap messages to fool routers and change RP mappings. Such attacks often occur on border routers. Because a BSR is inside the network whereas hosts are outside the network, you can protect a BSR against attacks from external hosts by enabling the border routers to perform neighbor checks and RPF checks on bootstrap messages and discard unwanted messages.
- 2) When a router in the network is controlled by an attacker or when an illegal router is present in the network, the attacker can configure this router as a C-BSR and make it win BSR election to control

the right of advertising RP information in the network. After being configured as a C-BSR, a router automatically floods the network with bootstrap messages. As a bootstrap message has a TTL value of 1, the whole network will not be affected as long as the neighbor router discards these bootstrap messages. Therefore, with a legal BSR address range configured on all routers in the entire network, all these routers will discard bootstrap messages from out of the legal address range.

The above-mentioned preventive measures can partially protect the security of BSRs in a network. However, if a legal BSR is controlled by an attacker, the above-mentioned problem will still occur.

Follow these steps to configure a C-BSR:

To do...	Use the command...	Remarks
Enter system view	<code>system-view</code>	—
Enter PIM view	pim	—
Configure an interface as a C-BSR	c-bsr <i>interface-type interface-number hash-mask-len [priority]</i>	Optional No C-BSRs are configured by default. The default priority is 0.
Configure a legal BSR address range	bsr-policy <i>acl-number</i>	Optional No restrictions on BSR address range by default



Note

Only one C-BSR is in effect on a Layer 3 switch at a time and the latest C-BSR configured on another interface will overwrite the existing one.

Configuring a PIM-SM domain border

As the administrative core of a PIM-SM domain, the BSR sends the collected RP-Set information in the form of bootstrap messages to all routers in the PIM-SM domain.

A PIM domain border is a bootstrap message boundary. Each BSR has its specific service scope. A number of PIM domain border interfaces partition a network into different PIM-SM domains. Bootstrap messages cannot cross a domain border in either direction.

Perform the following configuration on routers that can become a PIM-SM domain border.

Follow these steps to configure a PIM-SM domain border:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type interface-number</i>	—
Configure a PIM-SM domain border	pim bsr-boundary	Optional By default, no PIM-SM domain border is configured.



Caution

After this feature is configured, Bootstrap messages cannot pass the border. However, the other PIM messages can pass the domain border. The network can be effectively divided into domains that use different BSRs.

Filtering the Registration Packets from DR to RP

Within a PIM-SM domain, the source-side DR sends register messages to the RP, and these register messages have different multicast source or group addresses. You can configure a filtering rule to filter register messages so that the RP can serve specific multicast groups. If an (S, G) entry is denied by the filtering rule, or the action for this entry is not defined in the filtering rule, the RP will send a register-stop message to the DR to stop the registration process for the multicast data..

Follow these steps to filter the registration packets from RP to DR:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter PIM view	pim	—
Configure to filter the registration packets from RP to DR	register-policy <i>acl-number</i>	Required By default, the switch does not filter the registration packets from DR.



Caution

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.

Disabling RPT-to-SPT Switchover

Initially, a PIM-SM-enabled multicast device forwards multicast packets through an RPT. By default, the last-hop switch initiates an RPT-to-SPT switchover process. You can also disable RPT-to-SPT switchover through the configuration.

Follow these steps to disable RPT-to-SPT switchover:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter PIM view	pim	—
Disable RPT-to-SPT switchover	spt-switch-threshold <i>infinity</i> [group-policy <i>acl-number</i> [order <i>order-value</i>]]	Optional By default, the device switches to the SPT immediately after it receives the first multicast packet from the RPT.



Note

Typically, you need to configure the above-mentioned parameters on the receiver-side DR and the RP only. Since both the DR and RP are elected, however, you should carry out these configurations on the routers that may win DR election and on the C-RPs that may win RP election.

Configuring Common PIM Parameters

Complete the following tasks to configure common PIM parameters:

Task	Remarks
Configuring a Multicast Data Filter	Optional
Configuring the Hello Interval	Optional
Configuring PIM Neighbors	Optional
Configuring Multicast Source Lifetime	Optional
Configuring PIM Prune Delay	Optional
Clearing the Related PIM Entries	Optional

Configuring a Multicast Data Filter

No matter in a PIM-DM domain or a PIM-SM domain, routers can check passing-by multicast data based on the configured filtering rules and determine whether to continue forwarding the multicast data. In other words, PIM routers can act as multicast data filters. These filters can help implement traffic control on one hand, and control the information available to receivers downstream to enhance data security on the other hand.

Follow these steps to configure a multicast data filter:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter PIM view	pim	—
Configure a multicast group filter	source-policy <i>acl-number</i>	Optional No multicast data filter by default



Caution

- If you have configured a basic ACL, the switch filters all the received multicast packets based on the multicast source address, and discards packets that fail source address match.
- If you have configured an advanced ACL, the switch filters all the received multicast packets based on the multicast source address and group address, and discards packets that fail source and group address match.

Configuring the Hello Interval

In a PIM domain, a PIM router discovers PIM neighbors and maintains PIM neighboring relationships with other routers by periodically sending hello messages.

Follow these steps to configure the Hello interval:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the Hello interval on the interface	pim timer hello <i>seconds</i>	Required The default Hello interval is 30 seconds.



Caution

Before configuring related PIM functions, you must enable PIM-DM or PIM-SM first.

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 define what Layer 3 switches can become PIM neighbors of the current interface by configuring a basic ACL.

Follow these steps to configure PIM neighbors:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure a limit on the number of PIM neighbors on the interface	pim neighbor-limit <i>limit</i>	Optional By default, the upper limit on the number of PIM neighbors on an interface is 128.

To do...	Use the command...	Remarks
Configure a filtering rule to filter PIM neighbors	pim neighbor-policy <i>acl-number</i>	Optional By default, no filtering rule is configured.



Caution

If the number of existing PIM neighbors exceeds the user-defined limit, the existing PIM neighbors will not be deleted.

Configuring Multicast Source Lifetime

Initially, some data is lost when multicast receivers receive multicast data from a multicast source. The reason is that (S, G) entries in the PIM routing table and multicast routing table age out if no data stream is received within a configurable period of time, known as multicast source lifetime or (S, G) aging time. These entries need to be reestablished before the corresponding multicast data can be forwarded by the multicast switch again. In the process of table entry reestablishment, some data may be lost.

If the multicast source lifetime is appropriately lengthened when the data traffic has stopped, the multicast data, when arriving at the multicast switch again, can be forwarded by the switch without the need of reestablishing the table entries. This helps avoid data loss.

Follow these steps to configure multicast source lifetime:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter PIM view	pim	—
Configure multicast source lifetime	source-lifetime <i>interval</i>	Optional 210 seconds by default



Caution

The configured multicast source lifetime applies to all (S, G) entries in the PIM routing table and the multicast routing table rather than to a specific (S, G) entry, and the configuration changes the aging time of all the existing (S, G) entries.

Configuring PIM Prune Delay



Note

The PIM prune delay function is applicable only to PIM-SM networks, but not to PIM-DM networks.

Upon receiving a prune message from a downstream device, the upstream node removes the interface connecting the downstream node from the outgoing interface list of the (S, G) entry. If the downstream node finds shortly after it has sent a prune message that a member for the multicast group is present on the local subnet, it immediately sends a prune override message to the upstream to let the upstream node cancel the prune action.

The S3600 series Ethernet switches support prune delay configuration. Upon receiving a prune message from a downstream node, the upstream node does not take a prune action immediately; instead, it maintains the forwarding state of the interface to the downstream. If the upstream node receives a prune override message from the downstream node within the prune delay interval, it cancels the prune action; otherwise, it prunes the interface to the downstream when the prune delay times out.

An appropriate PIM prune delay setting can reduce the number of prune/graft operations to downstream nodes and thus lessen the burden to the device itself and the network.

Follow these steps to configure PIM prune delay:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter PIM view	pim	—
Configure the PIM prune delay interval	prune delay <i>interval</i>	Optional 5 seconds by default

Clearing the Related PIM Entries

You can execute the **reset** command in user view to clear the related statistics about multicast PIM.

Follow these steps to clear the related PIM entries:

To do...	Use the command...	Remarks
Clear PIM route entries	reset pim routing-table { all { <i>group-address</i> [mask { <i>mask-length</i> <i>mask</i> }] <i>source-address</i> [mask { <i>mask-length</i> <i>mask</i> }] incoming-interface <i>interface-type</i> <i>interface-number</i> } * }	Perform the configuration in user view.
Clear PIM neighbors	reset pim neighbor { all { <i>neighbor-address</i> interface <i>interface-type</i> <i>interface-number</i> } * }	

Displaying and Maintaining PIM

Configuration	Use the command...	Remarks
Display PIM multicast routing tables	display pim routing-table [{ { * g [<i>group-address</i> [mask { <i>mask-length</i> <i>mask</i> }]] ** rp [<i>rp-address</i> [mask { <i>mask-length</i> <i>mask</i> }]] } { <i>group-address</i> [mask { <i>mask-length</i> <i>mask</i> }] <i>source-address</i> [mask { <i>mask-length</i> <i>mask</i> }] } * } incoming-interface { <i>interface-type</i> <i>interface-number</i> null } { dense-mode sparse-mode }] * }	Available in any view

Configuration	Use the command...	Remarks
Display the information about PIM interfaces	display pim interface [<i>interface-type interface-number</i>]	Available in any view
Display the information about PIM neighbor routers	display pim neighbor [interface <i>interface-type interface-number</i>]	Available in any view
Display BSR information	display pim bsr-info	Available in any view
Display RP information	display pim rp-info [<i>group-address</i>]	Available in any view

PIM Configuration Examples

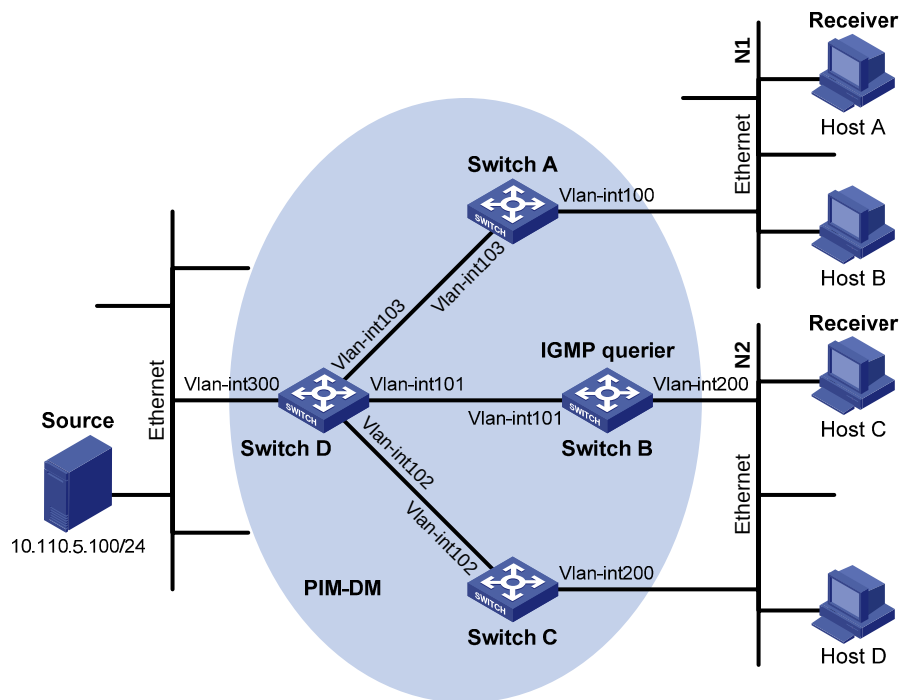
PIM-DM Configuration Example

Network requirements

- Receivers receive VOD information through multicast. The receiver groups of different organizations form stub networks, and one or more receiver hosts exist in each stub network. The entire PIM domain operates in the dense mode.
- Host A and Host C are multicast receivers in two stub networks.
- Switch D connects to the network that comprises the multicast source (Source) through VLAN-interface 300.
- Switch A connects to stub network N1 through VLAN-interface 100, and to Switch D through VLAN-interface 103.
- Switch B and Switch C connect to stub network N2 through their respective VLAN-interface 200, and to Switch D through VLAN-interface 101 and VLAN-interface 102 respectively.
- IGMP is required on Switch A, Switch B, Switch C, and hosts in N1 and N2. Switch B is the IGMP querier on the multi-access subnet.

Network diagram

Figure 4-7 Network diagram for PIM-DM configuration



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int100	10.110.1.1/24	Switch D	Vlan-int300	10.110.5.1/24
	Vlan-int103	192.168.1.1/24		Vlan-int103	192.168.1.2/24
Switch B	Vlan-int200	10.110.2.1/24		Vlan-int101	192.168.2.2/24
	Vlan-int101	192.168.2.1/24		Vlan-int102	192.168.3.2/24
Switch C	Vlan-int200	10.110.2.2/24			
	Vlan-int102	192.168.3.1/24			

Configuration procedure

- 1) Configure the interface IP addresses and unicast routing protocol for each switch

Configure the IP address and subnet mask for each interface as per [Figure 4-7](#). Detailed configuration steps are omitted here.

Configure the OSPF protocol for interoperation among the switches in the PIM-DM domain. Ensure the network-layer interoperation among Switch A, Switch B, Switch C and Switch D in the PIM-DM domain and enable dynamic update of routing information among the switches through a unicast routing protocol. Detailed configuration steps are omitted here.

- 2) Enable IP multicast routing, and enable PIM-DM on each interface

Enable IP multicast routing on Switch A, enable PIM-DM on each interface, and enable IGMP on VLAN-interface 100, which connects Switch A to the stub network.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim dm
```

```
[SwitchA-Vlan-interface103] quit
```

The configuration on Switch B and Switch C is similar to the configuration on Switch A.

Enable IP multicast routing on Switch D, and enable PIM-DM on each interface.

```
<SwitchD> system-view
[SwitchD] multicast routing-enable
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] pim dm
[SwitchD-Vlan-interface300] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim dm
[SwitchD-Vlan-interface103] quit
[SwitchD] interface vlan-interface 101
[SwitchD-Vlan-interface101] pim dm
[SwitchD-Vlan-interface101] quit
[SwitchD] interface vlan-interface 102
[SwitchD-Vlan-interface102] pim dm
[SwitchD-Vlan-interface102] quit
```

Verifying the configuration

Use the **display pim neighbor** command to view the PIM neighboring relationships among the switches. For example:

View the PIM neighboring relationships on Switch D.

```
[SwitchD] display pim neighbor
```

Neighbor's Address	Interface Name	Uptime	Expires
192.168.1.1	Vlan-interface1	00:47:08	00:01:39
192.168.2.1	Vlan-interface1	00:48:05	00:01:29
192.168.3.1	Vlan-interface1	00:49:08	00:01:34

Use the **display pim routing-table** command to view the PIM routing table information on each switch. For example:

View the PIM routing table information on Switch A.

```
<SwitchA> display pim routing-table
PIM-DM Routing Table
Total 1 (S,G) entry

(10.110.5.100, 225.1.1.1)
  Protocol 0x40: PIMDM, Flag 0xC: SPT NEG_CACHE
  Uptime: 00:00:23, Timeout in 187 sec
  Upstream interface: Vlan-interface103, RPF neighbor: 192.168.1.2
  Downstream interface list:
    Vlan-interface100, Protocol 0x1: IGMP, never timeout

Matched 1 (S,G) entry
```

The information on Switch B and Switch C is similar to that on Switch A.

View the PIM routing table information on Switch D.

```
<SwitchD> display pim routing-table
```

PIM-DM Routing Table

Total 1 (S,G) entry

(10.110.5.100, 225.1.1.1)

Protocol 0x40: PIMDM, Flag 0xC: SPT NEG_CACHE

Uptime: 00:00:23, Timeout in 187 sec

Upstream interface: Vlan-interface300, RPF neighbor: NULL

Downstream interface list:

Vlan-interface101, Protocol 0x200: SPT, timeout in 147 sec

Vlan-interface103, Protocol 0x200: SPT, timeout in 145 sec

Vlan-interface103, Protocol 0x200: SPT, timeout in 145 sec

Matched 1 (S,G) entry

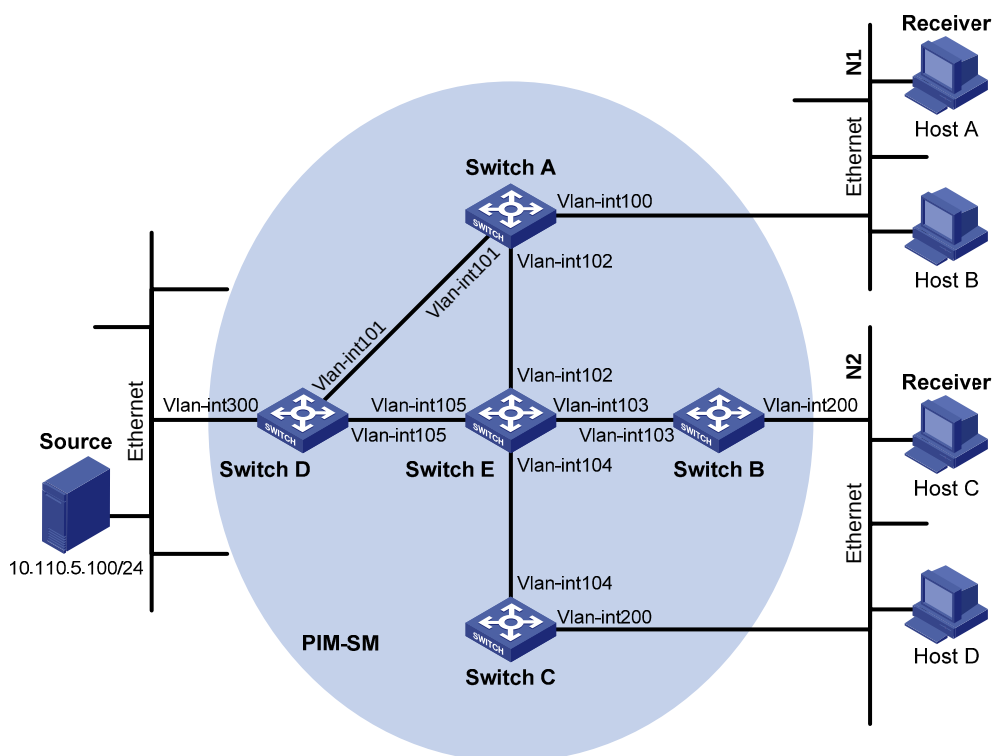
PIM-SM Configuration Example

Network requirements

- Receivers receive VOD information through multicast. The receiver groups of different organizations form stub networks, and one or more receiver hosts exist in each stub network. The entire PIM domain operates in the sparse mode (not divided into different BSR admin-scope regions).
- Host A and Host C are multicast receivers in two stub networks.
- Switch D connects to the network that comprises the multicast source (Source) through VLAN-interface 300.
- Switch A connects to stub network N1 through VLAN-interface 100, and to Switch D and Switch E through VLAN-interface 101 and VLAN-interface 102 respectively.
- Switch B and Switch C connect to stub network N2 through their respective VLAN-interface 200, and to Switch E through VLAN-interface 103 and VLAN-interface 104 respectively.
- Switch E connects to Switch A, Switch B, Switch C and Switch D, and its VLAN-interface 102 interface acts a C-BSR and a C-RP, with the range of multicast groups served by the C-RP being 225.1.1.0/24.

Network diagram

Figure 4-8 Network diagram for PIM-SM domain configuration



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlanint100	10.110.1.1/24	Switch D	Vlanint300	10.110.5.1/24
	Vlanint101	192.168.1.1/24		Vlanint101	192.168.1.2/24
	Vlanint102	192.168.9.1/24		Vlanint105	192.168.4.2/24
Switch B	Vlanint200	10.110.2.1/24	Switch E	Vlanint104	192.168.3.2/24
	Vlanint103	192.168.2.1/24		Vlanint103	192.168.2.2/24
Switch C	Vlanint200	10.110.2.2/24		Vlanint102	192.168.9.2/24
	Vlanint104	192.168.3.1/24		Vlanint105	192.168.4.1/24

Configuration procedure

- 1) Configure the interface IP addresses and unicast routing protocol for each switch

Configure the IP address and subnet mask for each interface as per [Figure 4-8](#). Detailed configuration steps are omitted here.

Configure the OSPF protocol for interoperability among the switches in the PIM-SM domain. Ensure the network-layer interoperability among Switch A, Switch B, Switch C, Switch D and Switch E in the PIM-SM domain and enable dynamic update of routing information among the switches through a unicast routing protocol. Detailed configuration steps are omitted here.

- 2) Enable IP multicast routing, and enable PIM-SM on each interface

Enable IP multicast routing on Switch A, enable PIM-SM on each interface, and enable IGMP on VLAN-interface 100, which connects Switch A to the stub network.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
SwitchA-Vlan-interface100] pim sm
```



```
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
[SwitchA-Vlan-interface102] quit
```

The configuration on Switch B and Switch C is similar to that on Switch A. The configuration on Switch D and Switch E is also similar to that on Switch A except that it is not necessary to enable IGMP on the corresponding interfaces on these two switches.

3) Configure a C-BSR and a C-RP

Configure the service scope of RP advertisements and the positions of the C-BSR and C-RP on Switch E.

```
<SwitchE> system-view
[SwitchE] acl number 2005
[SwitchE-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchE-acl-basic-2005] quit
[SwitchE] pim
[SwitchE-pim] c-bsr vlan-interface 102 24
[SwitchE-pim] c-rp vlan-interface 102 group-policy 2005
[SwitchE-pim] quit
```

Verifying the configuration

Display PIM neighboring relationships on Switch E.

```
<SwitchE> display pim neighbor
```

Neighbor's Address	Interface Name	Uptime	Expires
192.168.9.1	Vlan-interface102	02:47:04	00:01:42
192.168.2.1	Vlan-interface103	02:45:04	00:04:46
192.168.3.1	Vlan-interface104	02:42:24	00:04:45
192.168.4.2	Vlan-interface105	02:43:44	00:05:44

Display BSR information on Switch E.

```
<SwitchE> display pim bsr-info
Current BSR Address: 192.168.9.2
Priority: 0
Mask Length: 24
Expires: 00:01:39
Local host is BSR
```

Display RP information on Switch E.

```
<SwitchE> display pim rp-info
PIM-SM RP-SET information:
BSR is: 192.168.9.2

Group/MaskLen: 225.1.1.0/24
RP 192.168.9.2
Version: 2
Priority: 0
```

Uptime: 00:49:44
Expires: 00:01:46

Display PIM routing table information on Switch A.

<SwitchA> display pim routing-table

PIM-SM Routing Table

Total 1 (S,G) entries, 1 (*,G) entries, 0 (*,*,RP) entry

(*, 225.1.1.1), RP 192.168.9.2

Protocol 0x20: PIMSM, Flag 0x2003: RPT WC NULL_IIF

Uptime: 00:23:21, never timeout

Upstream interface: Vlan-interface102, RPF neighbor: 192.168.9.2

Downstream interface list:

Vlan-interface100, Protocol 0x1: IGMP, never timeout

(10.110.5.100, 225.1.1.1)

Protocol 0x20: PIMSM, Flag 0x80004: SPT

Uptime: 00:03:43, Timeout in 199 sec

Upstream interface: Vlan-interface102, RPF neighbor: 192.168.9.2

Downstream interface list:

Vlan-interface100, Protocol 0x1: IGMP, never timeout

Matched 1 (S,G) entries, 1 (*,G) entries, 0 (*,*,RP) entry

The displayed information of Switch B and Switch C is similar to that of Switch A.

Display PIM routing table information on Switch D.

<SwitchD> display pim routing-table

PIM-SM Routing Table

Total 1 (S,G) entry, 0 (*,G) entry, 0 (*,*,RP) entry

(10.110.5.100, 225.1.1.1)

Protocol 0x20: PIMSM, Flag 0x4: SPT

Uptime: 00:03:03, Timeout in 27 sec

Upstream interface: Vlan-interface300, RPF neighbor: NULL

Downstream interface list:

Vlan-interface101, Protocol 0x200: SPT, timeout in 147 sec

Vlan-interface105, Protocol 0x200: SPT, timeout in 145 sec

Matched 1 (S,G) entry, 0 (*,G) entry, 0 (*,*,RP) entry

Display PIM routing table information on Switch E.

<SwitchE> display pim routing-table

PIM-SM Routing Table

Total 1 (S,G) entry, 1 (*,G) entry, 0 (*,*,RP) entry

(*,225.1.1.1), RP 192.168.9.2

Protocol 0x20: PIMSM, Flag 0x2003: RPT WC NULL_IIF

Uptime: 00:02:34, Timeout in 176 sec

Upstream interface: Null, RPF neighbor: 0.0.0.0

Downstream interface list:

Vlan-interface102, Protocol 0x100: RPT, timeout in 176 sec

```

Vlan-interface103, Protocol 0x100: SPT, timeout in 135 sec

(10.110.5.100, 225.1.1.1)
  Protocol 0x20: PIMSM, Flag 0x4: SPT
  Uptime: 00:03:03, Timeout in 27 sec
  Upstream interface: Vlan-interface105, RPF neighbor: 192.168.4.2
  Downstream interface list:
    Vlan-interface102, Protocol 0x200: SPT, timeout in 147 sec
    Vlan-interface103, Protocol 0x200: SPT, timeout in 145 sec
  Matched 1 (S,G) entry, 1 (*,G) entry, 0 (*,*,RP) entry

```

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.

5 MSDP Configuration

When configuring MSDP, go to these sections for information you are interested in:

- [MSDP Overview](#)
- [Configuring MSDP Basic Functions](#)
- [Configuring Connection Between MSDP Peers](#)
- [Configuring SA Message Transmission](#)
- [Displaying and Maintaining MSDP](#)
- [MSDP Configuration Example](#)
- [Troubleshooting MSDP Configuration](#)



Note

- In this manual, the term “router” refers to a router in the generic sense or a Layer 3 Ethernet switch running an IP multicast protocol.
 - S3600-SI series Ethernet switches do not support MSDP.
 - Because Multicast Source Discovery Protocol (MSDP) does not work with IRF Fabric feature, MSDP cannot be configured in IRF Fabric.
-

MSDP Overview

Introduction to MSDP

Multicast Source Discovery Protocol (MSDP) is an inter-domain multicast solution developed to address the interconnection of Protocol Independent Multicast sparse mode (PIM-SM) domains. It is used to discover multicast source information in other PIM-SM domains.

In the basic PIM-SM mode, a multicast source registers only with the RP in the local PIM-SM domain, and the multicast source information of a domain is isolated from that of another domain. As a result, the RP is aware of the source information only within the local domain and a multicast distribution tree is built only within the local domain to deliver multicast data from a local multicast source to local receivers. If there is a mechanism that allows RPs of different PIM-SM domains to share their multicast source information, the local RP will be able to join multicast sources in other domains and multicast data can be transmitted among different domains.

MSDP achieves this objective. By establishing MSDP peer relationships among RPs of different PIM-SM domains, source active (SA) messages can be forwarded among domains and the multicast source information can be shared.

 Caution

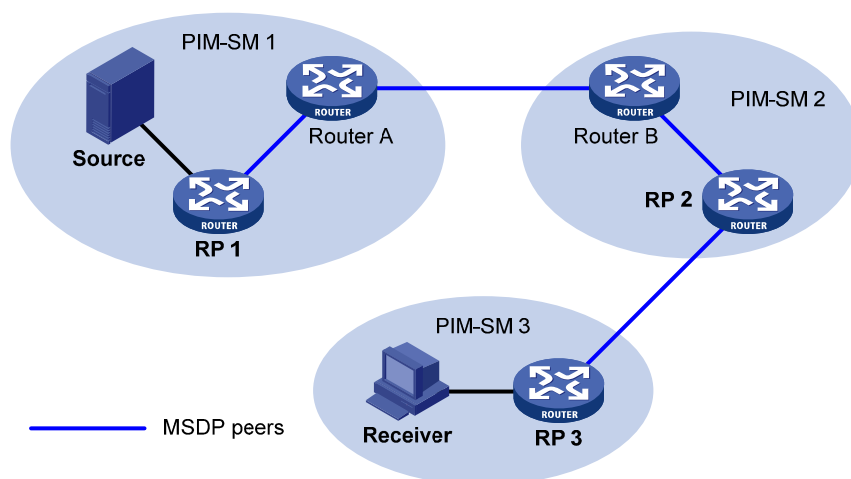
- MSDP is applicable only if the intra-domain multicast protocol is PIM-SM.
 - MSDP is meaningful only for the any-source multicast (ASM) model.
-

How MSDP Works

MSDP peers

With one or more pairs of MSDP peers configured in the network, an MSDP interconnection map is formed, where the RPs of different PIM-SM domains are interconnected in series. Relayed by these MSDP peers, an SA message sent by an RP can be delivered to all other RPs.

Figure 5-1 Where MSDP peers are in the network



As shown in [Figure 5-1](#), an MSDP peer can be created on any PIM-SM router. MSDP peers created on PIM-SM routers that assume different roles function differently.

1) MSDP peers on RPs

- Source-side MSDP peer: the MSDP peer nearest to the multicast source (Source), typically the source-side RP, like RP 1. The source-side RP creates SA messages and sends the messages to its remote MSDP peer to notify the MSDP peer of the locally registered multicast source information. A source-side MSDP must be created on the source-side RP; otherwise it will not be able to advertise the multicast source information out of the PIM-SM domain.
- Receiver-side MSDP peer: the MSDP peer nearest to the receivers, typically the source-side RP, like RP 3. Upon receiving an SA message, the receiver-side MSDP peer resolves the multicast source information carried in the message and joins the SPT rooted at the source across the PIM-SM domain. When multicast data from the multicast source arrives, the receiver-side MSDP peer forwards the data to the receivers along the RPT.

- Intermediate MSDP peer: an MSDP peer with multicast remote MSDP peers, like RP 2. An intermediate MSDP peer forwards SA messages received from one remote MSDP peer to other remote MSDP peers, functioning as a relay of multicast source information.
- 2) MSDP peers created on common PIM-SM routers (other than RPs)

Router A and Router B are MSDP peers on common multicast routers. Such MSDP peers just forward received SA messages.



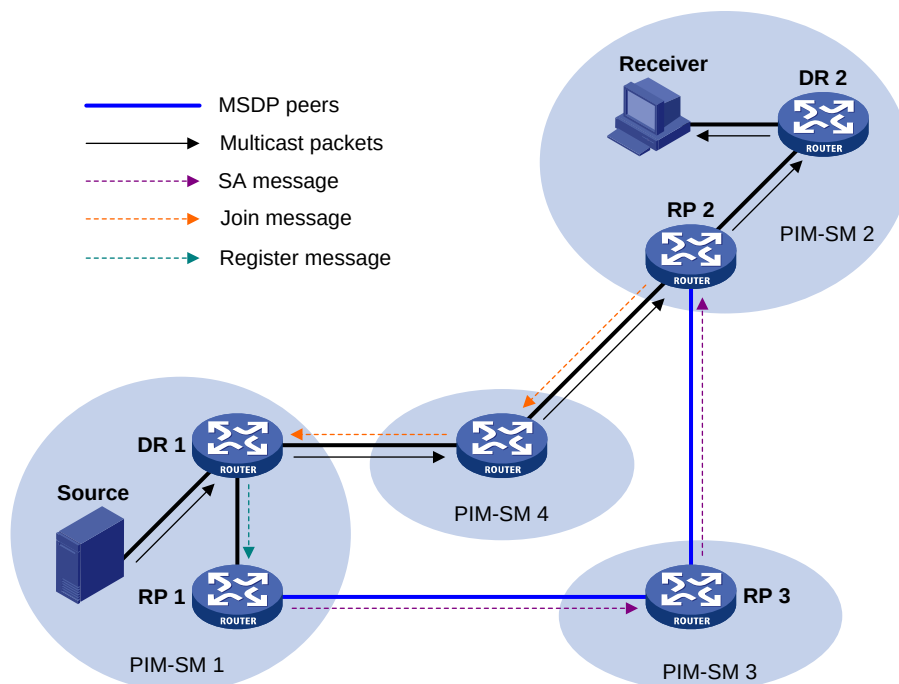
Note

An RP is dynamically elected from C-RPs. To enhance network robustness, a PIM-SM network typically has more than one C-RP. As the RP election result is unpredictable, MSDP peering relationships should be built among all C-RPs so that the winner C-RP is always on the "MSDP interconnection map", while loser C-RPs will assume the role of common PIM-SM routers on the "MSDP interconnection map".

Implementing inter-domain multicast delivery by leveraging MSDP peers

As shown in [Figure 5-2](#), an active source (Source) exists in the domain PIM-SM 1, and RP 1 has learned the existence of Source through multicast source registration. If RPs in PIM-SM 2 and PIM-SM 3 also wish to know the specific location of Source so that receiver hosts can receive multicast traffic originated from it, MSDP peering relationships should be established between RP 1 and RP 3 and between RP 3 and RP 2 respectively.

Figure 5-2 MSDP peering relationships



The process of implementing inter-domain multicast delivery by leveraging MSDP peers is as follows:

- 1) When the multicast source in PIM-SM 1 sends the first multicast packet to multicast group G, DR 1 encapsulates the multicast data within a register message and sends the register message to RP 1. Then, RP 1 gets aware of the information related to the multicast source.
- 2) As the source-side RP, RP 1 creates SA messages and periodically sends the SA messages to its MSDP peer. An SA message contains the source address (S), the multicast group address (G), and the address of the RP which has created this SA message (namely RP 1).
- 3) On MSDP peers, each SA message is subject to a Reverse Path Forwarding (RPF) check and multicast policy-based filtering, so that only SA messages that have arrived along the correct path and passed the filtering are received and forwarded. This avoids delivery loops of SA messages. In addition, you can configure MSDP peers into an MSDP mesh group so as to avoid flooding of SA messages between MSDP peers.
- 4) SA messages are forwarded from one MSDP peer to another, and finally the information of the multicast source traverses all PIM-SM domains with MSDP peers (PIM-SM 2 and PIM-SM 3 in this example).
- 5) Upon receiving the SA message create by RP 1, RP 2 in PIM-SM 2 checks whether there are any receivers for the multicast group in the domain.
 - If so, the RPT for the multicast group G is maintained between RP 2 and the receivers. RP 2 creates an (S, G) entry, and sends an (S, G) join message hop by hop towards DR 1 at the multicast source side, so that it can directly join the SPT rooted at the source over other PIM-SM domains. Then, the multicast data can flow along the SPT to RP 2 and is forwarded by RP 2 to the receivers along the RPT. Upon receiving the multicast traffic, the DR at the receiver side (DR 2) decides whether to initiate an RPT-to-SPT switchover process.
 - If no receivers for the group exist in the domain, RP 2 does not create an (S, G) entry and does not join the SPT rooted at the source.



Note

- An MSDP mesh group refers to a group of MSDP peers that have MSDP peering relationships among one another and share the same group name.
 - When using MSDP for inter-domain multicasting, once an RP receives information from a multicast source, it no longer relies on RPs in other PIM-SM domains. The receivers can override the RPs in other domains and directly join the multicast source based SPT.
-

RPF check rules for SA messages

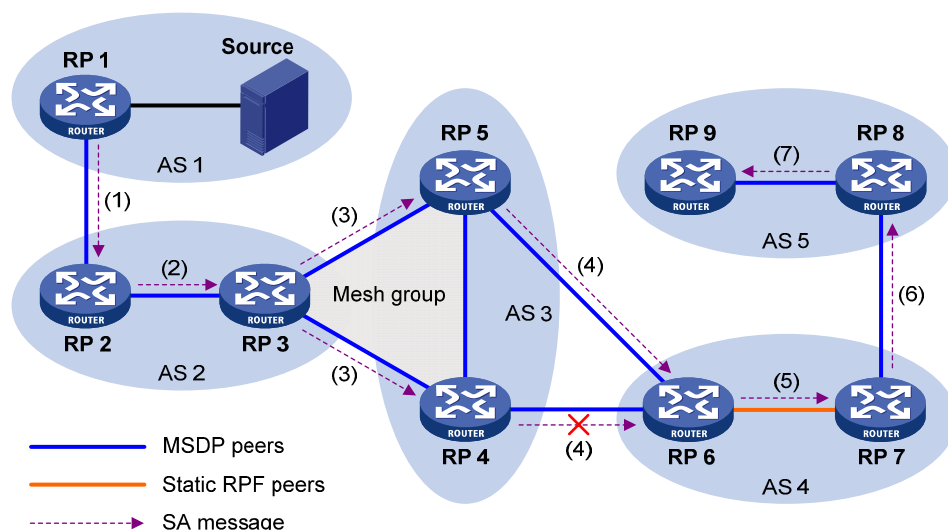
As shown in [Figure 5-3](#), there are five autonomous systems in the network, AS 1 through AS 5, with IGP enabled on routers within each AS and EBGP as the interoperation protocol among different ASs. Each AS contains at least one PIM-SM domain and each PIM-SM domain contains one or more RPs. MSDP peering relationships have been established among different RPs. RP 3, RP 4 and RP 5 are in an MSDP mesh group. On RP 7, RP 6 is configured as its static RPF peer.



Note

If only one MSDP peer exists in a PIM-SM domain, this PIM-SM domain is also called a stub domain. For example, autonomous system AS 4 in [Figure 5-3](#) is a stub domain. The MSDP peer in a stub domain can have multiple remote MSDP peers at the same time. You can configure one or more remote MSDP peers as static RPF peers. When an RP receives an SA message from a static RPF peer, the RP accepts the SA message and forwards it to other peers without performing an RPF check.

Figure 5-3 Diagram for RPF check for SA messages



As illustrated in [Figure 5-3](#), these MSDP peers dispose of SA messages according to the following RPF check rules:

- 1) When RP 2 receives an SA message from RP 1

Because the source-side RP address carried in the SA message is the same as the MSDP peer address, which means that the MSDP peer where the SA is from is the RP that has created the SA message, RP 2 accepts the SA message and forwards it to its other MSDP peer (RP 3).

- 2) When RP 3 receives the SA message from RP 2

Because the SA message is from an MSDP peer (RP 2) in the same AS, and the MSDP peer is the next hop on the optimal path to the source-side RP, RP 3 accepts the message and forwards it to other peers (RP 4 and RP 5).

- 3) When RP 4 and RP 5 receive the SA message from RP 3

Because the SA message is from an MSDP peer (RP 3) in the same mesh group, RP 4 and RP 5 both accept the SA message, but they do not forward the message to other members in the mesh group; instead, they forward it to other MSDP peers (RP 6 in this example) out of the mesh group.

- 4) When RP 6 receives the SA messages from RP 4 and RP 5 (suppose RP 5 has a higher IP address)

Although RP 4 and RP 5 are in the same SA (AS 3) and both are MSDP peers of RP 6, because RP 5 has a higher IP address, RP 6 accepts only the SA message from RP 5.

- 5) When RP 7 receives the SA message from RP 6

Because the SA message is from a static RPF peer (RP 6), RP 7 accepts the SA message and forwards it to other peer (RP 8).

6) When RP 8 receives the SA message from RP 7

An EBGp route exists between two MSDP peers in different ASs. Because the SA message is from an MSDP peer (RP 7) in a different AS, and the MSDP peer is the next hop on the EBGp route to the source-side RP, RP 8 accepts the message and forwards it to its other peer (RP 9).

7) When RP 9 receives the SA message from RP 8

Because RP 9 has only one MSDP peer, RP 9 accepts the SA message.

SA messages from other paths than described above will not be accepted nor forwarded by MSDP peers.

Implementing intra-domain Anycast RP by leveraging MSDP peers

Anycast RP refers to such an application that enables load balancing and redundancy backup between two or more RPs within a PIM-SM domain by configuring the same IP address for, and establishing MSDP peering relationships between, these RPs.

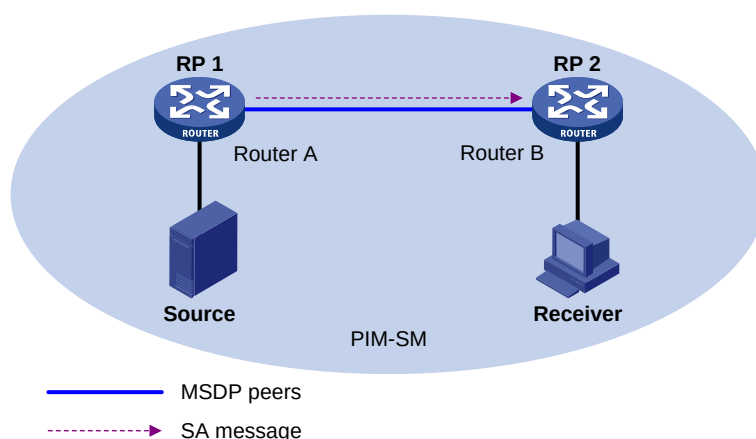
As shown in [Figure 5-4](#), within a PIM-SM domain, a multicast source sends multicast data to multicast group G, and Receiver is a member of the multicast group. To implement Anycast RP, configure the same IP address (known as anycast RP address, typically a private address) on Router A and Router B, configure these interfaces as C-RPs, and establish an MSDP peering relationship between Router A and Router B.



Note

Usually an Anycast RP address is configured on a logic interface, like a loopback interface.

Figure 5-4 Typical network diagram of Anycast RP



The work process of Anycast RP is as follows:

- 1) The multicast source registers with the nearest RP. In this example, Source registers with RP 1, with its multicast data encapsulated in the register message. When the register message arrives to RP 1, RP 1 decapsulates the message.

- 2) Receivers send join messages to the nearest RP to join in the RPT rooted at this RP. In this example, Receiver joins the RPT rooted at RP 2.
- 3) RPs share the registered multicast information by means of SA messages. In this example, RP 1 creates an SA message and sends it to RP 2, with the multicast data from Source encapsulated in the SA message. When the SA message reaches RP 2, RP 2 decapsulates the message.
- 4) Receivers receive the multicast data along the RPT and directly join the SPT rooted at the multicast source. In this example, RP 2 forwards the multicast data down the RPT. When Receiver receives the multicast data from Source, it directly joins the SPT rooted at Source.

The significance of Anycast RP is as follows:

- Optimal RP path: A multicast source registers with the nearest RP so that an SPT with the optimal path is built; a receiver joins the nearest RP so that an RPT with the optimal path is built.
- Load balancing between RPs: Each RP just needs to maintain part of the source/group information within the PIM-SM domain and forward part of the multicast data, thus achieving load balancing between different RPs.
- Redundancy backup between RPs: When an RP fails, the multicast source previously registered on it or the receivers previously joined it will register with or join another nearest RP, thus achieving redundancy backup between RPs.



Caution

- Be sure to configure a 32-bit subnet mask (255.255.255.255) for the Anycast RP address, namely configure the Anycast RP address into a host address.
 - An MSDP peer address must be different from the Anycast RP address.
-

Protocols and Standards

MSDP is documented in the following specifications:

- RFC 3618: Multicast Source Discovery Protocol (MSDP)
- RFC 3446: Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

Configuring MSDP Basic Functions

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.

Configuration Prerequisites

Before configuring basic MSDP functions, you need to configure:

- A unicast routing protocol
- PIM-SM basic functions

Configuring MSDP Basic Functions

Follow these steps to configure MSDP basic functions:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable MSDP function and enter MSDP view	msdp	Required Disabled by default
Create an MSDP peer connection	peer <i>peer-address</i> connect-interface <i>interface-type interface-number</i>	Required No MSDP peer connection is created by default.
Configure a static RPF peer	static-rpf-peer <i>peer-address</i> [rp-policy <i>ip-prefix-name</i>]	Optional No static RPF is configured by default.

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.

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

Complete the following tasks to configure an MSDP peer connection:

Task	Remarks
Configuring Description Information for MSDP Peers	Optional
Configuring an MSDP Mesh Group	Optional
Configuring MSDP Peer Connection Control	Optional

Configuring Description Information for MSDP Peers

You can configure description information for each MSDP peer to manage and memorize the MSDP peers.

Follow these steps to configure description information for an MSDP peer:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter MSDP view	msdp	—
Configure description information for an MSDP peer	peer <i>peer-address</i> description <i>text</i>	Optional By default, an MSDP peer has no description information.

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.

Follow these steps to configure an MSDP mesh group:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter MSDP view	msdp	—
Add an MSDP peer to a mesh group	peer <i>peer-address</i> mesh-group <i>name</i>	Required By default, an MSDP peer does not belong to any mesh group.



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 before they can join a mesh group.
- If you add the same MSDP peer to multiple mesh groups, only the latest configuration takes effect.

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.

Follow these steps to configure MSDP peer connection control:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter MSDP view	msdp	—
Shut down the connection with the specified MSDP peer	shutdown <i>peer-address</i>	Optional By default, all MSDP peering connections are up.
Configure the retry interval of MSDP peer connection establishment	timer retry <i>seconds</i>	Optional 30 seconds by default

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.

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.

Complete the following tasks to configure SA message transmission:

Task	Remarks
Configuring RP Address in SA Messages	Optional
Configuring SA Message Cache	Optional
Configuring the Transmission and Filtering of SA Request Messages	Optional
Configuring a Rule for Filtering the Multicast Sources of SA Messages	Optional
Configuring a Rule for Filtering Received and Forwarded SA Messages	Optional

Configuring RP Address in SA Messages

MSDP peers deliver SA messages to one another. Upon receiving an SA message, a router performs an RPF check on the message. If the router finds that the remote RP address is the same as the local RP address, it will discard the SA message. In anycast RP application, however, you need to configure RPs with the same IP address on two or more routers in the same PIM-SM domain, and configure these RPs as MSDP peers to one another. Therefore, a logic RP address (namely the RP address on a logic interface) that is different from the actual RP address must be designated for SA messages so that the messages can pass the RPF check.

Follow these steps to configure RP address in SA messages:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter MSDP view	msdp	—
Configure the address of the specified interface as the RP address in SA messages	originating-rp <i>interface-type interface-number</i>	Required By default, the RP address in SA messages is the RP address configured for PIM.



Note

In Anycast RP application, a C-BSR and a C-RP must be configured on different devices or ports.

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 Denial 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.

Follow these steps to configure SA message cache:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter MSDP view	msdp	—
Enable SA message caching mechanism	cache-sa-enable	Optional Enabled by default
Configure the maximum number of SA messages that can be cached	peer <i>peer-address</i> sa-cache-maximum <i>sa-limit</i>	Optional The default is 2,048.

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. The SA message that the remote MSDP peer sends in response 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.

Follow these steps to configure the transmission and filtering of SA request messages:

To do...	Use the command...	Remarks
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 <i>peer-address</i> 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.

To do...	Use the command...	Remarks
Configure a rule for filtering the SA messages received by an MSDP peer	peer <i>peer-address</i> sa-request-policy [acl <i>acl-number</i>]	Optional By default, a router receives all SA request messages from the MSDP peer.

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.

Follow these steps to configure a rule for filtering multicast sources using SA messages:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter MSDP view	msdp	—
Configure to filter multicast sources using SA messages	import-source [acl <i>acl-number</i>]	Optional By default, all the (S, G) entries in the domain are advertised in the SA message.

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. 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 if the TTL in its IP header is greater than the threshold; therefore, you can control the forwarding range of SA messages that carry encapsulated data by configuring the TTL threshold.

Follow these steps to configure a rule for filtering received and forwarded SA messages:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter MSDP view	msdp	—

To do...	Use the command...	Remarks
Configure to filter imported and exported SA messages	peer <i>peer-address</i> sa-policy { import export } [acl <i>acl-number</i>]	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 required for a multicast packet to be sent to the specified MSDP peer	peer <i>peer-address</i> minimum-ttl <i>tvl-value</i>	Optional By default, the value of TTL threshold is 0.

Displaying and Maintaining MSDP

Displaying and maintaining MSDP

To do...	Use the command...	Remarks
Display the brief information of MSDP peer state	display msdp brief	Available in any view
Display the detailed information of MSDP peer status	display msdp peer-status [<i>peer-address</i>]	Available in any view
Display the (S, G) state learned from MSDP peers	display msdp sa-cache [<i>group-address</i> <i>source-address</i> <i>as-number</i>] *	Available in any view
Display the number of sources and groups in the MSDP cache	display msdp sa-count [<i>autonomous-system-number</i>]	Available in any view
Reset the TCP connection with the specified MSDP peer	reset msdp peer <i>peer-address</i>	Available in user view
Clear the cached SA messages	reset msdp sa-cache [<i>group-address</i>]	Available in user view
Clear the statistics information of the specified MSDP peer without resetting the MSDP peer	reset msdp statistics [<i>peer-address</i>]	Available in user view

Tracing the transmission path of an SA message over the network

Follow these steps to trace the transmission path of an SA message over the network:

To do...	Use the command...	Remarks
Trace the transmission path of an SA message over the network	msdp-tracert <i>source-address</i> <i>group-address</i> <i>rp-address</i> [max-hops <i>max-hops</i>] [next-hop-info sa-info peer-info] * [skip-hops <i>skip-hops</i>]	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 <i>source-address</i> [<i>group-address</i> <i>last-hop-router-address</i> <i>group-address</i>]	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.

MSDP Configuration Example

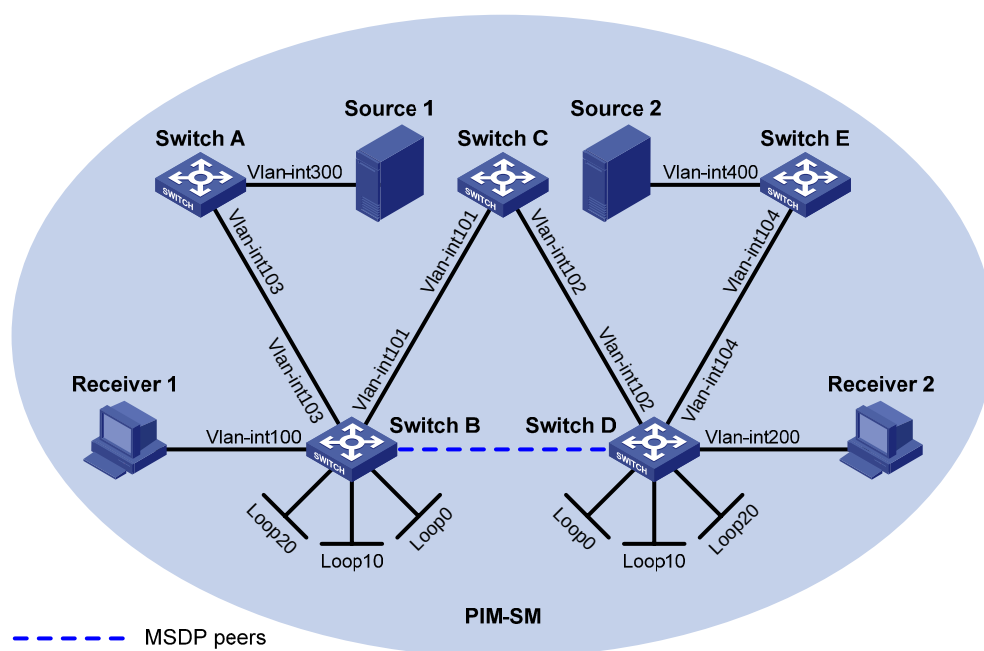
Anycast RP Configuration

Network requirements

- The PIM-SM domain has multiple multicast sources and receivers. OSPF runs within the domain to provide unicast routes.
- It is required to configure the anycast RP feature so that the receiver-side DRs and the source-side DRs can initiate a Join message to their respective RPs that are the topologically nearest to them.
- On Switch B and Switch D, configure the interface Loopback 10 as a C-BSR, and Loopback 20 as a C-RP.
- The router ID of Switch B is 1.1.1.1, while the router ID of Switch D is 2.2.2.2. Set up an MSDP peering relationship between Switch B and Switch D.

Network diagram

Figure 5-5 Network diagram for anycast RP configuration



Device	Interface	IP address	Device	Interface	IP address
Source 1	—	10.110.5.100/24	Switch C	Vlan-int101	192.168.1.2/24
Source 2	—	10.110.6.100/24		Vlan-int102	192.168.2.2/24
Switch A	Vlan-int300	10.110.5.1/24	Switch D	Vlan-int200	10.110.3.1/24
	Vlan-int103	10.110.2.2/24		Vlan-int104	10.110.4.1/24
Switch B	Vlan-int100	10.110.1.1/24		Vlan-int102	192.168.2.1/24
	Vlan-int103	10.110.2.1/24		Loop0	2.2.2.2/32
	Vlan-int101	192.168.1.1/24		Loop10	4.4.4.4/32
	Loop0	1.1.1.1/32		Loop20	10.1.1.1/32
	Loop10	3.3.3.3/32	Switch E	Vlan-int400	10.110.6.1/24
	Loop20	10.1.1.1/32		Vlan-int104	10.110.4.2/24

Configuration procedure

- 1) Configure the interface IP addresses and unicast routing protocol for each switch

Configure the IP address and subnet mask for each interface as per [Figure 5-5](#). Detailed configuration steps are omitted here.

Configure OSPF for interconnection between the switches. Ensure the network-layer interoperability among the switches, and ensure the dynamic update of routing information between the switches through a unicast routing protocol. Detailed configuration steps are omitted here.

- 2) Enable IP multicast routing, and enable PIM-SM and IGMP

Enable IP multicast routing on Switch B, enable PIM-SM on each interface, and enable IGMP on the host-side interface VLAN-interface 100.

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp enable
[SwitchB-Vlan-interface100] pim sm
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] pim sm
[SwitchB-Vlan-interface103] quit
[SwitchB] interface Vlan-interface 101
[SwitchB-Vlan-interface101] pim sm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface loopback 0
[SwitchB-LoopBack0] pim sm
[SwitchB-LoopBack0] quit
[SwitchB] interface loopback 10
[SwitchB-LoopBack10] pim sm
[SwitchB-LoopBack10] quit
[SwitchB] interface loopback 20
[SwitchB-LoopBack20] pim sm
[SwitchB-LoopBack20] quit
```

The configuration on Switch A, Switch C, Switch D, and Switch E is similar to the configuration on Switch B.

- 3) Configure C-BSRs and C-RPs.

Configure Loopback 10 as a C-BSR and configure Loopback 20 as a C-RP on Switch B.

```
[SwitchB] pim
[SwitchB-pim] c-bsr loopback 10 24
[SwitchB-pim] c-rp loopback 20
[SwitchB-pim] quit
```

The configuration on Switch D is similar to the configuration on Switch B.

- 4) Configure MSDP peers

Configure an MSDP peer on Loopback 0 of Switch B.

```
[SwitchB] msdp
[SwitchB-msdp] originating-rp loopback 0
```

```
[SwitchB-msdp] peer 2.2.2.2 connect-interface loopback 0
[SwitchB-msdp] quit
```

Configure an MSDP peer on Loopback 0 of Switch D.

```
[SwitchD] msdp
[SwitchD-msdp] originating-rp loopback 0
[SwitchD-msdp] peer 1.1.1.1 connect-interface loopback 0
[SwitchD-msdp] quit
```

5) Verify the configuration

You can use the **display msdp brief** command to view the brief information of MSDP peering relationships between the switches.

View the brief MSDP peer information on Switch B.

```
[SwitchB] display msdp brief
MSDP Peer Brief Information
```

Peer's Address	State	Up/Down time	AS	SA Count	Reset Count
2.2.2.2	Up	00:48:21	?	2	0

View the brief MSDP peer information on Switch D.

```
[SwitchD] display msdp brief
MSDP Peer Brief Information
```

Peer's Address	State	Up/Down time	AS	SA Count	Reset Count
1.1.1.1	Up	00:50:22	?	2	0

When Source 1 (10.110.5.100/24) sends multicast data to multicast group G (225.1.1.1), Receiver 1 joins multicast group G. By comparing the PIM routing information displayed on Switch B with that displayed on Switch D, you can see that Switch B now acts as the RP for Source 1 and Receiver 1. Source 1 registers with Switch B and Receiver 1 sends a join message to Switch B.

View the PIM routing information on Switch B.

```
[Switch B] display pim routing-table
PIM-SM Routing Table
Total 1 (S,G) entry, 1 (*,G) entry, 0 (*,*,RP) entry
(*, 225.1.1.1), RP 10.1.1.1
  Protocol 0x20: PIMSM, Flag 0x2003: RPT WC NULL_IIF
  Uptime: 00:00:13, never timeout
  Upstream interface: Null, RPF neighbor: 0.0.0.0
  Downstream interface list:
    Vlan-interface100, Protocol 0x1: IGMP, never timeout

(10.110.5.100, 225.1.1.1)
  Protocol 0x20: PIMSM, Flag 0x4: SPT
  Uptime: 00:03:08, Timeout in 206 sec
  Upstream interface: Vlan-interface103, RPF neighbor: NULL
  Downstream interface list:
    Vlan-interface100, Protocol 0x1: IGMP, never timeout
```

```
Matched 1 (S,G) entry, 1 (*,G) entry, 0 (*,*,RP) entry
```

View the PIM routing information on Switch D.

```
[SwitchD] display pim routing-table
```

PIM-SM Routing Table

Total 0 (S,G) entry, 0 (*,G) entry, 0 (*,*,RP) entry

Matched 0 (S,G) entry, 0 (*,G) entry, 0 (*,*,RP) entry

Troubleshooting MSDP Configuration

MSDP Peer Always in the Down State

Symptom

An MSDP peer is configured, but it is always in the down state.

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.

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.

No SA Entry in the SA Cache of the Router

Symptom

An MSDP fails to send (S, G) forwarding entries through an SA message.

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.

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.

6 IGMP Snooping Configuration

When configuring IGMP snooping, go to these sections for information you are interested in:

- [IGMP Snooping Overview](#)
- [Configuring IGMP Snooping](#)
- [Displaying and Maintaining IGMP Snooping](#)
- [IGMP Snooping Configuration Examples](#)
- [Troubleshooting IGMP Snooping](#)



Note

In this manual, the term “router” refers to a router in the generic sense or a Layer 3 Ethernet switch running an IP multicast protocol.

IGMP Snooping Overview

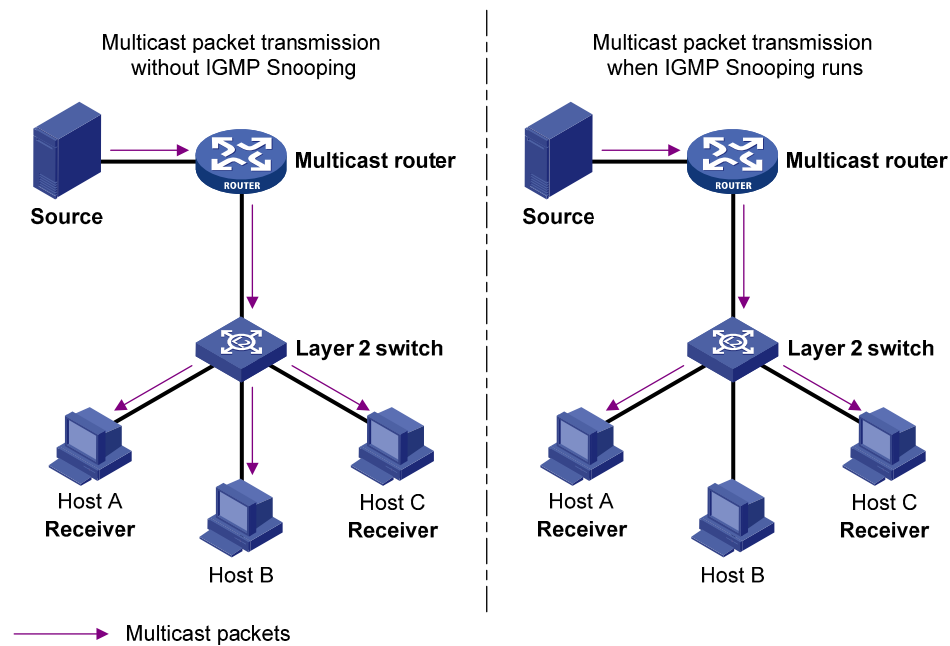
Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

Principle of IGMP Snooping

By analyzing received IGMP messages, a Layer 2 device running IGMP Snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings.

As shown in [Figure 6-1](#), when IGMP Snooping is not running on the switch, multicast packets are broadcast to all devices at Layer 2. When IGMP Snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than broadcast to all hosts, at Layer 2. However, multicast packets for unknown multicast groups are still broadcast at Layer 2.

Figure 6-1 Before and after IGMP Snooping is enabled on Layer 2 device

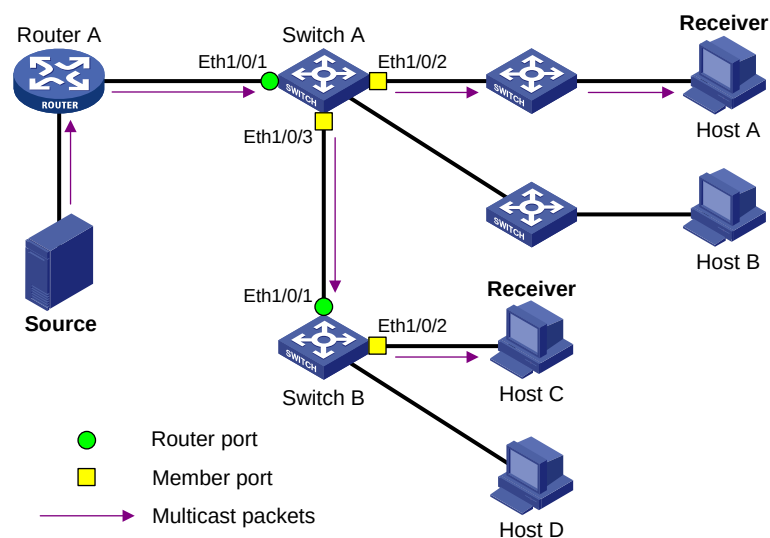


Basic Concepts in IGMP Snooping

IGMP Snooping related ports

As shown in [Figure 6-2](#), Router A connects to the multicast source, IGMP Snooping runs on Switch A and Switch B, Host A and Host C are receiver hosts (namely, multicast group members).

Figure 6-2 IGMP Snooping related ports



Ports involved in IGMP Snooping, as shown in [Figure 6-2](#), are described as follows:

- Router port: A router port is a port on the Layer 3 multicast device (DR or IGMP querier) side of the Ethernet switch. In the figure, Ethernet 1/0/1 of Switch A and Ethernet 1/0/1 of Switch B are router ports. A switch registers all its local router ports in its router port list.
- Member port: A member port is a port on the multicast group member side of the Ethernet switch. In the figure, Ethernet 1/0/2 and Ethernet 1/0/3 of Switch A and Ethernet 1/0/2 of Switch B are

member ports. The switch records all member ports on the local device in the IGMP Snooping forwarding table.

Port aging timers in IGMP Snooping and related messages and actions

Table 6-1 Port aging timers in IGMP Snooping and related messages and actions

Timer	Description	Message before expiry	Action after expiry
Router port aging timer	For each router port, the switch sets a timer initialized to the aging time of the route port	IGMP general query or PIM hello	The switch removes this port from its router port list
Member port aging timer	When a port joins a multicast group, the switch sets a timer for the port, which is initialized to the member port aging time	IGMP membership report	The switch removes this port from the multicast group forwarding table

Work Mechanism of IGMP Snooping

A switch running IGMP Snooping performs different actions when it receives different IGMP messages, as follows:

When receiving a general query

The IGMP querier periodically sends IGMP general queries to all hosts and routers on the local subnet to find out whether active multicast group members exist on the subnet.

Upon receiving an IGMP general query, the switch forwards it through all ports in the VLAN except the receiving port and performs the following to the receiving port:

- If the receiving port is a router port existing in its router port list, the switch resets the aging timer of this router port.
- If the receiving port is not a router port existing in its router port list, the switch adds it into its router port list and sets an aging timer for this router port.

When receiving a membership report

A host sends an IGMP report to the multicast router in the following circumstances:

- Upon receiving an IGMP query, a multicast group member host responds with an IGMP report.
- When intended to join a multicast group, a host sends an IGMP report to the multicast router to announce that it is interested in the multicast information addressed to that group.

Upon receiving an IGMP report, the switch forwards it through all the router ports in the VLAN, resolves the address of the multicast group the host is interested in, and performs the following to the receiving port:

- If the port is already in the forwarding table, the switch resets the member port aging timer of the port.
- If the port is not in the forwarding table, the switch installs an entry for this port in the forwarding table and starts the member port aging timer of this port.



Note

A switch will not forward an IGMP report through a non-router port for the following reason: Due to the IGMP report suppression mechanism, if member hosts of that multicast group still exist under non-router ports, the hosts will stop sending reports when they receive the message, and this prevents the switch from knowing if members of that multicast group are still attached to these ports.

For the description of IGMP report suppression mechanism, refer to [Work Mechanism of IGMPv1](#).

When receiving a leave message

When an IGMPv1 host leaves a multicast group, the host does not send an IGMP leave message, so the switch cannot know immediately that the host has left the multicast group. However, as the host stops sending IGMP reports as soon as it leaves a multicast group, the switch deletes the forwarding entry for the member port corresponding to the host from the forwarding table when its aging timer expires.

When an IGMPv2 or IGMPv3 host leaves a multicast group, the host sends an IGMP leave message to the multicast router to announce that it has left the multicast group.

Upon receiving an IGMP leave message on the last member port, a switch forwards it out all router ports in the VLAN. Because the switch does not know whether any other member hosts of that multicast group still exists under the port to which the IGMP leave message arrived, the switch does not immediately delete the forwarding entry corresponding to that port from the forwarding table; instead, it resets the aging timer of the member port.

Upon receiving the IGMP leave message from a host, the IGMP querier resolves from the message the address of the multicast group that the host just left and sends an IGMP group-specific query to that multicast group through the port that received the leave message. Upon receiving the IGMP group-specific query, a switch forwards it through all the router ports in the VLAN and all member ports of that multicast group, and performs the following to the receiving port:

- If any IGMP report in response to the group-specific query arrives to the member port before its aging timer expires, this means that some other members of that multicast group still exist under that port: the switch resets the aging timer of the member port.
- If no IGMP report in response to the group-specific query arrives to the member port before its aging timer expires as a response to the IGMP group-specific query, this means that no members of that multicast group still exist under the port: the switch deletes the forwarding entry corresponding to the port from the forwarding table when the aging timer expires.



Caution

After an Ethernet switch enables IGMP Snooping, when it receives the IGMP leave message sent by a host in a multicast group, it judges whether the multicast group exists automatically. If the multicast group does not exist, the switch drops this IGMP leave message.

Configuring IGMP Snooping

Complete the following tasks to configure IGMP Snooping:

Task	Remarks
Enabling IGMP Snooping	Required
Configuring the Version of IGMP Snooping	Optional
Configuring Timers	Optional
Configuring Fast Leave Processing	Optional
Configuring a Multicast Group Filter	Optional
Configuring the Maximum Number of Multicast Groups on a Port	Optional
Configuring IGMP Snooping Querier	Optional
Suppressing Flooding of Unknown Multicast Traffic in a VLAN	Optional
Configuring Static Member Port for a Multicast Group	Optional
Configuring a Static Router Port	Optional
Disabling a Port from Becoming a Router Port	Optional
Configuring a Port as a Simulated Group Member	Optional
Configuring a VLAN Tag for Query Message	Optional
Configuring Multicast VLAN	Optional

Enabling IGMP Snooping

Follow these steps to enable IGMP Snooping:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable IGMP Snooping globally	igmp-snooping enable	Required By default, IGMP Snooping is disabled globally.
Enter VLAN view	vlan <i>vlan-id</i>	—
Enable IGMP Snooping on the VLAN	igmp-snooping enable	Required By default, IGMP Snooping is disabled on all the VLANs.



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 enabling IGMP Snooping in a VLAN, be sure to enable IGMP Snooping globally in system view; otherwise the IGMP Snooping settings will not take effect.
- If IGMP Snooping and VLAN VPN are enabled on a VLAN at the same time, IGMP queries are likely to fail to pass the VLAN. You can solve this problem by configuring VLAN tags for queries. For details, see [Configuring a VLAN Tag for Query Messages](#).

Configuring the Version of IGMP Snooping

By configuring an IGMP snooping version, you actually configure the version of IGMP messages that IGMP snooping can process.

- IGMP snooping version 2 can process IGMPv1 and IGMPv2 messages, but not IGMPv3 messages, which will be flooded in the VLAN.
- IGMP snooping version 3 can process IGMPv1, IGMPv2 and IGMPv3 messages..

Follow these steps to configure the version of IGMP Snooping:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN view	vlan <i>vlan-id</i>	—
Configure the version of IGMP Snooping	igmp-snooping version <i>version-number</i>	Optional The default IGMP Snooping version is version 2.



Caution

- Before configuring related IGMP Snooping functions, you must enable IGMP Snooping in the specified VLAN.
- Different multicast group addresses should be configured for different multicast sources because IGMPv3 Snooping cannot distinguish multicast data from different sources to the same multicast group.

Configuring Timers

This section describes how to configure the aging timer of the router port, the aging timer of the multicast member ports, and the query response timer.

Follow these steps to configure timers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the aging timer of the router port	igmp-snooping router-aging-time <i>seconds</i>	Optional By default, the aging time of the router port is 105 seconds.
Configure the general query response timer	igmp-snooping max-response-time <i>seconds</i>	Optional By default, the general query response timeout time is 10 seconds.
Configure the aging timer of the multicast member port	igmp-snooping host-aging-time <i>seconds</i>	Optional By default, the aging time of multicast member ports is 260 seconds

Configuring Fast Leave Processing

With fast leave processing enabled, when the switch receives an IGMP leave message on a port, the switch directly removes that port from the forwarding table entry for the specific group.

If only one host is attached to the port, enable fast leave processing helps improve bandwidth and resource usage. If fast leave processing and unknown multicast packet dropping or non-flooding are enabled on a port to which more than one host is connected, when one host leaves a multicast group, the other hosts connected to port and interested in the same multicast group will fail to receive multicast data for that group.

Enabling fast leave processing in system view

Follow these steps to enable fast leave processing in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable fast leave processing	igmp-snooping fast-leave [vlan <i>vlan-list</i>]	Required By default, the fast leave processing feature is disabled.

Enabling fast leave processing in Ethernet port view

Follow these steps to enable fast leave processing in Ethernet view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable fast leave processing for specific VLANs	igmp-snooping fast-leave [vlan <i>vlan-list</i>]	Required By default, the fast leave processing feature is disabled.



Note

- The fast leave processing function works for a port only if the host attached to the port runs IGMPv2 or IGMPv3.
- The configuration performed in system view takes effect on all ports of the switch if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on all ports in the specified VLAN(s).
- The configuration performed in Ethernet port view takes effect on the port no matter which VLAN it belongs to if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on the port only if the port belongs to the specified VLAN(s).

Configuring a Multicast Group Filter

On an IGMP Snooping-enabled switch, the configuration of a multicast group allows the service provider to define restrictions on multicast programs available to different users.

In an actual application, when a user requests a multicast program, the user's host initiates an IGMP report. Upon receiving this report message, the switch checks the report against the ACL rule configured on the receiving port. If the receiving port can join this multicast group, the switch adds this port to the IGMP Snooping multicast group list; otherwise the switch drops this report message. Any multicast data that has failed the ACL check will not be sent to this port. In this way, the service provider can control the VOD programs provided for multicast users.

Make sure that an ACL rule has been configured before configuring this feature.

Configuring a multicast group filter in system view

Follow these steps to configure a multicast group filter in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a multicast group filter	igmp-snooping group-policy <i>acl-number [vlan vlan-list]</i>	Required No group filter is configured by default, namely hosts can join any multicast group.

Configuring a multicast group filter in Ethernet port view

Follow these steps to configure a multicast group filter in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure a multicast group filter	igmp-snooping group-policy <i>acl-number [vlan vlan-list]</i>	Optional No group filter is configured by default, namely hosts can join any multicast group.



Note

- A port can belong to multiple VLANs, you can configure only one ACL rule per VLAN on a port.
- If no ACL rule is configured, all the multicast groups will be filtered.
- Since most devices broadcast unknown multicast packets by default, this function is often used together with the function of dropping unknown multicast packets to prevent multicast streams from being broadcast as unknown multicast packets to a port blocked by this function.
- The configuration performed in system view takes effect on all ports of the switch if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on all ports in the specified VLAN(s).
- The configuration performed in Ethernet port view takes effect on the port no matter which VLAN it belongs to if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on the port only if the port belongs to the specified VLAN(s).

Configuring the Maximum Number of Multicast Groups on a Port

By configuring the maximum number of multicast groups that can be joined on a port, you can limit the number of multicast programs on-demand available to users, thus to regulate traffic on the port.

Follow these steps to configure the maximum number of multicast groups on a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Limit the number of multicast groups on a port	igmp-snooping group-limit <i>limit</i> [vlan <i>vlan-list</i> [overflow-replace]]	Required The maximum number of multicast groups on a port is 256 by default.



Note

- To prevent bursting traffic in the network or performance deterioration of the device caused by excessive multicast groups, you can set the maximum number of multicast groups that the switch should process.
- When the number of multicast groups exceeds the configured limit, the switch removes its multicast forwarding entries starting from the oldest one. In this case, the multicast packets for the removed multicast group(s) will be flooded in the VLAN as unknown multicast packets. As a result, non-member ports can receive multicast packets within a period of time. To avoid this from happening, enable the function of dropping unknown multicast packets.
- If an Ethernet port is a static member port for a multicast group, the configuration of the maximum number of multicast groups that can be joined does not take effect on the port.

Configuring IGMP Snooping Querier

In an IP multicast network running IGMP, a multicast router is responsible for sending IGMP general queries, so that all Layer 3 multicast devices can establish and maintain multicast forwarding entries, thus to forward multicast traffic correctly at the network layer. This router or Layer 3 switch is called IGMP querier.

Upon receiving an IGMP query with the source IP address 0.0.0.0 on a port, the switch does not enlist that port as a dynamic router port. This may prevent multicast forwarding entries from being correctly created at the data link layer and cause multicast traffic forwarding failure in the end. When a Layer 2 device acts as an IGMP-Snooping querier, to avoid the aforesaid problem, configure a non-all-zero IP address as the source IP address of IGMP queries.

IGMP Snooping querier related configurations include:

- Enabling IGMP Snooping querier,
- Configuring the IGMP query interval, and
- Configuring the source address to be carried in IGMP general and group specific queries..

Enabling IGMP Snooping querier

Follow these steps to enable IGMP Snooping querier:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable IGMP Snooping	igmp-snooping enable	Required By default, IGMP Snooping is disabled.
Enter VLAN view	vlan <i>vlan-id</i>	—
Enable IGMP Snooping	igmp-snooping enable	Required By default, IGMP Snooping is disabled.
Enable IGMP Snooping querier	igmp-snooping querier	Required By default, IGMP Snooping querier is disabled.

Configuring IGMP query interval

Follow these steps to configure IGMP query interval:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN view	vlan <i>vlan-id</i>	—
Configure the IGMP query interval	igmp-snooping query-interval <i>seconds</i>	Optional 60 seconds by default.

Configuring the source address to be carried in IGMP queries

Follow these steps to configure the source address to be carried in IGMP queries:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN view	vlan <i>vlan-id</i>	—
Configure the source IP address of IGMP general queries	igmp-snooping general-query source-ip { current-interface <i>ip-address</i> }	Optional 0.0.0.0 by default
Configure the source IP address of IGMP group-specific queries	igmp-snooping special-query source-ip { current-interface <i>ip-address</i> }	0.0.0.0 by default

Suppressing Flooding of Unknown Multicast Traffic in a VLAN

With IGMP Snooping enabled in a VLAN, multicast traffic for unknown multicast groups is flooded within the VLAN by default. This wastes network bandwidth and affects multicast forwarding efficiency.

With the unknown multicast flooding suppression function enabled, when receiving a multicast packet for an unknown multicast group, an IGMP Snooping switch creates a nonflooding entry and relays the packet to router ports only, instead of flooding the packet within the VLAN. If the switch has no router ports, it drops the multicast packet.

Follow these steps to suppress flooding of unknown multicast traffic in the VLAN:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable unknown multicast flooding suppression	igmp-snooping nonflooding-enable	Required By default, unknown multicast flooding suppression



Note

- If the function of dropping unknown multicast packets or the IRF fabric function is enabled, you cannot enable unknown multicast flooding suppression.
- Unknown multicast flooding suppression and multicast source port suppression cannot take effect at the same time. If both are enabled, only multicast source port suppression takes effect. In this case, multicast data received on the blocked port will be dropped.

Configuring Static Member Port for a Multicast Group

If the host connected to a port is interested in the multicast data for a specific group, you can configure that port as a static member port for that multicast group.

In Ethernet port view

Follow these steps to configure a static multicast group member port in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the current port as a static member port for a multicast group in a VLAN	multicast static-group <i>group-address</i> vlan <i>vlan-id</i>	Required By default, no port is configured as a static multicast group member port.

In VLAN interface view

Follow these steps to configure a static multicast group member port in VLAN interface view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface vlan-interface <i>interface-number</i>	—
Configure specified port(s) as static member port(s) of a multicast group in the VLAN	multicast static-group <i>group-address</i> interface <i>interface-list</i>	Required By default, no port is configured as a static multicast group member port.



Caution

- You can configure up to 200 static member ports on an S3600 series switch.
- If a port has been configured as an IRF fabric port or a reflect port, it cannot be configured as a static member port.

Configuring a Static Router Port

In a network where the topology is unlikely to change, you can configure a port on the switch as a static router port, so that the switch has a static connection to a multicast router and receives IGMP messages from that router.

In Ethernet port view

Follow these steps to configure a static router port in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the current port as a static router port	multicast static-router-port vlan <i>vlan-id</i>	Required By default, no static router port is configured.

In VLAN view

Follow these steps to configure a static router port in VLAN view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN view	vlan <i>vlan-id</i>	—
Configure a specified port as a static router port	multicast static-router-port <i>interface-type interface-number</i>	Required By default, no static router port is configured.

Disabling a Port from Becoming a Router Port

A MAC-forced forwarding (MFF) network isolates hosts at Layer 2 and allows multicast packets to pass through user ports. However, the following case may occur:

If host A joins a multicast group, it sends IGMP membership reports, and then the switch connected to it forwards the messages out every router port. If the user port on the switch connecting to host B becomes a router port, host B may receive the IGMP membership report, and thus obtain other information of host A from the message.

To avoid this, you can disable a port of the S3600 series switches from becoming a router port so that this port will not forward IGMP membership report messages.

Follow these steps to disable a port from becoming a router port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Disable the port from becoming a router port	igmp-snooping query-pkt-deny	Required Not disabled by default.



Note

- This feature is recommended in MFF networks only.
- For details about MFF, refer to *ARP Operation*.

Configuring a Port as a Simulated Group Member

Simulated joining in IGMP Snooping is implemented in the same way as in IGMP except that IGMP Snooping establishes and maintains IGMP Snooping entries.

Enabling simulated joining in VLAN interface view

Follow these steps to enable simulated joining in VLAN interface view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface <i>Vlan-interface interface-number</i>	—
Enable simulated joining	igmp host-join <i>group-address</i> [source-ip <i>source-address</i>] port <i>interface-list</i>	Required Disabled by default

Configuring simulated joining in Ethernet port view

Follow these steps to configure a port as a simulated group member:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type interface-number</i>	—
Configure the current port as a simulated multicast group member	igmp host-join <i>group-address</i> [source-ip <i>source-address</i>] vlan <i>vlan-id</i>	Required Simulated joining is disabled by default.



Caution

- Before configuring a simulated host, enable IGMP Snooping in VLAN view first.
- The port to be configured must belong to the specified VLAN; otherwise the configuration does not take effect.
- You can use the source-ip source-address command to specify a multicast source address that the port will join as a simulated host. This configuration takes effect when IGMPv3 Snooping is enabled in the VLAN.

Configuring a VLAN Tag for Query Messages

By configuring the VLAN tag carried in IGMP general and group-specific queries forwarded and sent by IGMP Snooping switches, you can enable multicast packet forwarding between different VLANs in a Layer-2 multicast network environment.

Follow these steps to configure VLAN tag for query message:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a VLAN tag for query messages	igmp-snooping vlan-mapping <i>vlan vlan-id</i>	Required By default, the VLAN tag in IGMP general and group-specific query messages is not changed.



Note

It is not recommended to configure this function while the multicast VLAN function is in effect.

Configuring Multicast VLAN

In traditional multicast implementations, when users in different VLANs listen to the same multicast group, the multicast data is copied on the multicast router for each VLAN that contains receivers. This is a big waste of network bandwidth.

In an IGMP Snooping environment, by configuring a multicast VLAN and adding ports to the multicast VLAN, you can allow users in different VLANs to share the same multicast VLAN. This saves bandwidth because multicast streams are transmitted only within the multicast VLAN. In addition, because the multicast VLAN is isolated from user VLANs, this method also enhances the information security.

Multicast VLAN is mainly used in Layer 2 switching, but you must make the corresponding configurations on the Layer 3 switch.

Follow these steps to configure multicast VLAN on the Layer 3 switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a multicast VLAN and enter VLAN view	vlan <i>vlan-id</i>	—
Return to system view	quit	—
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	—
Enable IGMP	igmp enable	Required By default, the IGMP feature is disabled.
Return to system view	quit	—
Enter Ethernet port view for the Layer 2 switch to be configured	interface <i>interface-type</i> <i>interface-number</i>	—
Define the port as a trunk or hybrid port	port link-type { trunk hybrid }	Required
Specify the VLANs to be allowed to pass the Ethernet port	port hybrid vlan <i>vlan-id-list</i> { tagged untagged }	Required The multicast VLAN defined on the Layer 2 switch must be included, and the port must be configured to forward tagged packets for the multicast VLAN if the port type is hybrid.
	port trunk permit vlan <i>vlan-list</i>	

Follow these steps to configure multicast VLAN on the Layer 2 switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable IGMP Snooping	igmp-snooping enable	—

To do...	Use the command...	Remarks
Enter VLAN view	vlan <i>vlan-id</i>	—
Enable IGMP Snooping	igmp-snooping enable	Required
Enable multicast VLAN	service-type multicast	Required
Return to system view	quit	—
Enter Ethernet port view for the Layer 3 switch	interface <i>interface-type</i> <i>interface-number</i>	—
Define the port as a trunk or hybrid port	port link-type { trunk hybrid }	Required
Specify the VLANs to be allowed to pass the Ethernet port	port hybrid vlan <i>vlan-list</i> { tagged untagged }	Required The multicast VLAN must be included, and the port must be configured to forward tagged packets for the multicast VLAN if the port type is hybrid.
	port trunk permit vlan <i>vlan-list</i>	
Enter Ethernet port view for a user device	interface <i>interface-type</i> <i>interface-number</i>	—
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 <i>vlan-id-list</i> { tagged untagged }	Required The multicast VLAN must be included, and the port must be configured to forward tagged packets for the multicast VLAN.



Note

- One port can belong to only one multicast VLAN.
- The port connected to a user terminal must be a hybrid port.
- The multicast member ports must be in the same VLAN with the router port. Otherwise, the multicast member port cannot receive multicast packets.
- If a router port is in a multicast VLAN, the router port must be configured as a trunk port or a hybrid port that allows tagged packets to pass for the multicast VLAN. Otherwise, all the multicast member ports in this multicast VLAN cannot receive multicast packets.
- The multicast VLAN function and the VLAN mapping function cannot be configured at the same time.

Displaying and Maintaining IGMP Snooping

To do...	Use the command...	Remarks
Display the current IGMP Snooping configuration	display igmp-snooping configuration	Available in any view
Display IGMP Snooping message statistics	display igmp-snooping statistics	Available in any view

To do...	Use the command...	Remarks
Display the information about IP and MAC multicast groups in one or all VLANs	display igmp-snooping group [vlan <i>vlan-id</i>]	Available in any view
Clear IGMP Snooping statistics	reset igmp-snooping statistics	Available in user view

IGMP Snooping Configuration Examples

Configuring IGMP Snooping

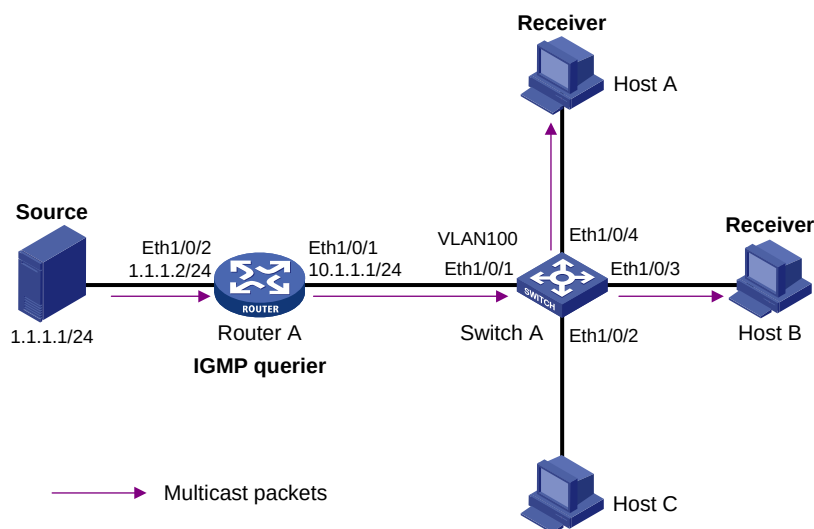
Network requirements

To prevent multicast traffic from being flooded at Layer 2, enable IGMP snooping on Layer 2 switches.

- As shown in [Figure 6-3](#), Router A connects to a multicast source (Source) through Ethernet 1/0/2, and to Switch A through Ethernet 1/0/1.
- Run PIM-DM and IGMP on Router A. Run IGMP snooping on Switch A. Router A acts as the IGMP querier.
- The multicast source sends multicast data to the multicast group 224.1.1.1. Host A and Host B are receivers of the multicast group 224.1.1.1.

Network diagram

Figure 6-3 Network diagram for IGMP Snooping configuration



Configuration procedure

- 1) Configure the IP address of each interface

Configure an IP address and subnet mask for each interface as per [Figure 6-3](#). The detailed configuration steps are omitted.

- 2) Configure Router A

Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on Ethernet 1/0/1.

```
<RouterA> system-view
```

```
[RouterA] multicast routing-enable
```

```
[RouterA] interface Ethernet 1/0/1
[RouterA-Ethernet1/0/1] igmp enable
[RouterA-Ethernet1/0/1] pim dm
[RouterA-Ethernet1/0/1] quit
[RouterA] interface Ethernet 1/0/2
[RouterA-Ethernet1/0/2] pim dm
[RouterA-Ethernet1/0/2] quit
```

3) Configure Switch A

Enable IGMP Snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
    Enable IGMP-Snooping ok.
```

Create VLAN 100, assign Ethernet 1/0/1 through Ethernet 1/0/4 to this VLAN, and enable IGMP Snooping in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port Ethernet 1/0/1 to Ethernet 1/0/4
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
```

4) Verify the configuration

View the detailed information of the multicast group in VLAN 100 on Switch A.

```
<SwitchA> display igmp-snooping group vlan100
    Total 1 IP Group(s).
    Total 1 MAC Group(s).

Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Static Router port(s):
    Dynamic Router port(s):
        Ethernet1/0/1
    IP group(s):the following ip group(s) match to one mac group.
        IP group address: 224.1.1.1
        Static host port(s):
        Dynamic host port(s):
            Ethernet1/0/3          Ethernet1/0/4
    MAC group(s):
        MAC group address: 0100-5e01-0101
        Host port(s): Ethernet1/0/3          Ethernet1/0/4
```

As shown above, the multicast group 224.1.1.1 has been registered on Switch A, with the dynamic router port Ethernet 1/0/1 and dynamic member ports Ethernet 1/0/3 and Ethernet 1/0/4. This means that Host A and Host B have joined the multicast group 224.1.1.1.

Configuring Multicast VLAN

Network requirements

As shown in [Figure 6-4](#), Workstation is a multicast source. Switch A forwards multicast data from the multicast source. A Layer 2 switch, Switch B forwards the multicast data to the end users Host A and Host B.

[Table 6-2](#) describes the network devices involved in this example and the configurations you should make on them.

Table 6-2 Network devices and their configurations

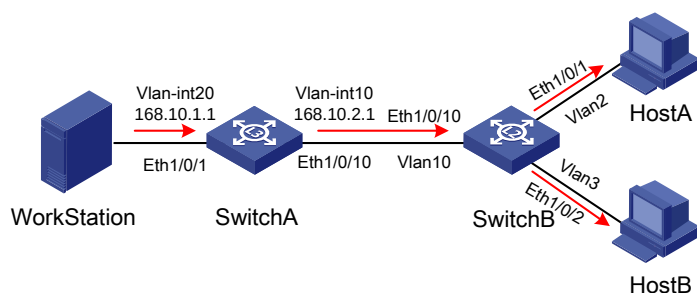
Device	Device description	Networking description
Switch A	Layer 3 switch	The interface IP address of VLAN 20 is 168.10.1.1. Ethernet 1/0/1 is connected to the workstation and belongs to VLAN 20. The interface IP address of VLAN 10 is 168.10.2.1. Ethernet 1/0/10 belongs to VLAN 10. Ethernet 1/0/10 is connected to Switch B.
Switch B	Layer 2 switch	• VLAN 2 contains Ethernet 1/0/1 and VLAN 3 contains Ethernet 1/0/2. • The default VLANs of Ethernet 1/0/1 and Ethernet 1/0/2 are VLAN 2 and VLAN 3 respectively. • VLAN 10 contains Ethernet 1/0/10, Ethernet 1/0/1, and Ethernet 1/0/2. Ethernet 1/0/10 is connected to Switch A. • VLAN 10 is a multicast VLAN. • Ethernet 1/0/1 sends untagged packets for VLAN 2 and VLAN 10. • Ethernet 1/0/2 sends untagged packets for VLAN 3 and VLAN 10.
Host A	User 1	Host A is connected to Ethernet 1/0/1 on Switch B.
Host B	User 2	Host B is connected to Ethernet 1/0/2 on Switch B.

In this configuration example, you need to configure the ports that connect Switch A and Switch B to each other as hybrid ports. The following text describes the configuration details. You can also configure these ports as trunk ports. The configuration procedure is omitted here. For details, see [Configuring Multicast VLAN](#).

Configure a multicast VLAN, so that users in VLAN 2 and VLAN 3 can receive multicast streams through the multicast VLAN.

Network diagram

Figure 6-4 Network diagram for multicast VLAN configuration



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 PIM DM on the VLAN interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] vlan 20
[SwitchA-vlan20] port Ethernet 1/0/1
[SwitchA-vlan20] quit
[SwitchA] 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 VLAN 10.

```
[SwitchA] vlan 10
[SwitchA-vlan10] quit
```

Define Ethernet 1/0/10 as a hybrid port, add the port to VLAN 10, and configure the port to forward tagged packets for VLAN 10.

```
[SwitchA] interface Ethernet 1/0/10
[SwitchA-Ethernet1/0/10] port link-type hybrid
[SwitchA-Ethernet1/0/10] port hybrid vlan 10 tagged
[SwitchA-Ethernet1/0/10] quit
```

Configure the interface IP address of VLAN 10 as 168.10.2.1, and enable PIM-DM and IGMP.

```
[SwitchA] interface Vlan-interface 10
[SwitchA-Vlan-interface10] ip address 168.10.2.1 255.255.255.0
[SwitchA-Vlan-interface10] igmp enable
[SwitchA-Vlan-interface10] pim dm
```

2) Configure Switch B:

Enable the IGMP Snooping feature on Switch B.

```
<SwitchB> system-view
[SwitchB] igmp-snooping enable
```

Create VLAN 2, VLAN 3 and VLAN 10, configure VLAN 10 as the multicast VLAN, and then enable IGMP Snooping on it.

```
[SwitchB] vlan 2 to 3
```

Please wait.... Done.

```
[SwitchB] vlan 10
```

```
[SwitchB-vlan10] service-type multicast
```

```
[SwitchB-vlan10] igmp-snooping enable
```

```
[SwitchB-vlan10] quit
```

Define Ethernet 1/0/10 as a hybrid port, add the port to VLAN 2, VLAN 3, and VLAN 10, and configure the port to forward tagged packets for 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 Ethernet 1/0/1 as a hybrid port, add the port to VLAN 2 and VLAN 10, configure the port to forward untagged packets for 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 Ethernet 1/0/2 as a hybrid port, add the port to VLAN 3 and VLAN 10, configure the port to forward untagged packets for 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
```

Troubleshooting IGMP Snooping

Symptom: Multicast function does not work on the switch.

Solution:

Possible reasons are:

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 in the specific 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.

Table of Contents

1 802.1x Configuration	1-1
Introduction to 802.1x	1-1
Architecture of 802.1x Authentication	1-1
The Mechanism of an 802.1x Authentication System	1-3
Encapsulation of EAPoL Messages	1-3
802.1x Authentication Procedure	1-5
Timers Used in 802.1x	1-8
802.1x Implementation on an S3600 Series Switch	1-9
Introduction to 802.1x Configuration	1-12
Basic 802.1x Configuration	1-13
Configuration Prerequisites	1-13
Configuring Basic 802.1x Functions	1-13
Timer and Maximum User Number Configuration	1-14
Advanced 802.1x Configuration	1-15
Configuring Proxy Checking	1-16
Configuring Client Version Checking	1-16
Enabling DHCP-triggered Authentication	1-17
Configuring Guest VLAN	1-17
Configuring 802.1x Re-Authentication	1-18
Configuring the 802.1x Re-Authentication Timer	1-18
Displaying and Maintaining 802.1x Configuration	1-19
Configuration Example	1-19
802.1x Configuration Example	1-19
2 Quick EAD Deployment Configuration	2-1
Introduction to Quick EAD Deployment	2-1
Quick EAD Deployment Overview	2-1
Operation of Quick EAD Deployment	2-1
Configuring Quick EAD Deployment	2-2
Configuration Prerequisites	2-2
Configuration Procedure	2-2
Displaying and Maintaining Quick EAD Deployment	2-3
Quick EAD Deployment Configuration Example	2-3
Troubleshooting	2-5
3 HABP Configuration	3-1
Introduction to HABP	3-1
HABP Server Configuration	3-1
HABP Client Configuration	3-2
Displaying and Maintaining HABP Configuration	3-2
4 System Guard Configuration	4-1
System Guard Overview	4-1
Guard Against IP Attacks	4-1
Guard Against TCN Attacks	4-1

Layer 3 Error Control	4-1
CPU Protection	4-1
Configuring System Guard	4-2
Configuring System Guard Against IP Attacks	4-2
Configuring System Guard Against TCN Attacks	4-2
Enabling Layer 3 Error Control	4-3
Configuring CPU Protection	4-3
Displaying and Maintaining System Guard Configuration	4-4

1 802.1x Configuration

When configuring 802.1x, go to these sections for information you are interested in:

- [Introduction to 802.1x](#)
- [Introduction to 802.1x Configuration](#)
- [Basic 802.1x Configuration](#)
- [Advanced 802.1x Configuration](#)
- [Displaying and Maintaining 802.1x Configuration](#)
- [Configuration Example](#)

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 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.

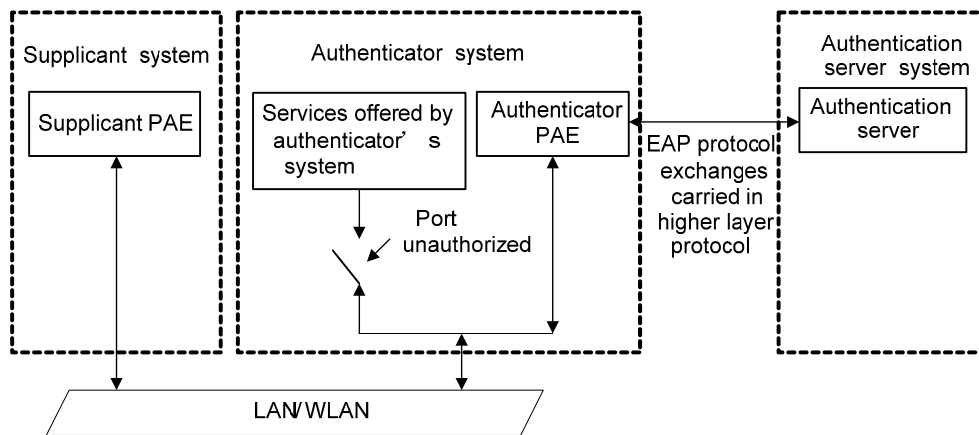
This section covers these topics:

- [Architecture of 802.1x Authentication](#)
- [The Mechanism of an 802.1x Authentication System](#)
- [Encapsulation of EAPoL Messages](#)
- [802.1x Authentication Procedure](#)
- [Timers Used in 802.1x](#)
- [802.1x Implementation on an S3600 Series Switch](#)

Architecture of 802.1x Authentication

As shown in [Figure 1-1](#), 802.1x adopts a client/server architecture with three entities: a supplicant system, an authenticator system, and an authentication server system.

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 at 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 extensible authentication protocol over LAN (EAPoL).
- The authenticator system is another entity residing at one end of a LAN segment. It authenticates the connected supplicant systems. The authenticator system is usually an 802.1x-supported network device (such as a H3C series 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 Authentication, Authorization, and Accounting (AAA) services to users. It also stores user information, such as user name, password, the VLAN a user belongs to, priority, and the Access Control Lists (ACLs) applied.

The four basic concepts 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.

PAE

A port access entity (PAE) 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 status (authorized/unauthorized) 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.

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.

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.

The way a port is controlled

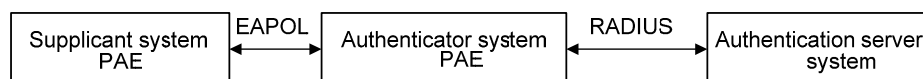
A port of a H3C series switch can be controlled in the following two ways.

- 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-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.

The Mechanism of an 802.1x Authentication System

IEEE 802.1x authentication system uses the Extensible Authentication Protocol (EAP) to exchange information between the supplicant system and the authentication server.

Figure 1-2 The mechanism of an 802.1x authentication system



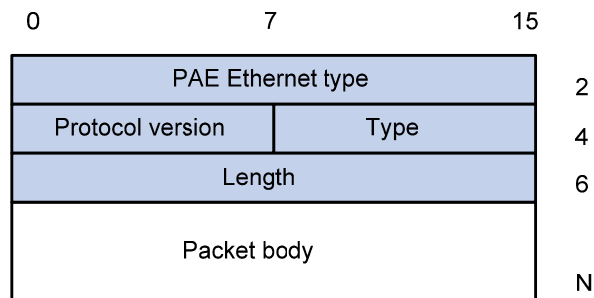
- EAP protocol packets transmitted between the supplicant system PAE and the authenticator system PAE are encapsulated as EAPoL packets.
- EAP protocol packets transmitted between the authenticator system PAE and the RADIUS server can either be encapsulated as EAP over RADIUS (EAPoR) packets or be terminated at system PAEs. The system PAEs then communicate with RADIUS servers through Password Authentication Protocol (PAP) or Challenge-Handshake Authentication Protocol (CHAP) 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.

Encapsulation of EAPoL Messages

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:

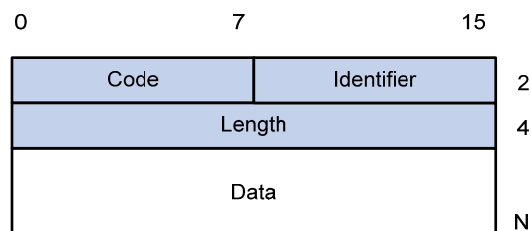
- The PAE Ethernet type field holds the protocol identifier. The identifier for 802.1x is 0x888E.
- The Protocol version field holds the version of the protocol supported by the sender of the EAPoL packet.
- The Type field can be one of the following:
 - 00: Indicates that the packet is an EAP-packet, 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 Alerting Standards Forum (ASF).
- 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.

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:

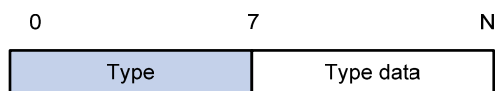
- The Code field indicates the EAP packet type, which can be Request, Response, Success, or Failure.
- The Identifier field is used to match a Response packet with the corresponding Request packet.

- The Length field indicates the size of an EAP packet, which includes the Code, Identifier, Length, and Data fields.
- The Data field carries the EAP packet, whose format 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



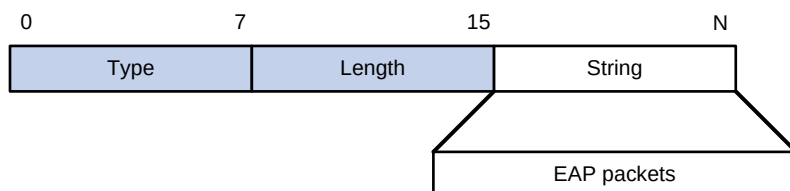
- The Type field indicates the EAP authentication type. A value of 1 indicates Identity and that the packet is used to query the identity of the peer. A value of 4 represents MD5-Challenge (similar to PPP CHAP) and indicates that the packet includes query information.
- The Type Date field differs with types of Request and Response packets.

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 Operation* for information about the format of a RADIUS protocol packet.)

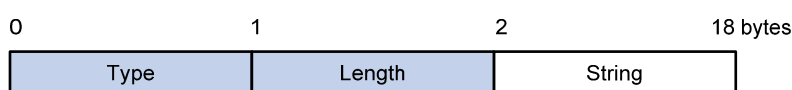
The EAP-message field, whose format is shown in [Figure 1-6](#), is used to encapsulate EAP packets. The maximum size of the string field is 253 bytes. EAP packets with their size larger than 253 bytes are fragmented and are encapsulated in multiple EAP-message fields. The type code of the EAP-message 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



802.1x Authentication Procedure

A H3C S3600 series Ethernet switch can authenticate supplicant systems in EAP terminating mode or EAP relay mode.

EAP relay mode

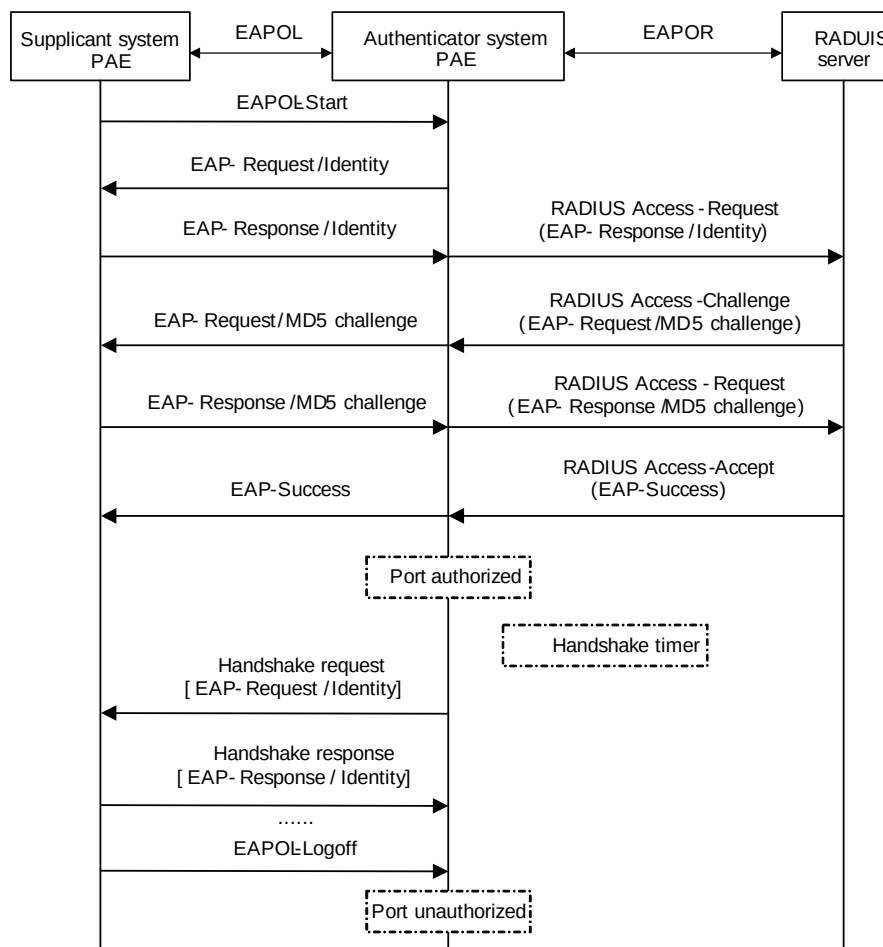
This mode is defined in 802.1x. In this mode, EAP packets are encapsulated in higher level protocol (such as EAPoR) packets to enable them to successfully reach the authentication server. Normally, this mode requires that the RADIUS server support the two newly-added fields: the EAP-message field (with 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 (tunneled transport layer security), and Protected Extensible Authentication Protocol (PEAP), 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 allows the supplicant system and the RADIUS server to check each other's security certificate and authenticate each other's identity, guaranteeing that data is transferred to the right destination and preventing data from being intercepted.
- 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

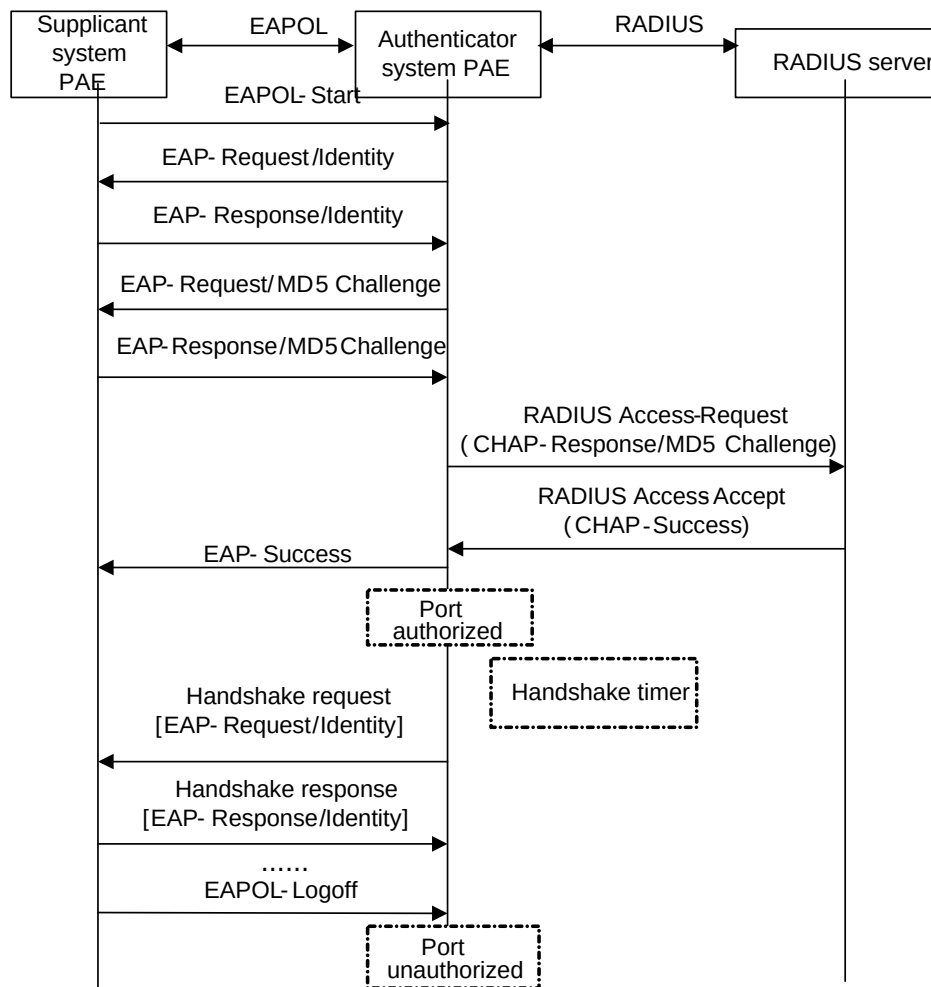
In EAP relay mode, packets are not modified during transmission. Therefore if one of the four ways are used (that is, PEAP, EAP-TLS, EAP-TTLS or EAP-MD5) to authenticate, ensure that the authenticating ways used on the supplicant system and the RADIUS server are the same. However for the switch, you can simply enable the EAP relay mode by using the **dot1x authentication-method eap** command.

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.

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. You can set the maximum number of transmission attempts by using the **dot1x retry** command. An online user will be considered offline when the switch has not received any response packets after the maximum number of handshake request transmission attempts is reached.
- **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. During this quiet period, the switch does not perform any 802.1x authentication-related actions for the supplicant system.

- Re-authentication timer (**reauth-period**). The switch initiates 802.1x re-authentication at the interval set by the re-authentication timer.
- RADIUS server timer (**server-timeout**). This timer sets the server-timeout period. After sending an authentication request packet to the RADIUS server, the 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 not receive version response packets from the supplicant system when the timer expires.

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



Note

H3C's CAMS Server is a service management system used to manage networks and to secure networks and user information. With the cooperation of other networking devices (such as switches) in the network, a CAMS server can implement the AAA functions and rights management.

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.
- Sends Trap packets without disconnecting the supplicant system.

This function needs the cooperation of 802.1x client and a CAMS server.

- The 802.1x client needs to be 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.
-

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.

The guest VLAN function

The guest VLAN function enables supplicant systems 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 sends authentication triggering request (EAP-Request/Identity) packets to 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 Operation* for detailed information about the dynamic VLAN delivery function.

Enabling 802.1x re-authentication

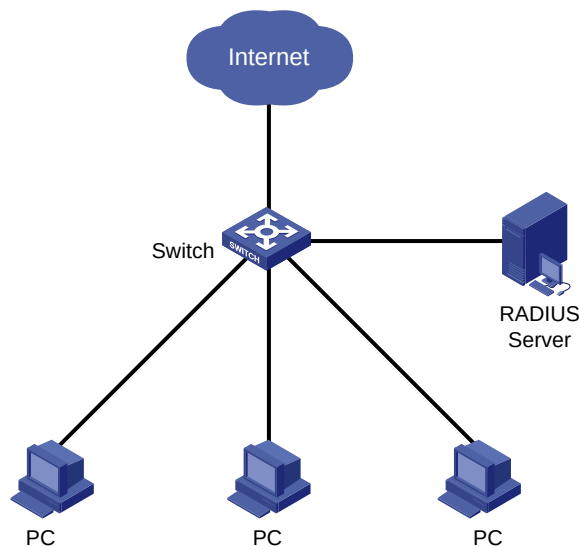
802.1x re-authentication is timer-triggered or packet-triggered. It re-authenticates users who have passed authentication. With 802.1x re-authentication enabled, the switch can monitor the connection status of users periodically. If the switch receives no re-authentication response from a user in a period of time, it tears down the connection to the user. To connect to the switch again, the user needs to initiate 802.1x authentication with the client software again.



Note

- When re-authenticating a user, a switch goes through the complete authentication process. It transmits the username and password of the user to the server. The server may authenticate the username and password, or, however, use re-authentication for only accounting and user connection status checking and therefore does not authenticate the username and password any more.
 - An authentication server running CAMS authenticates the username and password during re-authentication of a user in the EAP authentication mode but does not in PAP or CHAP authentication mode.
-

Figure 1-10 802.1x re-authentication



802.1x re-authentication can be enabled in one of the following two ways:

- The RADIUS server has the switch perform 802.1x re-authentication of users. The RADIUS server sends the switch an Access-Accept packet with the Termination-Action attribute field of 1. Upon receiving the packet, the switch re-authenticates the user periodically.
- You enable 802.1x re-authentication on the switch. With 802.1x re-authentication enabled, the switch re-authenticates users periodically.



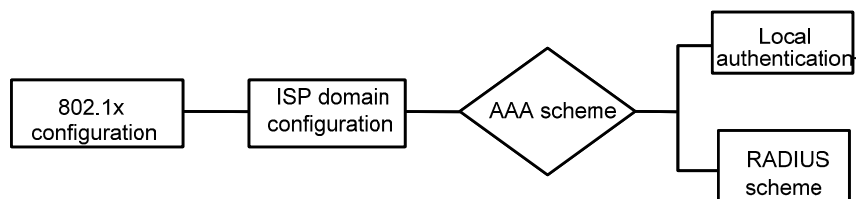
Note

802.1x re-authentication will fail if a CAMS server is used and configured to perform authentication but not accounting. This is because a CAMS server establishes a user session after it begins to perform accounting. Therefore, to enable 802.1x re-authentication, do not configure the **accounting none** command in the domain. This restriction does not apply to other types of servers.

Introduction to 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 or local authentication scheme).

Figure 1-11 802.1x 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 a RADIUS scheme) to be adopted in the ISP domain.
- If you specify to use a local authentication scheme, you need to configure the user names and passwords manually on the switch. Users can pass the authentication through 802.1x client if they provide user names and passwords that match those configured on the switch.
- 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.
- You can also specify to adopt the 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 Operation* for detailed information about AAA scheme configuration.

Basic 802.1x Configuration

Configuration 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.

Configuring Basic 802.1x Functions

Follow these steps to configure basic 802.1x functions:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enable 802.1x globally		dot1x	Required By default, 802.1x is disabled globally.
Enable 802.1x for specified ports	In system view	dot1x interface <i>interface-list</i>	Required By default, 802.1x is disabled on all ports.
	In port view	interface <i>interface-type</i> <i>interface-number</i>	
		dot1x	
		quit	
Set port access control mode for specified ports	In system view	dot1x port-control { authorized-force unauthorized-force auto } [interface <i>interface-list</i>]	Optional By default, an 802.1x-enabled port operates in the auto mode.
	In port view	interface <i>interface-type</i> <i>interface-number</i>	
		dot1x port-control { authorized-force unauthorized-force auto }	
		quit	
Set port access method for specified ports	In system view	dot1x port-method { macbased portbased } [interface <i>interface-list</i>]	Optional The default port access method is MAC-address-based (that is, the macbased keyword is used by default).
	In port view	interface <i>interface-type</i> <i>interface-number</i>	
		dot1x port-method { macbased portbased }	
		quit	
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.

To do...	Use the command...	Remarks
Enable online user handshaking	dot1x handshake enable	Optional By default, online user handshaking is enabled.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the handshake packet protection function	dot1x handshake secure	Optional By default, the handshake packet protection function is disabled.



Caution

- 802.1x configurations take effect only after you enable 802.1x both globally and for specified ports.
- The settings of 802.1x and MAC address learning limit are mutually exclusive. Enabling 802.1x on a port will prevent you from setting the limit on MAC address learning on the port and vice versa.
- The settings of 802.1x and aggregation group member are mutually exclusive. Enabling 802.1x on a port will prevent you from adding the port to an aggregation group and vice versa.
- When a device operates as an authentication server, its authentication method for 802.1x users cannot be configured as EAP.
- With the support of the H3C proprietary client, handshake packets are used to test whether or not a user is online.
- As clients that are not of H3C do not support the online user handshaking function, switches cannot receive handshake acknowledgement packets from them in handshaking periods. To prevent users being falsely considered offline, you need to disable the online user handshaking function in this case.
- The handshake packet protection function requires the cooperation of the client and the authentication server. If either of the two ends does not support the function, you need to disable it on the other one.

Timer and Maximum User Number Configuration

Follow these steps to configure 802.1x timers and the maximum number of users:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Set the maximum number of concurrent on-line users for specified ports	In system view	dot1x max-user <i>user-number</i> [interface <i>interface-list</i>]	Optional By default, a port can accommodate up to 256 users at a time.
	In port view	interface <i>interface-type</i> <i>interface-number</i>	
		dot1x max-user <i>user-number</i>	
		quit	

To do...	Use the command...	Remarks
Set the maximum retry times to send request packets	dot1x retry <i>max-retry-value</i>	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 <i>handshake-period-value</i> quiet-period <i>quiet-period-value</i> server-timeout <i>server-timeout-value</i> supp-timeout <i>supp-timeout-value</i> tx-period <i>tx-period-value</i> ver-period <i>ver-period-value</i> }	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
Enable 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.

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
- 802.1x re-authentication configuration
- Configuration of the 802.1x re-authentication timer

You need to configure basic 802.1x functions before configuring the above 802.1x features.

Configuring Proxy Checking

Follow these steps to configure proxy checking:

To do...		Use the command...	Remarks
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 <i>interface-list</i>]	Required By default, the 802.1x proxy checking is disabled on a port.
	In port view	interface <i>interface-type</i> <i>interface-number</i>	
		dot1x supp-proxy-check { logoff trap }	
		quit	



Note

- The proxy checking function needs the cooperation of H3C's 802.1x client (iNode) program.
- The proxy checking function depends on the online user handshaking function. To enable the proxy detecting function, you need to enable the online user handshaking function first.
- The configuration listed in the above table 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).

Configuring Client Version Checking

Follow these steps to configure client version checking:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enable 802.1x client version checking	In system view	dot1x version-check [interface <i>interface-list</i>]	Required By default, 802.1x client version checking is disabled on a port.
	In port view	interface <i>interface-type</i> <i>interface-number</i>	
		dot1x version-check	
		quit	
Set the maximum number of retries to send version checking request packets		dot1x retry-version-max <i>max-retry-version-value</i>	Optional By default, the maximum number of retries to send version checking request packets is 3.

To do...	Use the command...	Remarks
Set the client version checking period timer	dot1x timer ver-period <i>ver-period-value</i>	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.

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.

Follow these steps to enable DHCP-triggered authentication:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable DHCP-triggered authentication	dot1x dhcp-launch	Required By default, DHCP-triggered authentication is disabled.

Configuring Guest VLAN

Follow these steps to configure guest VLAN:

To do...	Use the command...	Remarks
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	In system view dot1x guest-vlan <i>vlan-id</i> [interface <i>interface-list</i>]	Required By default, the guest VLAN function is disabled.
	In port view interface <i>interface-type</i> <i>interface-number</i>	
	dot1x guest-vlan <i>vlan-id</i>	
	quit	



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.
- The guest VLAN function cannot be implemented if you configure the **dot1x dhcp-launch** command on the switch to enable DHCP-triggered authentication. This is because the switch does not send authentication packets in that case.

Configuring 802.1x Re-Authentication

Follow these steps to enable 802.1x re-authentication:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enable 802.1x re-authentication on port(s)	In system view	dot1x re-authenticate [interface <i>interface-list</i>]	Required By default, 802.1x re-authentication is disabled on a port.
	In port view	dot1x re-authenticate	



Note

- To enable 802.1x re-authentication on a port, you must first enable 802.1x globally and on the port.
- When re-authenticating a user, a switch goes through the complete authentication process. It transmits the username and password of the user to the server. The server may authenticate the username and password, or, however, use re-authentication for only accounting and user connection status checking and therefore does not authenticate the username and password any more.
- An authentication server running CAMS authenticates the username and password during re-authentication of a user in the EAP authentication mode but does not in PAP or CHAP authentication mode.

Configuring the 802.1x Re-Authentication Timer

After 802.1x re-authentication is enabled on the switch, the switch determines the re-authentication interval in one of the following two ways:

- The switch uses the value of the Session-timeout attribute field of the Access-Accept packet sent by the RADIUS server as the re-authentication interval.
- The switch uses the value configured with the **dot1x timer reauth-period** command as the re-authentication interval for access users.

Note the following:

During re-authentication, the switch always uses the latest re-authentication interval configured, no matter which of the above-mentioned two ways is used to determine the re-authentication interval. For example, if you configure a re-authentication interval on the switch and the switch receives an Access-Accept packet whose Termination-Action attribute field is 1, the switch will ultimately use the value of the Session-timeout attribute field as the re-authentication interval.

The following introduces how to configure the 802.1x re-authentication timer on the switch.

Follow these steps to configure the re-authentication interval:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a re-authentication interval	dot1x timer reauth-period <i>reauth-period-value</i>	Optional By default, the re-authentication interval is 3,600 seconds.

Displaying and Maintaining 802.1x Configuration

To do...	Use the command...	Remarks
Display the configuration, session, and statistics information about 802.1x	display dot1x [sessions statistics] [interface interface-list]	Available in any view
Clear 802.1x-related statistics information	reset dot1x statistics [interface interface-list]	Available in user view

Configuration Example

802.1x Configuration Example

Network requirements

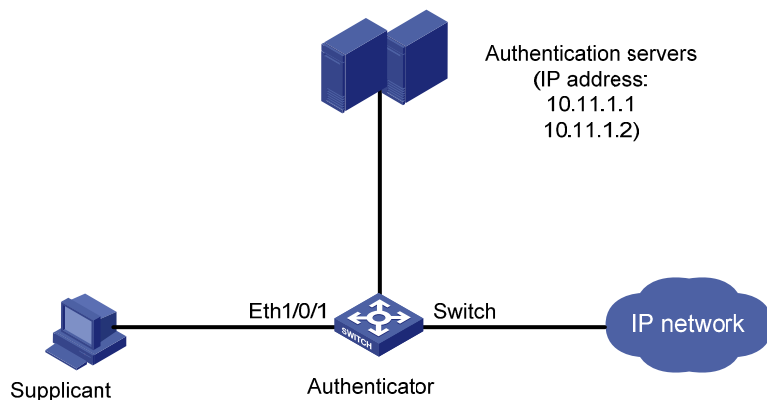
- Authenticate users on all ports to control their accesses to the Internet. The switch operates in MAC-based access control mode.
- All supplicant systems that pass the authentication belong to the default domain named “aabbcc.net”. The domain can accommodate up to 30 users. As for authentication, a 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.

Network diagram

Figure 1-12 Network diagram for AAA configuration with 802.1x and RADIUS enabled



Configuration procedure



Note

Following configuration covers the major AAA/RADIUS configuration commands. Refer to *AAA Operation* for the information about these commands. Configuration on the client and the RADIUS servers is omitted.

Enable 802.1x globally.

```
<Sysname> system-view
```

System View: return to User View with Ctrl+Z.

```
[Sysname] dot1x
```

Enable 802.1x on Ethernet 1/0/1.

```
[Sysname] dot1x interface Ethernet 1/0/1
```

Set the access control method to MAC-based (This operation can be omitted, as MAC-based is the default).

```
[Sysname] dot1x port-method macbased interface Ethernet 1/0/1
```

Create a RADIUS scheme named “radius1” and enter RADIUS scheme view.

```
[Sysname] radius scheme radius1
```

Assign IP addresses to the primary authentication and accounting RADIUS servers.

```
[Sysname-radius-radius1] primary authentication 10.11.1.1
```

```
[Sysname-radius-radius1] primary accounting 10.11.1.2
```

Assign IP addresses to the secondary authentication and accounting RADIUS server.

```

[Sysname-radius-radius1] secondary authentication 10.11.1.2
[Sysname-radius-radius1] secondary accounting 10.11.1.1

# Set the password for the switch and the authentication RADIUS servers to exchange messages.
[Sysname-radius-radius1] key authentication name

# Set the password for the switch and the accounting RADIUS servers to exchange messages.
[Sysname-radius-radius1] key accounting money

# Set the interval and the number of the retries for the switch to send packets to the RADIUS servers.
[Sysname-radius-radius1] timer 5
[Sysname-radius-radius1] retry 5

# Set the timer for the switch to send real-time accounting packets to the RADIUS servers.
[Sysname-radius-radius1] timer realtime-accounting 15

# Configure to send the user name to the RADIUS server with the domain name truncated.
[Sysname-radius-radius1] user-name-format without-domain
[Sysname-radius-radius1] quit

# Create the domain named "aabbcc.net" and enter its view.
[Sysname] domain 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.
[Sysname-isp-aabbcc.net] scheme radius-scheme radius1 local

# Specify the maximum number of users the user domain can accommodate to 30.
[Sysname-isp-aabbcc.net] access-limit enable 30

# Enable the idle disconnecting function and set the related parameters.
[Sysname-isp-aabbcc.net] idle-cut enable 20 2000
[Sysname-isp-aabbcc.net] quit

# Set the default user domain to aabbcc.net.
[Sysname] domain default enable aabbcc.net

# Create a local access user account.
[Sysname] local-user localuser
[Sysname-luser-localuser] service-type lan-access
[Sysname-luser-localuser] password simple localpass

```

2 Quick EAD Deployment Configuration

When configuring quick EAD deployment, go to these sections for information you are interested in:

- [Introduction to Quick EAD Deployment](#)
- [Configuring Quick EAD Deployment](#)
- [Displaying and Maintaining Quick EAD Deployment](#)
- [Quick EAD Deployment Configuration Example](#)
- [Troubleshooting](#)

Introduction to Quick EAD Deployment

Quick EAD Deployment Overview

As an integrated solution, an Endpoint Admission Defense (EAD) solution can improve the overall defense power of a network. In real applications, however, deploying EAD clients proves to be time consuming and inconvenient.

To address the issue, the H3C S3600 series provides the forcible deployment of EAD clients with 802.1x authentication, easing the work of EAD client deployment.

Operation of Quick EAD Deployment

Quick EAD deployment is achieved with the two functions: restricted access and HTTP redirection.

Restricted access

Before passing 802.1x authentication, a user is restricted (through ACLs) to a specific range of IP addresses or a specific server. Services like EAD client upgrading/download and dynamic address assignment are available on the specific server.

HTTP redirection

In the HTTP redirection approach, when the terminal users that have not passed 802.1x authentication access the Internet through Internet Explorer, they are redirected to a predefined URL for EAD client download.

The two functions ensure that all the users without an EAD client have downloaded and installed one from the specified server themselves before they can access the Internet, thus decreasing the complexity and effort that EAD client deployment may involve.



Note

The quick EAD deployment feature takes effect only when the access control mode of an 802.1x-enabled port is set to **auto**.

Configuring Quick EAD Deployment

Configuration Prerequisites

- Enable 802.1x on the switch.
- Set the access mode to **auto** for 802.1x-enabled ports.

Configuration Procedure

Configuring a free IP range

A free IP range is an IP range that users can access before passing 802.1x authentication.

Follow these steps to configure a free IP range:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the URL for HTTP redirection	dot1x url <i>url-string</i>	Required
Configure a free IP range	dot1x free-ip <i>ip-address</i> { <i>mask-address</i> <i>mask-length</i> }	Required By default, no free IP range is configured.



Caution

- You must configure the URL for HTTP redirection before configuring a free IP range. A URL must start with `http://` and the segment where the URL resides must be in the free IP range. Otherwise, the redirection function cannot take effect.
- You must disable the DHCP-triggered authentication function of 802.1x before configuring a free IP range.
- With dot1x enabled but quick EAD deployment disabled, users cannot access the DHCP server if they fail 802.1x authentication. With quick EAD deployment enabled, users can obtain IP addresses dynamically before passing authentication if the IP address of the DHCP server is in the free IP range.
- The quick EAD deployment function applies to only ports with the access control mode set to **auto** through the **dot1x port-control** command.
- At present, 802.1x is the only access approach that supports quick EAD deployment.
- Currently, the quick EAD deployment function does not support port security. The configured free IP range cannot take effect if you enable port security.
- The quick EAD deployment function and the MAC address authentication function are mutually exclusive. You cannot configure both the functions on the switch.

Setting the ACL timeout period

The quick EAD deployment function depends on ACLs in restricting access of users failing authentication. Each online user that has not passed authentication occupies a certain amount of ACL resources. After a user passes authentication, the occupied ACL resources will be released. When a

large number of users log in but cannot pass authentication, the switch may run out of ACL resources, preventing other users from logging in. A timer called ACL timer is designed to solve this problem.

You can control the usage of ACL resources by setting the ACL timer. The ACL timer starts once a user gets online. If the user has not passed authentication when the ACL timer expires, the occupied ACL resources are released for other users to use. When a tremendous of access requests are present, you can decrease the timeout period of the ACL timer appropriately for higher utilization of ACL resources.

Follow these steps to configure the ACL timer:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the ACL timer	dot1x timer acl-timeout <i>acl-timeout-value</i>	Required By default, the ACL timeout period is 30 minutes.

Displaying and Maintaining Quick EAD Deployment

To do...	Use the command...	Remarks
Display configuration information about quick EAD deployment	display dot1x [sessions statistics] [interface interface-list]	Available in any view

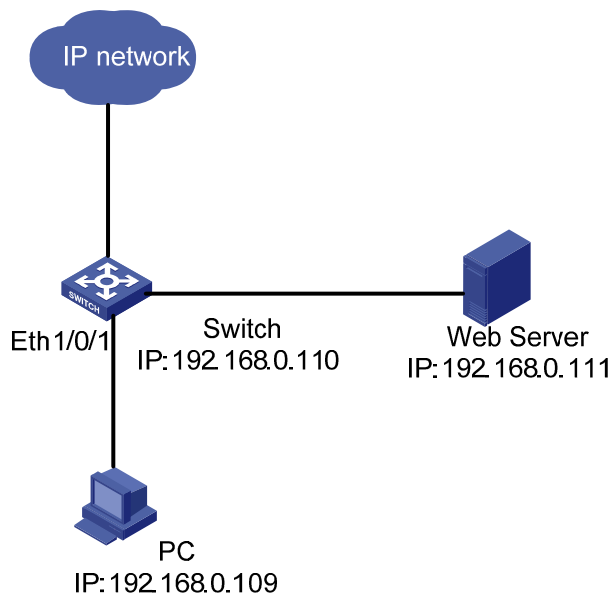
Quick EAD Deployment Configuration Example

Network requirements

A user connects to the switch directly. The switch connects to the Web server and the Internet. The user will be redirected to the Web server to download the authentication client and upgrade software when accessing the Internet through IE before passing authentication. After passing authentication, the user can access the Internet.

Network diagram

Figure 2-1 Network diagram for quick EAD deployment



Configuration procedure



Note

Before enabling quick EAD deployment, be sure that:

- The Web server is configured properly.
- The default gateway of the user's PC is configured as the IP address of the connected VLAN interface on the switch.

Configure the URL for HTTP redirection.

```
<Sysname> system-view
```

```
[Sysname] dot1x url http://192.168.0.111
```

Configure a free IP range.

```
[Sysname] dot1x free-ip 192.168.0.111 24
```

Set the ACL timer to 10 minutes.

```
[Sysname] dot1x timer acl-timeout 10
```

Enable dot1x globally.

```
[Sysname] dot1x
```

Enable dot1x for Ethernet 1/0/1.

```
[Sysname] dot1x interface Ethernet 1/0/1
```

Troubleshooting

Symptom: A user cannot be redirected to the specified URL server, no matter what URL the user enters in the IE address bar.

Solution:

- If a user enters an IP address in a format other than the dotted decimal notation, the user may not be redirected. This is related with the operating system used on the PC. In this case, the PC considers the IP address string a name and tries to resolve the name. If the resolution fails, the PC will access a specific website. Generally, this address is not in dotted decimal notation. As a result, the PC cannot receive any ARP response and therefore cannot be redirected. To solve this problem, the user needs to enter an IP address that is not in the free IP range in dotted decimal notation.
- If a user enters an address in the free IP range, the user cannot be redirected. This is because the switch considers that the user wants to access a host in the free IP range, unconcerned about whether this PC exists or not. To solve this problem, the user needs to enter an address not in the free IP range.
- Check that you have configured an IP address in the free IP range for the Web server and a correct URL for redirection, and that the server provides Web services properly.

3 HABP Configuration

When configuring HABP, go to these sections for information you are interested in:

- [Introduction to HABP](#)
- [HABP Server Configuration](#)
- [HABP Client Configuration](#)
- [Displaying and Maintaining HABP Configuration](#)

Introduction to HABP

When a switch is configured with the 802.1x function, 802.1x will authenticate and authorize 802.1x-enabled ports and allow only the authorized ports to forward packets. In case a port fails 802.1x authentication and authorization, service packets from and to that port will be blocked, making it impossible to manage the switch attached to the port. The Huawei Authentication Bypass Protocol (HABP) aims at solving 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 built on the client-server model. Typically, the HABP server sends HABP requests to the client periodically to collect the MAC address(es) of the attached switch(es). The client responds to the requests, and forwards the HABP requests to the attached switch(es). The HABP server usually runs on the administrative device while the HABP client runs on the attached switches.

For ease of switch management, it is recommended that you enable HABP for 802.1x-enabled switches.

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.

Follow these steps to configure an HABP server:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable HABP	habp enable	Optional By default, HABP is enabled.

To do...	Use the command...	Remarks
Configure the current switch to be an HABP server	habp server vlan <i>vlan-id</i>	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.
Configure the interval to send HABP request packets.	habp timer <i>interval</i>	Optional The default interval for an HABP server to send HABP request packets is 20 seconds.

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.

Follow these steps to configure an HABP client:

To do...	Use the command...	Remarks
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.

Displaying and Maintaining HABP Configuration

To do...	Use the command...	Remarks
Display HABP configuration and status	display habp	Available in any view
Display the MAC address table maintained by HABP	display habp table	Available in any view
Display statistics on HABP packets	display habp traffic	Available in any view

4 System Guard Configuration



Note

The CPU protection function is added. See [CPU Protection](#) and [Configuring CPU Protection](#).

When configuring System Guard, go to these sections for information you are interested in:

- [System Guard Overview](#)
- [Configuring System Guard](#)
- [Displaying and Maintaining System Guard Configuration](#)

System Guard Overview

Guard Against IP Attacks

System-guard operates to inspect the IP packets over 10-second intervals for the CPU for suspicious source IP addresses. Once the packets from such an IP address hit the predefined threshold, the switch with System Guard enabled will take the following action: If the packets from the source IP address need to be processed by the CPU, the switch decreases the precedence of delivering such packets to the CPU.

Guard Against TCN Attacks

System Guard monitors the rate at which TCN/TC packets are received on the ports. If a port receives an excessive number of TCN/TC packets within a given period of time, the switch sends only one TCN/TC packet in every 10 seconds to the CPU and discards the rest TCN/TC packets, while outputting trap and log information.

Layer 3 Error Control

With the Layer 3 error control feature enabled, the switch delivers all Layer 3 packets that the switch considers to be error packets to the CPU.

CPU Protection

When the device is under attack, a large amount of packets will be sent to the device CPU for processing, which causes the device CPU usage to become exceptionally high and thus adversely affects normal services on the device. The CPU protection function allows you to control the amount of packets sent to the CPU within a given time period by setting the CPU protection parameter, thus preventing exceptionally high CPU usage.

Configuring System Guard

Configuring System Guard Against IP Attacks

Configuration of System Guard against IP attacks includes these tasks:

- Enabling System Guard against IP attacks
- Setting the maximum number of infected hosts that can be concurrently monitored
- Configuring parameters related to MAC address learning

Follow these steps to configure System Guard against IP attacks:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable System Guard against IP attacks	system-guard ip enable	Required Disabled by default
Set the maximum number of infected hosts that can be concurrently monitored	system-guard ip detect-maxnum <i>number</i>	Optional 30 by default
Set the maximum number of addresses that the system can learn, the maximum number of times an address can be hit before an action is taken and the address isolation time (presented in the number of multiples of MAC address aging time)	system-guard ip detect-threshold <i>ip-record-threshold</i> <i>record-times-threshold</i> <i>isolate-time</i>	Optional By default, <i>ip-record-threshold</i> is 30; <i>record-times-threshold</i> is 1, and <i>isolate-time</i> is 3.



Note

The correlations among the arguments of the **system-guard ip detect-threshold** command can be clearly described with this example: If you set *ip-record-threshold*, *record-times-threshold* and *isolate-time* to 30, 1 and 3 respectively, when the system detects successively three times that over 50 IP packets (destined for an address other than an IP address of the switch) from a source IP address are received within a period of 10 seconds, the system considers that it is being attacked—the system sorts out the source IP address and decreases the precedence of delivering packets from the source IP address to the CPU for a period of 5 times the MAC address aging time.

Configuring System Guard Against TCN Attacks

Configuration of System Guard against TCN attacks includes these tasks:

- Enabling System Guard against TCN attacks
- Setting the threshold of TCN/TC packet receiving rate

Follow these steps to configure System Guard against TCN attacks:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable System Guard against TCN attacks	system-guard tcn enable	Required Disabled by default

To do...	Use the command...	Remarks
Set the threshold of TCN/TC packet receiving rate	system-guard tcn rate-threshold <i>rate-threshold</i>	Optional 1 pps by default



Note

As the system monitoring cycle is 10 seconds, the system sends trap and log information if more than 10 TCN/TC packets are received within 10 seconds by default. If the TCN/TC packet receiving rate is lower than the set threshold within a 10-second monitoring cycle, the system will not send trap or log information in the next 10-second monitoring cycle.

Enabling Layer 3 Error Control

Follow these steps to enable Layer 3 error control:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable Layer 3 error control	system-guard l3err enable	Required Enabled by default

Configuring CPU Protection



Caution

The CPU protection function is achieved through limiting the amount of packets sent to the CPU within a given time period. With CPU protection enabled, some normal packets may fail to be sent to the CPU for processing timely, which will adversely affect the device performance. Therefore, do not use this function unless you have to.

Follow these steps to configure the CPU protection function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the CPU protection function and configure the CPU protection parameter	system-guard cpu-rcv-limit <i>protection-parameter</i>	Required Disabled by default.

Displaying and Maintaining System Guard Configuration

To do...	Use the command...	Remarks
Display the monitoring result and parameter settings of System Guard against IP attacks	display system-guard ip state	Available in any view
Display the information about IP packets received by the CPU	display system-guard ip-record	
Display the status of Layer 3 error control	display system-guard l3err state	
Display the status of TCN	display system-guard tcn state	

Table of Contents

1 AAA Overview	1-1
Introduction to AAA	1-1
Authentication	1-1
Authorization	1-1
Accounting	1-2
Introduction to ISP Domain	1-2
Introduction to AAA Services	1-2
Introduction to RADIUS	1-2
Introduction to HWTACACS	1-6
2 AAA Configuration	2-1
AAA Configuration Task List	2-1
Creating an ISP Domain and Configuring Its Attributes	2-2
Configuring an AAA Scheme for an ISP Domain	2-3
Configuring Dynamic VLAN Assignment	2-6
Configuring the Attributes of a Local User	2-8
Cutting Down User Connections Forcibly	2-10
RADIUS Configuration Task List	2-10
Creating a RADIUS Scheme	2-12
Configuring RADIUS Authentication/Authorization Servers	2-12
Configuring Ignorance of Assigned RADIUS Authorization Attributes	2-13
Configuring RADIUS Accounting Servers	2-14
Configuring Shared Keys for RADIUS Messages	2-15
Configuring the Maximum Number of RADIUS Request Transmission Attempts	2-16
Configuring the Type of RADIUS Servers to be Supported	2-16
Configuring the Status of RADIUS Servers	2-17
Configuring the Attributes of Data to be Sent to RADIUS Servers	2-18
Configuring the Local RADIUS Server	2-19
Configuring Timers for RADIUS Servers	2-20
Enabling Sending Trap Message when a RADIUS Server Goes Down	2-21
Enabling the User Re-Authentication at Restart Function	2-21
HWTACACS Configuration Task List	2-23
Creating a HWTACACS Scheme	2-23
Configuring TACACS Authentication Servers	2-23
Configuring TACACS Authorization Servers	2-24
Configuring TACACS Accounting Servers	2-25
Configuring Shared Keys for HWTACACS Messages	2-25
Configuring the Attributes of Data to be Sent to TACACS Servers	2-26
Configuring the Timers Regarding TACACS Servers	2-27
Displaying and Maintaining AAA Configuration	2-28
Displaying and Maintaining AAA Configuration	2-28
Displaying and Maintaining RADIUS Protocol Configuration	2-28
Displaying and Maintaining HWTACACS Protocol Configuration	2-29

AAA Configuration Examples	2-29
Remote RADIUS Authentication of Telnet/SSH Users	2-29
Local Authentication of FTP/Telnet Users	2-31
HWTACACS Authentication and Authorization of Telnet Users	2-32
Auto VLAN Configuration Example	2-33
Troubleshooting AAA	2-34
Troubleshooting RADIUS Configuration	2-34
Troubleshooting HWTACACS Configuration	2-35
3 EAD Configuration	3-1
Introduction to EAD	3-1
Typical Network Application of EAD	3-1
EAD Configuration	3-2
EAD Configuration Example	3-2

1 AAA Overview

Introduction to AAA

AAA is the acronym for the three security functions: authentication, authorization and accounting. It provides a uniform framework for you to configure these three functions to implement network security management.

- Authentication: Defines what users can access the network,
- Authorization: Defines what services can be available to the users who can access the network, and
- Accounting: Defines how to charge the users who are using network resources.

Typically, AAA operates in the client/server model: the client runs on the managed resources side while the server stores the user information. Thus, AAA is well scalable and can easily implement centralized management of user information.

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 username, 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. You can use standard or extended RADIUS protocols in conjunction with such systems as iTELLIN/CAMS for user authentication. Remote authentication allows convenient centralized management and is feature-rich. However, to implement remote authentication, a server is needed and must be configured properly.

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.

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.

Introduction to ISP Domain

An Internet service provider (ISP) domain is a group of users who belong to the same ISP. For a username in the format of `userid@isp-name` or `userid.isp-name`, the `isp-name` following the "@" or "." character is the ISP domain name. The access device uses `userid` as the username 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 username 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.

Introduction to AAA Services

Introduction to RADIUS

AAA is a management framework. It can be implemented by not only one protocol. But in practice, the most commonly used service for AAA is RADIUS.

What is RADIUS

Remote Authentication Dial-in User Service (RADIUS) is a distributed service 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 network access servers throughout the network.

RADIUS operates in the client/server model.

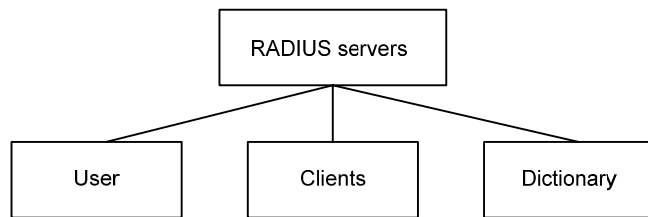
- A switch acting as a RADIUS client passes user information to a specified RADIUS server, and takes appropriate action (such as establishing/terminating user connection) depending on the responses returned from the server.
- The RADIUS server receives user connection requests, authenticates users, and 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 username, 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

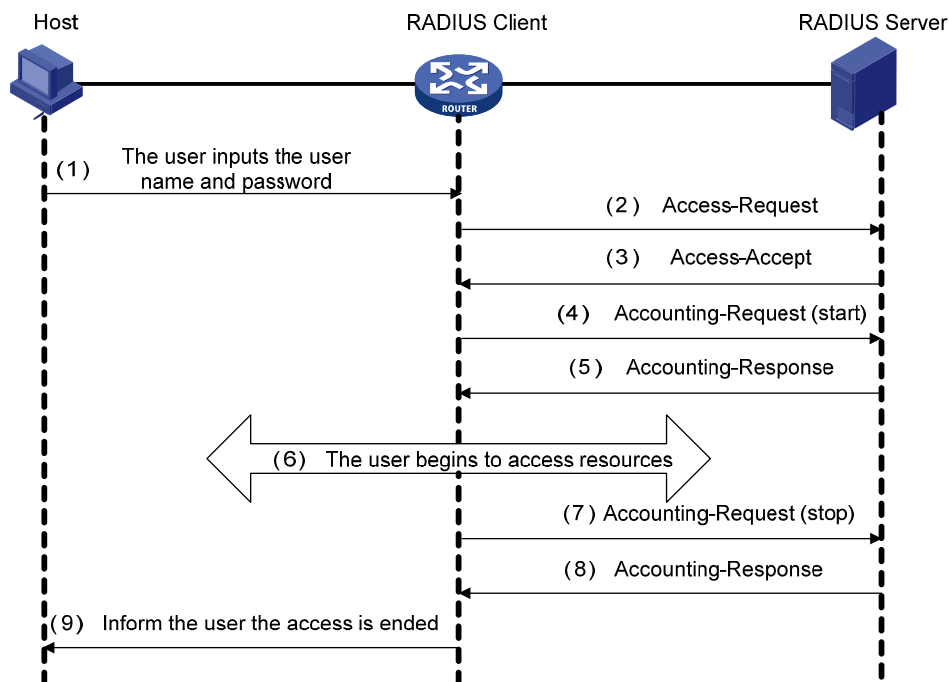


In addition, a RADIUS server can act as a client of some other AAA server to provide authentication or accounting proxy service.

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:

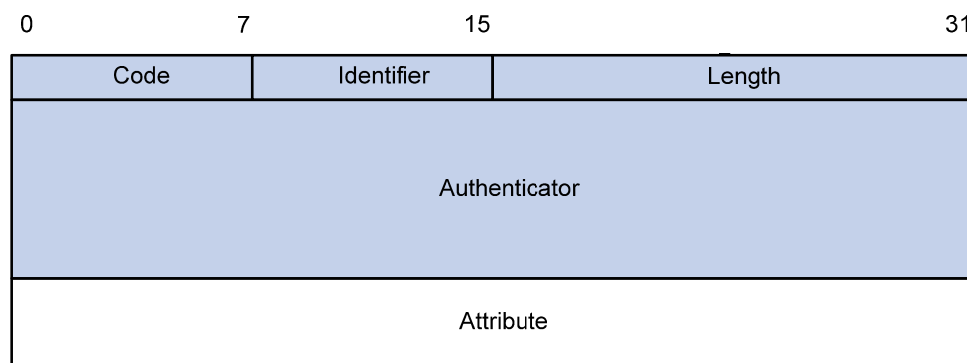
- 2) The user enters the username and password.
- 3) The RADIUS client receives the username and password, and then sends an authentication request (Access-Request) to the RADIUS server.
- 4) The RADIUS server compares the received user information with that in the Users database to authenticate the user. If the authentication succeeds, the RADIUS server sends back to the

- RADIUS client an authentication response (Access-Accept), which contains the user's authorization information. If the authentication fails, the server returns an Access-Reject response.
- 5) 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.
 - 6) The RADIUS server returns a start-accounting response (Accounting-Response).
 - 7) The user starts to access network resources.
 - 8) The RADIUS client sends a stop-accounting request (Accounting-Request, with the Status-Type attribute value = stop) to the RADIUS server.
 - 9) The RADIUS server returns a stop-accounting response (Accounting-Response).
 - 10) The access to network resources is ended.

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).

Code	Message type	Message description
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 changes, 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

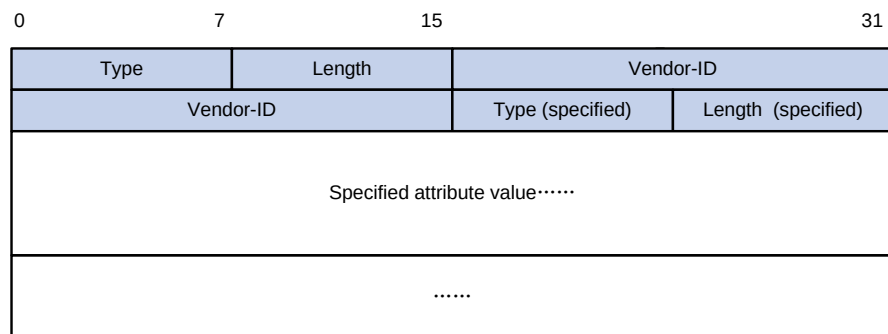
Type field value	Attribute type	Type field value	Attribute type
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier

Type field value	Attribute type	Type field value	Attribute type
11	Filter-ID	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-ID	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

The RADIUS protocol 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



Introduction to HWTACACS

What is HWTACACS

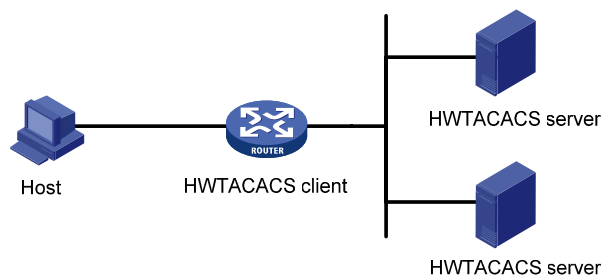
Huawei Terminal Access Controller Access Control System (HWTACACS) is an enhanced security protocol based on TACACS (RFC 1492). Similar to the RADIUS protocol, it implements AAA for different types of users (such as PPP, VPDN, and terminal users) through communicating with TACACS server in client-server 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.

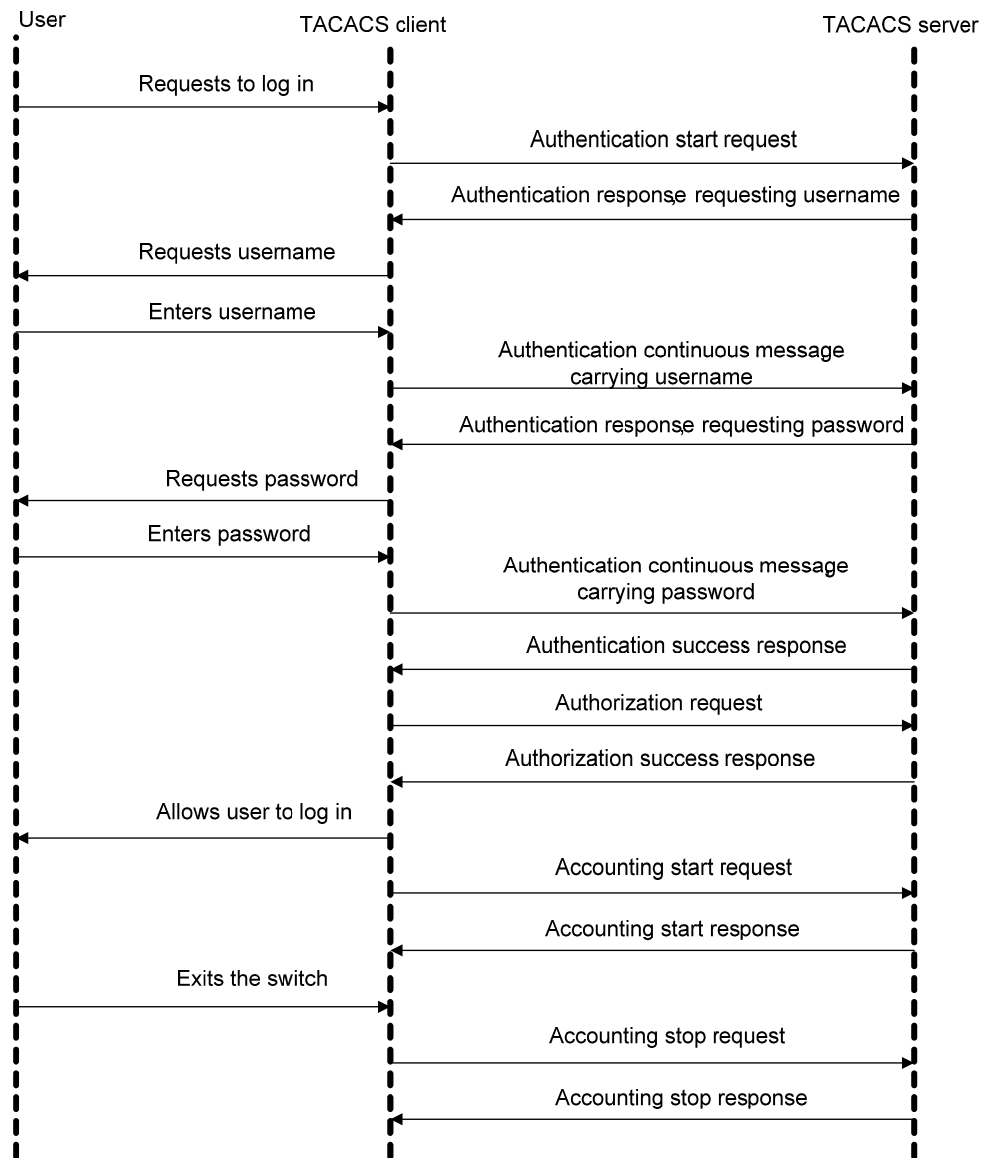
In a typical HWTACACS application (as shown in [Figure 1-5](#)), a terminal user needs to log into the switch to perform some operations. As a HWTACACS client, the switch sends the username and password to the TACACS server for authentication. After passing authentication and being authorized, the user successfully logs into the switch to perform operations.

Figure 1-5 Network diagram for a typical HWTACACS application

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 server.
- 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.

2 AAA Configuration



Note

- A feature named Auto VLAN is added. For its configuration information, refer to [Configuring dynamic VLAN list assignment](#). For its configuration example, refer to [Auto VLAN Configuration Example](#).
- A feature allowing ignorance of assigned RADIUS authorization attributes is added. For details, refer to [Configuring Ignorance of Assigned RADIUS Authorization Attributes](#).

AAA Configuration Task List

You need to configure AAA to provide network access services for legal users while protecting network devices and preventing unauthorized access and repudiation behavior.

Complete the following tasks to configure AAA (configuring a combined AAA scheme for an ISP domain):

Task			Remarks
AAA configuration	Creating an ISP Domain and Configuring Its Attributes		Required
	Configuring a combined AAA scheme		Required
	Configuring an AAA Scheme for an ISP Domain	None authentication	• Use one of the authentication methods • You need to configure RADIUS or HWATACACS before performing RADIUS or HWTACACS authentication
		Local authentication	
		RADIUS authentication	
		HWTACACS authentication	
	Configuring Dynamic VLAN Assignment		Optional
	Configuring the Attributes of a Local User		Optional
	Cutting Down User Connections Forcibly		Optional

Complete the following tasks to configure AAA (configuring separate AAA schemes for an ISP domain):

Task		Remarks
AAA configuration	Creating an ISP Domain and Configuring Its Attributes	Required
	Configuring separate AAA schemes	Required
	Configuring an AAA Scheme for an ISP Domain	Required With separate AAA schemes, you can specify authentication, authorization and accounting schemes respectively. You need to configure RADIUS or HWATACACS before performing RADIUS or HWTACACS authentication.
	Configuring Dynamic VLAN Assignment	Optional
	Configuring the Attributes of a Local User	Optional
	Cutting Down User Connections Forcibly	Optional

Creating an ISP Domain and Configuring Its Attributes

Follow these steps to create an ISP domain and configure its attributes:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the form of the delimiter between the username and the ISP domain name	domain delimiter { at dot }	Optional By default, the delimiter between the username and the ISP domain name is "@".
Create an 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.
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 the ISP domain can accommodate	access-limit { disable enable max-user-number }	Optional By default, there is no limit on the number of access users that the ISP domain can accommodate.
Set the idle-cut function	idle-cut { disable enable minute flow }	Optional By default, the idle-cut function is disabled.
Set the accounting-optional switch	accounting optional	Optional By default, the accounting-optional switch is off.

To do...	Use the command...	Remarks
Set the messenger function	messenger time { enable <i>limit interval</i> disable }	Optional By default, the messenger function is disabled.
Set the self-service server location function	self-service-url { disable enable <i>url-string</i> }	Optional By default, the self-service server location function is disabled.

Note that:

- 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 username, the switch assumes that the user belongs to the default ISP domain.
- If you have configured to use "." as the delimiter, for a username that contains multiple ".", the first "." will be used as the domain delimiter.
- If you have configured to use "@" as the delimiter, the "@" must not appear more than once in the username. If "." is the delimiter, the username must not contain any "@".
- 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 does 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 RADIUS server that supports self-service, such as Comprehensive Access Management Server (CAMS). Through self-service, users can manage and control their account or card numbers by themselves. A server installed with self-service software is called a self-service server.



Note

H3C's CAMS Server is a service management system used to manage networks and ensure network and user information security. With the cooperation of other networking devices (such as switches) in a network, a CAMS server can implement the AAA functions and right management.

Configuring an AAA Scheme for an ISP Domain

You can configure either a combined AAA scheme or separate AAA schemes.

Configuring a combined AAA scheme

You can use the **scheme** command to specify an AAA scheme for an ISP domain.

Follow these steps to configure a combined AAA scheme:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
Create an ISP domain and enter its view, or enter the view of an existing ISP domain	domain <i>isp-name</i>	Required
Configure an AAA scheme for the ISP domain	scheme { local none radius-scheme <i>radius-scheme-name</i> [local] hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] }	Required By default, an ISP domain uses the local AAA scheme.



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, the local scheme is not used; otherwise, the local scheme is used.
- 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, the local scheme is not used; if the TACACS server is not reachable or there is a key error or NAS IP error, the local scheme is used.
- 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 or HWTACACS scheme at the same time.
- If you configure to use **none** as the primary scheme, FTP users of the domain cannot pass authentication. Therefore, you cannot specify **none** as the primary scheme if you want to enable FTP service.

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.

1) 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.

2) For FTP users

Only authentication is supported for FTP users.

Authentication: RADIUS, local, or HWTACACS.

Follow these steps to configure separate AAA schemes:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create an ISP domain and enter its view, or enter the view of an existing ISP domain	domain <i>isp-name</i>	Required
Configure an authentication scheme for the ISP domain	authentication { radius-scheme <i>radius-scheme-name</i> [local] hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] local none }	Optional By default, no separate authentication scheme is configured.
Configure a HWTACACS authentication scheme for user level switching	authentication super hwtacacs-scheme <i>hwtacacs-scheme-name</i>	Optional By default, no HWTACACS authentication scheme is configured.
Configure an authorization scheme for the ISP domain	authorization { none hwtacacs-scheme <i>hwtacacs-scheme-name</i> }	Optional By default, no separate authorization scheme is configured.
Configure an accounting scheme for the ISP domain	accounting { none radius-scheme <i>radius-scheme-name</i> hwtacacs-scheme <i>hwtacacs-scheme-name</i> }	Optional By default, no separate accounting scheme is configured.



Note

- 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.
- The S3600 series switches adopt hierarchical protection for command lines so as to inhibit users at lower levels from using higher level commands to configure the switches. For details about configuring a HWTACACS authentication scheme for low-to-high user level switching, refer to *Switching User Level* in the *Command Line Interface Operation*.

Configuration guidelines

Suppose a combined AAA scheme is available. The system selects AAA schemes according to the following principles:

- If authentication, authorization, accounting each have a separate scheme, the separate schemes are used.
- If you configure only a separate authentication scheme (that is, there are no separate authorization and accounting schemes configured), the combined scheme is used for authorization and

accounting. In this case, if the combined scheme uses RADIUS or HWTACACS, the system never uses the secondary scheme for authorization and accounting.

- If you configure no separate scheme, the combined scheme is used for authentication, authorization, and accounting. In this case, if the system uses the secondary local scheme for authentication, it also does so for authorization and accounting; if the system uses the first scheme for authentication, it also does so for authorization and accounting, even if authorization and accounting fail.

Configuring Dynamic VLAN Assignment

VLAN assignment modes

In networks where 802.1x and MAC address authentications are used, RADIUS servers are often used to control the access rights of authenticated users by issuing dynamic VLANs. By receiving and resolving RADIUS packets, the switches can assign the ports connecting to users to specific VLANs, thus controlling the users' access to network resources.

Currently, the switch supports the following two types of assigned VLAN IDs: integer, string, and VLAN list.

- 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.
- VLAN list: For users connected to an authentication port to access resources in different VLANs, on the RADIUS server, you can configure a VLAN list, assign the port to all the VLANs in the VLAN list, and specify the tagging mode in which the port joins a VLAN, that is, specify whether the port sends the data frames of that VLAN with the VLAN tag attached. In this case, you need to make some configurations on the switch too, so that the switch can recognize the VLAN list carried in a RADIUS packet and assign the port to the VLANs specified in the VLAN list. Configuring a switch to recognize VLAN lists carried in RADIUS packets is referred to as the configuration of Auto VLAN in this document.

Configuring dynamic VLAN list assignment

The RADIUS server issues a VLAN list to a switch by sending RADIUS packets. Each RADIUS packet contains a Tunnel-Private-Group-ID attribute (attribute 81 in the RADIUS standard) string, which includes one or multiple number+suffix combinations (such as 1u, 2t, and 3) that indicate a VLAN list, where: a number indicates a VLAN ID, and a suffix indicates whether data frames of the VLAN are sent tagged.

When the switch receives the VLAN list information, it assigns the authentication port to the VLANs in the VLAN list, and specifies whether the frames of a VLAN are sent tagged according to the suffix of the VLAN ID in the VLAN list as follows:

- For a VLAN ID with suffix **t** or **T**, the authentication port sends the frames of the VLAN tagged.
- For the first VLAN ID with suffix **u** or **U**, or with no suffix in the VLAN list, the authentication port sends the frames of the VLAN untagged and configures the VLAN as its default VLAN; for the other VLAN IDs with suffix **u** or **U**, or with no suffix, the authentication port still sends the frames of the corresponding VLANs tagged.

That is, except the VLAN corresponding to the first VLAN ID with suffix **u** or **U**, or with no suffix in the VLAN list, the authentication port sends the frames of all the VLANs specified in the VLAN list tagged.

Suppose the RADIUS server issues a VLAN list "1u 2t 3" to a switch. After the switch resolves the list, it assigns the authentication port to VLAN 1, VLAN 2, and VLAN 3, configures VLAN 1 as the default VLAN of the authentication port, and configures the authentication port to send frames of VLAN 1 untagged and send frames of VLAN 2 and VLAN 3 tagged.

According to the way a switch resolves a VLAN list, the resolution results of VLAN lists "1u 2u 3u", "1 2 3", "1 2t 3t", "2t 1u 3", "2t 1 3t", and "2t 1 3u" are all the same as that of "1u 2t 3".



Note

- Because the switch needs to assign a port to multiple VLANs specified in a VLAN list, only hybrid and trunk ports support the Auto VLAN feature.
 - For a trunk port, the issued VLAN list must include a default VLAN ID, that is, the VLAN IDs in the VLAN list cannot be all followed by suffix **t** or **T**.
 - A VLAN list issued by the RADIUS server can contain up to 64 VLAN IDs. Otherwise, the authentication fails. In addition, a RADIUS attribute string can contain up to 253 characters. For a VLAN list of more than 253 characters, even though the VLAN list contains no more than 64 VLAN IDs, the authentication switch will not accept this VLAN list, which will also cause the authentication to fail;
 - If a VLAN ID appears in a VLAN list more than once, the tag processing mode for the VLAN depends on the suffix of the VLAN ID appearing the last time; According to this rule, if VLAN list "1u 2u 1t" or "1u 2u 1" is issued to a port, the port joins VLAN 1 and VLAN 2, sending frames of VLAN 1 and VLAN 2 tagged, this VLAN list the same as "2t 1t";
 - The VLAN IDs in the VLAN list must be within the valid VLAN ID range; however, they are not required to be sorted in an ascending or descending order;
 - A VLAN ID starting with 0 is considered illegal;
 - A Tunnel-Private-Group-ID string cannot include characters other than numbers, **U**, **u**, **T**, and **t**. For example, 3.0 and -3 are illegal characters;
 - The number of spaces preceding and following a VLAN ID and its suffix is not restricted, but there should be no space between a VLAN ID and its suffix. For example, the resolution results of VLAN lists " 1u 2t 3", "1u 2t 3 ", "1u 2t 3", and "1u2t3" are all the same as that of "1u 2t 3", while VLAN lists "1uu2t 3", "1 u 2t 3", and "u" are all illegal.
-

In actual applications, to use this feature together with Guest VLAN, you should better set port control to port-based mode. For more information, refer to Basic 802.1x Configuration of *802.1x and System Guard Operation*.

Follow these steps to configure dynamic VLAN assignment:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create an ISP domain and enter its view	domain <i>isp-name</i>	—
Set the VLAN assignment mode	vlan-assignment-mode { integer string vlan-list }	Optional By default, the VLAN assignment mode is integer.
Create a VLAN and enter its view	vlan <i>vlan-id</i>	—
Set a VLAN name for VLAN assignment	name <i>string</i>	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 assigns 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.
- Only 802.1X authentication and RADIUS server authentication-based MAC address authentication support the Auto VLAN feature.
- After a VLAN list is issued to a port, if you use commands to assign/remove the port to/from a VLAN in the VLAN list, some users will be disconnected.
- After a VLAN list is issued to a port, you can use commands to change the default VLAN of the port. However, the change takes effect after all the users are disconnected from the port.

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 username. 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.

Follow these steps to configure the attributes of a local user:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
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 <i>user-name</i>	Required By default, there is no local user in the system.
Set a password for the local user	password { simple cipher } <i>password</i>	Required
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.
Authorize the user to access specified type(s) of service	service-type { ftp lan-access { telnet ssh terminal }* [level <i>level</i>] }	Required By default, the system does not authorize the user to access any service.
Set the privilege level of the user	level <i>level</i>	Optional By default, the privilege level of the user is 0.
Configure the authorized VLAN for the local user	authorization vlan <i>string</i>	Required By default, no authorized VLAN is configured for the local user.
Set the attributes of the user whose service type is lan-access	attribute { ip <i>ip-address</i> mac <i>mac-address</i> idle-cut <i>second</i> access-limit <i>max-user-number</i> vlan <i>vlan-id</i> location { nas-ip <i>ip-address</i> port <i>port-number</i> port <i>port-number</i> } }*	Optional When binding the user to a remote port, you must use nas-ip <i>ip-address</i> to specify a remote access server IP address (here, <i>ip-address</i> is 127.0.0.1 by default, representing this device). When binding the user to a local port, you need not use nas-ip <i>ip-address</i> .



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 username 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.
- If the clients connected to a port have different authorized VLANs, only the first client passing the MAC address authentication can be assigned with an authorized VLAN. The switch will not assign authorized VLANs for subsequent users passing MAC address authentication. In this case, you are recommended to connect only one MAC address authentication user or multiple users with the same authorized VLAN to a port.
- For local **RADIUS** authentication to take effect, the VLAN assignment mode must be set to **string** after you specify authorized VLANs for local users.

Cutting Down User Connections Forcibly

Follow these steps to cut down user connections forcibly:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Cut down user connections forcibly	cut connection { all access-type { dot1x mac-authentication } domain <i>isp-name</i> interface <i>interface-type interface-number</i> ip <i>ip-address</i> mac <i>mac-address</i> radius-scheme <i>radius-scheme-name</i> vlan <i>vlan-id</i> ucibindex <i>ucib-index</i> user-name <i>user-name</i> }	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.

RADIUS Configuration Task List

H3C's Ethernet switches can function not only as RADIUS clients but also as local RADIUS servers.

Complete the following tasks to configure RADIUS (the switch functions as a RADIUS client):

Task		Remarks
Configuring the RADIUS client	Creating a RADIUS Scheme	Required
	Configuring RADIUS Authentication/Authorization Servers	Required
	Configuring Ignorance of Assigned RADIUS Authorization Attributes	Optional
	Configuring RADIUS Accounting Servers	Required
	Configuring Shared Keys for RADIUS Messages	Optional
	Configuring the Maximum Number of RADIUS Request Transmission Attempts	Optional
	Configuring the Type of RADIUS Servers to be Supported	Optional
	Configuring the Status of RADIUS Servers	Optional
	Configuring the Attributes of Data to be Sent to RADIUS Servers	Optional
	Configuring Timers for RADIUS Servers	Optional
	Enabling Sending Trap Message when a RADIUS Server Goes Down	Optional
	Enabling the User Re-Authentication at Restart Function	Optional
Configuring the RADIUS server	Refer to the configuration of the RADIUS Server.	—

Complete the following tasks to configure RADIUS (the switch functions as a local RADIUS server):

Task		Remarks
Configuring the RADIUS server	Creating a RADIUS Scheme	Required
	Configuring RADIUS Authentication/Authorization Servers	Required
	Configuring RADIUS Accounting Servers	Required
	Configuring Shared Keys for RADIUS Messages	Optional
	Configuring the Maximum Number of RADIUS Request Transmission Attempts	Optional
	Configuring the Type of RADIUS Servers to be Supported	Optional
	Configuring the Status of RADIUS Servers	Optional
	Configuring the Attributes of Data to be Sent to RADIUS Servers	Optional
	Configuring the Local RADIUS Server	Required
	Configuring Timers for RADIUS Servers	Optional
	Enabling Sending Trap Message when a RADIUS Server Goes Down	Optional
Configuring the RADIUS client	Refer to the configuration of the RADIUS client	—

The RADIUS service 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 service 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 [AAA Configuration](#)).

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.

Follow these steps to create a RADIUS scheme:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable RADIUS authentication port	radius client enable	Optional By default, RADIUS authentication port is enabled.
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.



Note

A RADIUS scheme can be referenced by multiple ISP domains simultaneously.

Configuring RADIUS Authentication/Authorization Servers

Follow these steps to configure RADIUS authentication/authorization servers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	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 <i>ip-address [port-number]</i>	Required By default, the IP address and UDP port number of the primary server are 0.0.0.0 and 1812 respectively for a newly created RADIUS scheme.
Set the IP address and port number of the secondary RADIUS authentication/authorization server	secondary authentication <i>ip-address [port-number]</i>	Optional By default, the IP address and UDP port number of the secondary server are 0.0.0.0 and 1812 respectively for a newly created RADIUS scheme.



Note

- 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.

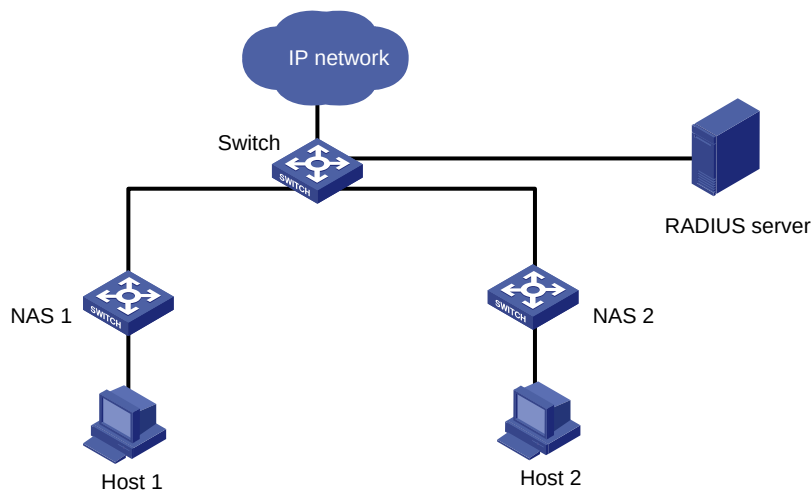
Configuring Ignorance of Assigned RADIUS Authorization Attributes

A RADIUS server can be configured to assign multiple authorization attributes, such as authorization VLAN and idle timeout. Some users may need the attributes but some users may not. Such conflict occurs if the RADIUS server does not support user-based attribute assignment or it performs uniformed user management.

The RADIUS authorization attribute ignoring function can solve this issue. It is configured as per RADIUS scheme. Users using a RADIUS scheme with this function enabled can ignore certain unexpected attributes.

As shown in [Figure 2-1](#), NAS 1 and NAS 2 are connected to the same RADIUS server for authentication. For easy management, the RADIUS server issues the same authorization attributes to all the users. However, users attached to NAS 1 need these attributes while users attached to NAS 2 do not want to use the assigned Attribute 28, idle-timeout. You can configure the attribute ignoring function on NAS 2 to ignore Attribute 28.

Figure 2-1 Network diagram for the RADIUS authorization attribute ignoring function



Follow these steps to configure the RADIUS authorization attribute ignoring function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Configure the RADIUS authorization attribute ignoring function	attribute-ignore { standard vendor vendor-id } type <i>type-value</i>	Required Disabled by default.

Note

In a RADIUS scheme, you can configure:

- One standard attribute ignoring command
- One proprietary attribute ignoring command per vendor
- Up to three attribute ignoring commands in total

Configuring RADIUS Accounting Servers

Follow these steps to configure RADIUS accounting servers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.

To do...	Use the command...	Remarks
Set the IP address and port number of the primary RADIUS accounting server	primary accounting <i>ip-address [port-number]</i>	Required By default, the IP address and UDP port number of the primary accounting server are 0.0.0.0 and 1813 for a newly created RADIUS scheme.
Set the IP address and port number of the secondary RADIUS accounting server	secondary accounting <i>ip-address [port-number]</i>	Optional By default, the IP address and UDP port number of the secondary accounting server are 0.0.0.0 and 1813 for a newly created RADIUS scheme.
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 <i>retry-times</i>	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 <i>retry-times</i>	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.



Note

- 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.

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.

Follow these steps to configure shared keys for RADIUS messages:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	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 <i>string</i>	Required By default, no shared key is created.
Set a shared key for RADIUS accounting messages	key accounting <i>string</i>	Required By default, no shared key is created.



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.

Configuring the Maximum Number of RADIUS Request Transmission Attempts

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.

Follow these steps to configure the maximum transmission attempts of a RADIUS request:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the maximum number of RADIUS request transmission attempts	retry <i>retry-times</i>	Optional By default, the system can try three times to transmit a RADIUS request.

Configuring the Type of RADIUS Servers to be Supported

Follow these steps to configure the type of RADIUS servers to be supported:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Configure the type of RADIUS servers to be supported	server-type { extended standard }	Optional



Note

- If you change the RADIUS server type, the units of data flows sent to RADIUS servers will be restored to the defaults.
- When the third party RADIUS server is used, you can select **standard** or **extended** as the server-type in a RADIUS scheme; when the CAMS server is used, you can select **extended** as the server-type in a RADIUS scheme.

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.

Follow these steps to set the status of RADIUS servers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the status of the primary RADIUS authentication/authorization server	state primary authentication { block active }	Optional By default, the RADIUS servers specified with IP addresses in the RADIUS scheme are all in the active state.
Set the status of the primary RADIUS accounting server	state primary accounting { block active }	

To do...	Use the command...	Remarks
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 }	

Configuring the Attributes of Data to be Sent to RADIUS Servers

Follow these steps to configure the attributes of data to be sent to RADIUS servers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the format of the usernames to be sent to RADIUS server	user-name-format { with-domain without-domain }	Optional By default, the usernames 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 RADIUS scheme, the data unit and packet unit for outgoing RADIUS flows are byte and one-packet respectively.
Set the MAC address format of the Calling-Station-Id (Type 31) field in RADIUS packets	calling-station-id mode { mode1 mode2 } { lowercase uppercase }	Optional By default, the MAC address format is XXXX-XXXX-XXXX, in lowercase.
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	



Note

- Generally, the access users are named in the *userid@isp-name* or *userid.isp-name* format. Here, *isp-name* after the "@" or "." 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 usernames that carry ISP domain names. In this case, it is necessary to remove domain names from usernames before sending the usernames 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 usernames to be sent to RADIUS server.
- For a RADIUS scheme, if you have specified to remove ISP domain names from usernames, 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 usernames by default.
- The purpose of setting the MAC address format of the Calling-Station-Id (Type 31) field in RADIUS packets is to improve the switch's compatibility with different RADIUS servers. This setting is necessary when the format of Calling-Station-Id field recognizable to RADIUS servers is different from the default MAC address format on the switch. For details about field formats recognizable to RADIUS servers, refer to the corresponding RADIUS server manual.

Configuring the Local RADIUS Server

The switch provides the local RADIUS server function (including authentication and authorization), also known as the local RADIUS server function, in addition to RADIUS client service, where separate authentication/authorization server and the accounting server are used for user authentication.

Follow these steps to configure the local RADIUS server function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable UDP ports for local RADIUS services	local-server enable	Optional By default, the UDP ports for local RADIUS services are enabled.
Configure the parameters of the local RADIUS server	local-server nas-ip <i>ip-address</i> key <i>password</i>	Required By default, a local RADIUS server is configured with an NAS IP address of 127.0.0.1.



Caution

- If you adopt the local RADIUS 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.
- The switch supports IP addresses and shared keys for up to 16 network access servers (NAS). That is, when acting as the local RADIUS server, the switch can provide authentication service to up to 16 network access servers (including the switch itself) at the same time.
- When acting as the local RADIUS server, the switch does not support EAP authentication (that is you cannot set the 802.1x authentication method as **eap** by using the **dot1x authentication-method eap** command).

Configuring Timers for 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.

Follow these steps to set timers for RADIUS servers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.

To do...	Use the command...	Remarks
Set the response timeout time of RADIUS servers	timer response-timeout <i>seconds</i>	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 <i>minutes</i>	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 <i>minutes</i>	Optional By default, the real-time accounting interval is 12 minutes.

Enabling Sending Trap Message when a RADIUS Server Goes Down

Follow these steps to specify to send trap message when a RADIUS server goes down:

To do...	Use the command...	Remarks
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.

Enabling the User Re-Authentication at Restart Function



Note

The user re-authentication at restart function applies only 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.

Follow these steps to enable the user re-authentication at restart function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter RADIUS scheme view	radius scheme <i>radius-scheme-name</i>	—
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.

HWTACACS Configuration Task List

Complete the following tasks to configure HWTACACS:

Task		Remarks
Configuring the TACACS client	Creating a HWTACACS Scheme	Required
	Configuring TACACS Authentication Servers	Required
	Configuring TACACS Authorization Servers	Required
	Configuring TACACS Accounting Servers	Optional
	Configuring Shared Keys for RADIUS Messages	Optional
	Configuring the Attributes of Data to be Sent to TACACS Servers	Optional
	Configuring the Timers Regarding TACACS Servers	Optional
Configuring the TACACS server	Refer to the configuration of TACACS servers.	—

Creating a HWTACACS 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.

Follow these steps to create a HWTACACS scheme:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a HWTACACS scheme and enter its view	hwtacacs scheme <i>hwtacacs-scheme-name</i>	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.

Configuring TACACS Authentication Servers

Follow these steps to configure TACACS authentication servers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a HWTACACS scheme and enter its view	hwtacacs scheme <i>hwtacacs-scheme-name</i>	Required By default, no HWTACACS scheme exists.

To do...	Use the command...	Remarks
Set the IP address and port number of the primary TACACS authentication server	primary authentication <i>ip-address [port]</i>	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 <i>ip-address [port]</i>	Optional 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.

Configuring TACACS Authorization Servers

Follow these steps to configure TACACS authorization servers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a HWTACACS scheme and enter its view	hwtacacs scheme <i>hwtacacs-scheme-name</i>	Required By default, no HWTACACS scheme exists.
Set the IP address and port number of the primary TACACS authorization server	primary authorization <i>ip-address [port]</i>	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 <i>ip-address [port]</i>	Optional 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.

Configuring TACACS Accounting Servers

Follow these steps to configure TACACS accounting servers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a HWTACACS scheme and enter its view	hwtacacs scheme <i>hwtacacs-scheme-name</i>	Required By default, no HWTACACS scheme exists.
Set the IP address and port number of the primary TACACS accounting server	primary accounting <i>ip-address [port]</i>	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 <i>ip-address [port]</i>	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 <i>retry-times</i>	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.

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.

Follow these steps to configure shared keys for HWTACACS messages:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a HWTACACS scheme and enter its view	hwtacacs scheme <i>hwtacacs-scheme-name</i>	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.

Configuring the Attributes of Data to be Sent to TACACS Servers

Follow these steps to configure the attributes for data to be sent to TACACS servers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a HWTACACS scheme and enter its view	hwtacacs scheme <i>hwtacacs-scheme-name</i>	Required By default, no HWTACACS scheme exists.
Set the format of the usernames to be sent to TACACS server	user-name-format { with-domain without-domain }	Optional By default, the usernames 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 }	
Set the source IP address of outgoing HWTACACS messages	HWTACACS scheme view nas-ip <i>ip-address</i>	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 <i>ip-address</i>	

**Caution**

Generally, the access users are named in the *userid@isp-name* or *userid.isp-name* format. Where, *isp-name* after the "@" or "." character represents the ISP domain name. If the TACACS server does not accept the usernames that carry ISP domain names, it is necessary to remove domain names from usernames before they are sent to TACACS server.

Configuring the Timers Regarding TACACS Servers

Follow these steps to configure the timers regarding TACACS servers:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a HWTACACS scheme and enter its view	hwtacacs scheme <i>hwtacacs-scheme-name</i>	Required By default, no HWTACACS scheme exists.
Set the response timeout time of TACACS servers	timer response-timeout <i>seconds</i>	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 <i>minutes</i>	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 <i>minutes</i>	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.
-

Displaying and Maintaining AAA Configuration

Displaying and Maintaining AAA Configuration

To do...	Use the command...	Remarks
Display configuration information about one specific or all ISP domains	display domain [<i>isp-name</i>]	Available in any view
Display information about user connections	display connection [access-type { dot1x mac-authentication } domain <i>isp-name</i> interface <i>interface-type interface-number</i> ip <i>ip-address</i> mac <i>mac-address</i> radius-scheme <i>radius-scheme-name</i> hwtacacs-scheme <i>hwtacacs-scheme-name</i> vlan <i>vlan-id</i> ucibindex <i>ucib-index</i> user-name <i>user-name</i>]	
Display information about local users	display local-user [domain <i>isp-name</i> idle-cut { disable enable } vlan <i>vlan-id</i> service-type { ftp lan-access ssh telnet terminal } state { active block } user-name <i>user-name</i>]	

Displaying and Maintaining RADIUS Protocol Configuration

To do...	Use the command...	Remarks
Display RADIUS message statistics about local RADIUS server	display local-server statistics	Available in any view
Display configuration information about one specific or all RADIUS schemes	display radius scheme [<i>radius-scheme-name</i>]	
Display RADIUS message statistics	display radius statistics	
Display buffered non-response stop-accounting requests	display stop-accounting-buffer { radius-scheme <i>radius-scheme-name</i> session-id <i>session-id</i> time-range <i>start-time stop-time</i> user-name <i>user-name</i> }	Available in user view
Delete buffered non-response stop-accounting requests	reset stop-accounting-buffer { radius-scheme <i>radius-scheme-name</i> session-id <i>session-id</i> time-range <i>start-time stop-time</i> user-name <i>user-name</i> }	
Clear RADIUS message statistics	reset radius statistics	

Displaying and Maintaining HWTACACS Protocol Configuration

To do...	Use the command...	Remarks
Display the configuration or statistic information about one specific or all HWTACACS schemes	display hwtacacs [<i>hwtacacs-scheme-name</i> [statistics]]	Available in any view
Display buffered non-response stop-accounting requests	display stop-accounting-buffer { hwtacacs-scheme <i>hwtacacs-scheme-name</i>	
Clear HWTACACS message statistics	reset hwtacacs statistics { accounting authentication authorization all }	Available in user view
Delete buffered non-response stop-accounting requests	reset stop-accounting-buffer hwtacacs-scheme <i>hwtacacs-scheme-name</i>	

AAA Configuration Examples

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.

Network requirements

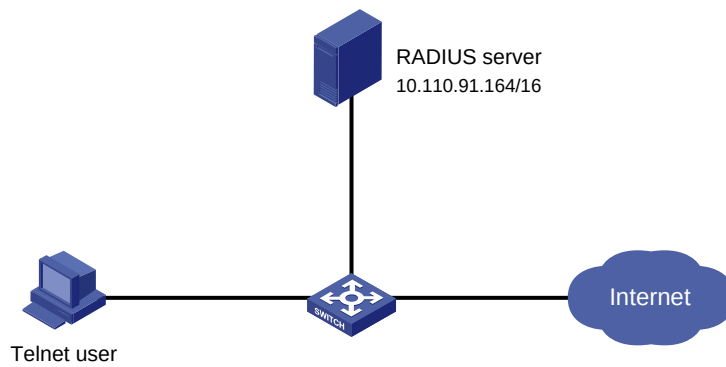
In the network environment shown in [Figure 2-2](#), you are required to configure the switch so that the Telnet users logging into the switch are authenticated by the RADIUS server.

- A RADIUS authentication server with IP address 10.110.91.164 is connected to the switch.
- On the switch, set the shared key it uses to exchange messages with the authentication RADIUS server to **aabbcc**.
- A CAMS server is used as the RADIUS server. You can select **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 **aabbcc**, set the authentication port number, and add Telnet usernames and login passwords.

The Telnet usernames 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 usernames to be sent to the RADIUS server in the RADIUS scheme.

Network diagram

Figure 2-2 Remote RADIUS authentication of Telnet users



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

Adopt AAA authentication for Telnet users.

```
[Sysname] user-interface vty 0 4
```

```
[Sysname-ui-vty0-4] authentication-mode scheme
```

```
[Sysname-ui-vty0-4] quit
```

Configure an ISP domain.

```
[Sysname] domain cams
```

```
[Sysname-isp-cams] access-limit enable 10
```

```
[Sysname-isp-cams] quit
```

Configure a RADIUS scheme.

```
[Sysname] radius scheme cams
```

```
[Sysname-radius-cams] accounting optional
```

```
[Sysname-radius-cams] primary authentication 10.110.91.164 1812
```

```
[Sysname-radius-cams] key authentication aabbcc
```

```
[Sysname-radius-cams] server-type Extended
```

```
[Sysname-radius-cams] user-name-format with-domain
```

```
[Sysname-radius-cams] quit
```

Associate the ISP domain with the RADIUS scheme.

```
[Sysname] domain cams
```

```
[Sysname-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.

Local Authentication of FTP/Telnet Users



Note

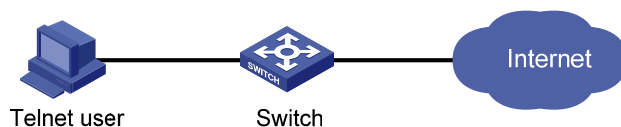
The configuration procedure for local authentication of FTP users is similar to that for Telnet users. The following text only takes Telnet users as example to describe the configuration procedure for local authentication.

Network requirements

In the network environment shown in [Figure 2-3](#), you are required to configure the switch so that the Telnet users logging into the switch are authenticated locally.

Network diagram

Figure 2-3 Local authentication of Telnet users



Configuration procedure

Method 1: Using local authentication scheme.

Enter system view.

```
<Sysname> system-view
```

Adopt AAA authentication for Telnet users.

```
[Sysname] user-interface vty 0 4
```

```
[Sysname-ui-vty0-4] authentication-mode scheme
```

```
[Sysname-ui-vty0-4] quit
```

Create and configure a local user named telnet.

```
[Sysname] local-user telnet
```

```
[Sysname-luser-telnet] service-type telnet
```

```
[Sysname-luser-telnet] password simple aabbcc
```

```
[Sysname-luser-telnet] quit
```

Configure an authentication scheme for the default "system" domain.

```
[Sysname] domain system
```

```
[Sysname-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 [Remote RADIUS Authentication of Telnet/SSH Users](#). However, you need to:

- Change the server IP address, and the UDP port number of the authentication server to 127.0.0.1, and 1645 respectively in the configuration step "Configure a RADIUS scheme" in [Remote RADIUS Authentication of Telnet/SSH Users](#).
- Enable the local RADIUS server function, set the IP address and shared key for the network access server to 127.0.0.1 and aabbcc, respectively.
- Configure local users.

HWTACACS Authentication and Authorization of Telnet Users

Network requirements

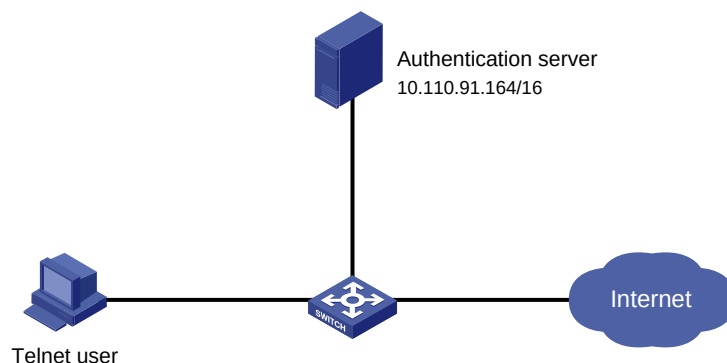
You are required to configure the switch so that the Telnet users logging into the switch are authenticated and authorized by the TACACS server.

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 **aabbcc**. Configure the switch to strip domain names off usernames before sending usernames to the TACACS server.

Configure the shared key to **aabbcc** on the TACACS server for exchanging messages with the switch.

Network diagram

Figure 2-4 Remote HWTACACS authentication and authorization of Telnet users



Configuration procedure

Add a Telnet user.

(Omitted here)

Configure a HWTACACS scheme.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwtac
[Sysname-hwtacacs-hwtac] primary authentication 10.110.91.164 49
[Sysname-hwtacacs-hwtac] primary authorization 10.110.91.164 49
[Sysname-hwtacacs-hwtac] key authentication aabbcc
[Sysname-hwtacacs-hwtac] key authorization aabbcc
[Sysname-hwtacacs-hwtac] user-name-format without-domain
[Sysname-hwtacacs-hwtac] quit
```



```
# Configure the domain name of the HWTACACS scheme to hwtac.
```

```
[Sysname] domain hwtacacs
```

```
[Sysname-isp-hwtacacs] scheme hwtacacs-scheme hwtac
```

Auto VLAN Configuration Example

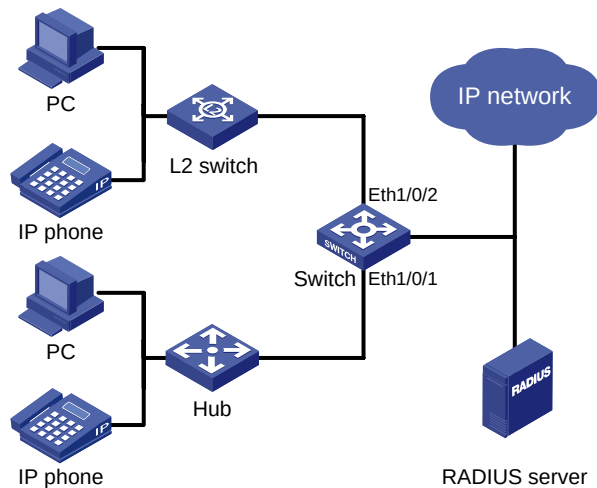
Network requirements

As shown in [Figure 2-5](#), use 802.1X authentication on Ethernet 1/0/1 and Ethernet 1/0/2 to authenticate users. After a user passes the authentication on a port, the RADIUS server issues a VLAN list to the switch, which assigns the authentication port to a VLAN that the IP phone needs to access. After that, the IP phone can access the network. The access control mode is port-based.

- All users belong to ISP domain **abc**; the RADIUS scheme is **bbb**;
- The RADIUS server is connected to Switch; the IP address of the RADIUS server is 1.1.1.1.
- The shared key used when Switch and the RADIUS server exchange packets is **hello**.

Network diagram

Figure 2-5 Network diagram for Auto VLAN configuration



Configuration procedure

- Configuration on the RADIUS server

The configuration may vary on different RADIUS servers. Configure VLAN lists on the RADIUS server by referring to [Configuring dynamic VLAN list assignment](#).

- Configuration on 802.1x clients

The configuration may vary on different 802.1x clients. Configure 802.1x clients by referring to related 802.1x client configuration guides.

- Configuration on the authentication switch

```
<Switch> system-view
```

```
# Configure the authentication scheme.
```

```
[Switch] radius scheme bbb
```

```
[Switch-radius-bbb] primary authentication 1.1.1.1
```

```
[Switch-radius-bbb] key authentication hello
```

```
[Switch-radius-bbb] primary accounting 1.1.1.1
```

```
[Switch-radius-bbb] key accounting hello
```

```

[Switch-radius-bbb] quit

# Create authentication domain aaa, and then enter domain view.
[Switch] domain aaa

# Configure the VLAN assignment mode in domain aaa as VLAN list.
[Switch-isp-aaa] vlan-assignment-mode vlan-list

# Specify the authentication scheme for the domain.
[Switch-isp-aaa] radius-scheme bbb
[Switch-isp-aaa] quit

# Configure the authentication scheme.
[Switch] radius scheme bbb
[Switch-radius-bbb] primary authentication 1.1.1.1
[Switch-radius-bbb] key authentication hello
[Switch-radius-bbb] primary accounting 1.1.1.1
[Switch-radius-bbb] key accounting hello

# Enable 802.1X authentication on Switch.
[Switch] dot1x

# Enable port-based 802.1X authentication on Ethernet 1/0/1.
[Switch] interface Ethernet1/0/1
[Switch-Ethernet1/0/1] dot1x
[Switch-Ethernet1/0/1] dot1x port-method portbased

# Enable port-based 802.1X authentication on Ethernet 1/0/2.
[Switch] interface Ethernet1/0/2
[Switch-Ethernet1/0/2] dot1x
[Switch-Ethernet1/0/2] dot1x port-method portbased

```

Troubleshooting AAA

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 username is not in the `userid@isp-name` or `userid.isp-name` format, or the default ISP domain is not correctly specified on the switch — Use the correct username 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.

Troubleshooting HWTACACS Configuration

See the previous section if you encounter an HWTACACS fault.

3 EAD Configuration

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.

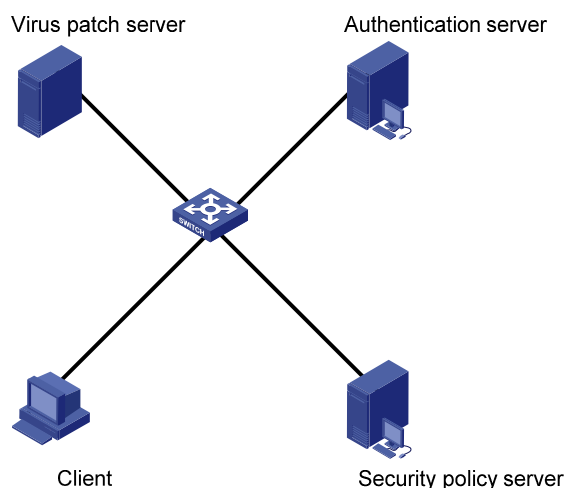
With EAD, a switch:

- 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.

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 3-1](#) shows a typical network application of EAD.

Figure 3-1 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.

EAD Configuration

The EAD configuration includes:

- Configuring the attributes of access users (such as username, 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 a RADIUS scheme.
- Configuring the IP address of the security policy server.
- Associating the ISP domain with the 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 [AAA Overview](#).

Follow these steps to configure EAD:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter RADIUS scheme view	radius scheme <i>radius-scheme-name</i>	—
Configure the RADIUS server type to extended	server-type extended	Required
Configure the IP address of a security policy server	security-policy-server <i>ip-address</i>	Required Each RADIUS scheme supports up to eight IP addresses of security policy servers.

EAD Configuration Example

Network requirements

In [Figure 3-2](#):

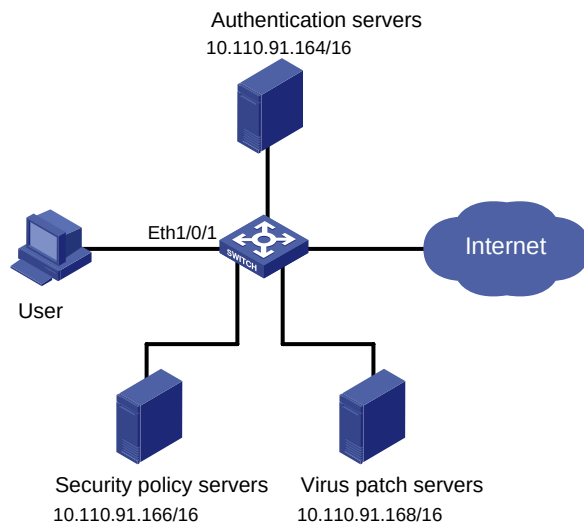
- A user is connected to Ethernet 1/0/1 on the switch.
- The user adopts 802.1x client supporting EAD extended function.
- You are required to configure the switch to use RADIUS server for remote user authentication and use security policy server for EAD control on users.

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.

Network diagram

Figure 3-2 EAD configuration



Configuration procedure

Configure 802.1x on the switch. Refer to “Configuring 802.1x” in *802.1x and System Guard Configuration*.

Configure a domain.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] quit
```

Configure a RADIUS scheme.

```
[Sysname] radius scheme cams
[Sysname-radius-cams] primary authentication 10.110.91.164 1812
[Sysname-radius-cams] accounting optional
[Sysname-radius-cams] key authentication expert
[Sysname-radius-cams] server-type extended
```

Configure the IP address of the security policy server.

```
[Sysname-radius-cams] security-policy-server 10.110.91.166
```

Associate the domain with the RADIUS scheme.

```
[Sysname-radius-cams] quit
[Sysname] domain system
[Sysname-isp-system] radius-scheme cams
```

Table of Contents

1 Web Authentication Configuration	1-1
Introduction to Web Authentication	1-1
Web Authentication Configuration	1-1
Configuration Prerequisites	1-1
Configuring Web Authentication	1-2
Configuring HTTPS Access for Web Authentication	1-3
Configuration Prerequisites	1-3
Configuration Procedure	1-3
Customizing Web Authentication Pages	1-4
Customizing Page Elements	1-4
Customizing Authentication Pages	1-5
Editing an Authentication Page File	1-5
Displaying and Maintaining Web Authentication	1-7
Web Authentication Configuration Example	1-7

1 Web Authentication Configuration



Note

- Support of setting the maximum online time for Web authentication users is added. See [Configuring Web Authentication](#).
 - Support of HTTPS access for Web Authentication is added. See [Configuring HTTPS Access for Web Authentication](#).
 - Support of customizing Web Authentication pages is added. See [Customizing Web Authentication Pages](#).
-

When configuring Web authentication, go to these sections for information you are interested in:

- [Introduction to Web Authentication](#)
- [Web Authentication Configuration](#)
- [Displaying and Maintaining Web Authentication](#)
- [Web Authentication Configuration Example](#)

Introduction to Web Authentication

Web authentication is a port-based authentication method that is used to control the network access rights of users. With Web authentication, users are freed from installing any special authentication client software.

With Web authentication enabled, before a user passes the Web authentication, it cannot access any network, except that it can access the authentication page or some free IP addresses. After the user passes the Web authentication, it can access any reachable networks.

Web Authentication Configuration

Configuration Prerequisites

Configure an ISP domain and an AAA RADIUS scheme for the domain before performing the following configurations.



Caution

- Web authentication can use only a RADIUS authentication scheme; it does not support local authentication.
- The user number limit configured under an AAA scheme does not take effect for Web authentication. Web authentication does not support accounting. Configure accounting for the AAA scheme as optional.

Configuring Web Authentication

Follow these steps to configure Web authentication:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the IP address and port number of the Web authentication server	web-authentication web-server ip <i>ip-address</i> [port <i>port-number</i>]	Required If no port number is specified, port 80 will be used. No Web authentication server is set by default.
Enable Web authentication globally	web-authentication enable	Required Disabled globally by default
Enable Web authentication on a port	interface <i>interface-type</i> <i>interface-number</i>	Required Disabled on port by default
	web-authentication select method { shared designated }	
	quit	
Set a free IP address range that can be accessed by users before Web authentication	web-authentication free-ip <i>ip-address</i> { <i>mask-length</i> <i>mask</i> }	Optional No such address range by default
Set an authentication-free user	web-authentication free-user ip <i>ip-address</i> mac <i>mac-address</i>	Optional No such user by default
Forcibly log out the specified or all users.	web-authentication cut connection { all mac <i>mac-address</i> user-name <i>user-name</i> interface <i>interface-type</i> <i>interface-number</i> }	Optional
Set the idle user checking interval for Web authentication	web-authentication timer idle-cut <i>timer</i>	Optional 900 seconds by default
Set the maximum online time for Web authentication users	web-authentication timer max-online <i>timer</i>	Optional 1800 seconds by default
Set the maximum number of online Web authentication	web-authentication max-connection <i>number</i>	Optional 128 users by default on a port,

To do...	Use the command...	Remarks
users	interface <i>interface-type</i> <i>interface-number</i>	and 512 users by default on a device
	web-authentication max-connection <i>number</i>	



Caution

- Before enabling global Web authentication, you should first set the IP address of a Web authentication server.
- Web authentication cannot be enabled when one of the following features is enabled, and vice versa: 802.1x, MAC authentication, port security, port aggregation and IRF.
- You can make Web authentication settings on individual ports before Web authentication is enabled globally, but they will not take effect. The Web authentication settings on ports take effect immediately once you enable Web authentication globally.
- A Web authentication client and the switch with Web authentication enabled must be able to communicate at the network layer so that the Web authentication page can be displayed on the Web authentication client.
- Web authentication is mutually exclusive with functions that depend on ACLs such as IP filtering, ARP intrusion detection, QoS, and port binding.
- After a user gets online in shared access method, if you configure an authentication-free user whose IP address and MAC address are the same as those of the online user, the online user will be forced to get offline.

Configuring HTTPS Access for Web Authentication

HTTP and HTTPS can be used for interaction between an authentication client and an access device:

- If HTTP is used, there are potential security problems because HTTP packets are transferred in plain text;
- If HTTPS is used, data security is ensured because HTTPS packets are transferred in ciphertext based on SSL.

After you configure HTTPS access for Web authentication on the switch, the switch will allow clients to use HTTPS to open the authentication pages for secure transmission of authentication information.

Configuration Prerequisites

To configure the access protocol as HTTPS, be sure to configure the PKI domain and SSL server policy, and request a certificate for the PKI domain at first. For information about SSL and PKI configuration, refer to *PKI Operation* and *SSL Operation* in this manual.

Configuration Procedure

Follow these steps to specify the access protocol for Web authentication:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify the access protocol	web-authentication protocol { http https server-policy <i>policy-name</i> }	Required HTTP is used by default.



Caution

- You must configure this command before enabling Web authentication. That is, after enabling Web authentication, you cannot change the access protocol for Web authentication.
- The SSL server policy must exist and, after the HTTPS access configuration, must not be removed.

Customizing Web Authentication Pages

The Web authentication device supports customizing authentication pages in the following ways:

- Use the default page framework and customize page elements as described in [Customizing Page Elements](#).
- Edit HTML files to push pictures, advertisements and the like to users. Refer to [Customizing Authentication Pages](#) and [Editing an Authentication Page File](#).

Customizing Page Elements

The default Web authentication page is a frame, which consists of four parts. The device allows you to customize the four parts in form of text strings.

Follow these steps to customize Web authentication page elements:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Customize the Web authentication page elements	web-authentication customize { corp-name <i>corporation-text</i> email <i>email-string</i> phone-num <i>phonenumber-string</i> platform-name <i>platform-text</i> }	Optional By default, there is no customized information on Web authentication pages.



Note

The **web-authentication customize** command is used to customize part of the information provided on the default authentication page. You cannot change the overall style of the authentication page. This is applicable to simple authentication pages.

Customizing Authentication Pages

The device also supports Web authentication pages totally developed by third parties as long as the authentication pages comply with rules of customizing the authentication page file. You can load such customized authentication pages to the device, providing authentication pages with richer contents and flexible styles.

Follow these steps to customize Web authentication pages:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure or modify the Web authentication page file	web-authentication customize file <i>fileName</i>	Optional By default, there is no customized authentication page file.



Note

- After you configure and load a Web authentication page file, the device will display the loaded Web authentication pages. The customized information (configured in section [Customizing Page Elements](#)) for the default authentication page will not be displayed.
- The file name specified by *fileName* must contain the system root directory and the relative path, such as **unit1>flash:/test.zip**.

Editing an Authentication Page File

With Web authentication, the device allows you to customize the Web authentication pages to be pushed to users. You can compress and then upload the customized authentication page files in HTML format to the local storage medium of the device. Each authentication page file includes seven main index pages, which are login page, login success page, login failure page, online page, system busy page, authentication-free page, and Logout success page.

A Web authentication page must comply with the authentication page file customization rules to ensure normal Web authentication and system operation.

Rules on file names

The main pages of the authentication pages have predefined file names, which cannot be changed. The following table lists the names.

Table 1-1 Main authentication page file names

Main authentication page	File name
Login page	login.htm
Login success page	loginSuccess.htm
Login failure page	loginFail.htm
Online page Pushed for online state notification	online.htm

Main authentication page	File name
System busy page Pushed when the system is busy or the user is in the login process	busy.htm
Authentication-free page	freeUser.htm
logout success page	logoutSuccess.htm



Note

You can define the names of the files other than the main authentication page files. The file names and directory names are case-insensitive.

Rules on page requests

The web authentication module supports only Post and Get requests.

- Get requests are used to get the static files in the authentication pages and allow no recursion. For example, if file Login.htm includes contents that perform Get action on file ca.htm, file ca.htm cannot include any reference to file Login.htm.
- Post requests are used when users submit username and password pairs, log on the system, and log off the system.

Rules on Post request attributes

- 1) Observe the following requirements when editing a form of an authentication page:
 - An authentication page can have multiple forms, but there must be one and only one form whose action is null. Otherwise, user information cannot be sent to the local portal server.
 - The username attribute is fixed as **WaUser**, and the password attribute is fixed as **WaPwd**.
 - Attribute **WaButton** is required to indicate the action that the user requests, which can be **Login** or **Logout**.
 - A login Post request must contain WaUser, WaPwd, and WaButton attributes.
 - A Logout Post request must contain the WaButton attribute.
- 2) Authentication pages **login.htm** and **loginFail.htm** must contain the login Post request.

The following example shows part of the script in page **login.htm**.

```
<form method = post >
<p>User name:<input type="text" name = "WaUser" style="width:160px;height:22px"
maxlength=64>
<p>Password :<input type="password" name = "WaPwd" style="width:160px;height:22px"
maxlength=32>
<p><input type=SUBMIT value="Login" name = "WaButton" style="width:60px;">
</form>
```

- 3) Authentication pages **loginSuccess.htm** and **online.htm** must contain the Logout Post request.

The following example shows part of the script in page **online.htm**.

```
<form action=login.cgi method = post >
<p><input type=SUBMIT value="Logout" name="WaButton" style="width:60px;">
```

</form>

Rules on page file compression and saving

- A set of authentication page files must be compressed into a standard zip file. A zip file name is in the form of *****.zip, and can contain only letters, numerals, and underscores.
- Zip files can be transferred to the device through FTP or TFTP.

Rules on file size and contents

For the system to push customized authentication pages smoothly, you need comply with the following size and content requirements on authentication pages.

- The size of the zip file of each set of authentication pages, including the main authentication pages and the page elements, must be no more than 500 KB.
- The size of a single page, including the main authentication page and the page elements, must be no more than 50 KB before being compressed.
- Page elements can contain only static contents such as HTML, JS, CSS, and pictures.

Displaying and Maintaining Web Authentication

To do...	Use the command...	Remarks
Display global and port Web authentication configuration information	display web-authentication configuration	Available in any view
Display information about specified or all online Web-authentication users.	display web-authentication connection { all interface interface-type interface-number user-name user-name }	

Web Authentication Configuration Example

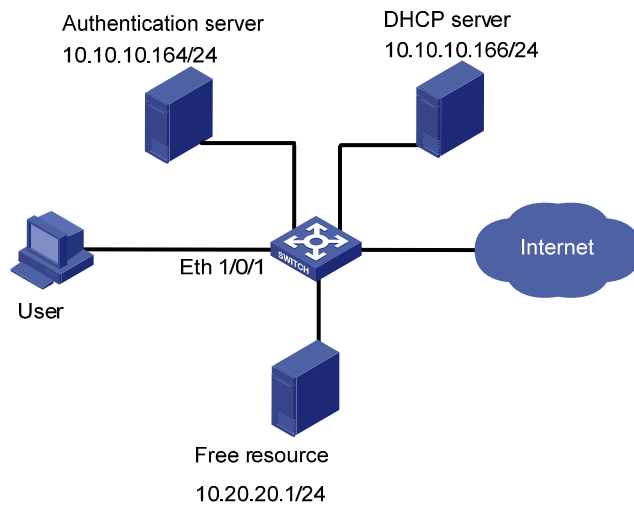
Network requirements

As shown in [Figure 1-1](#), a user connects to the Ethernet switch through port Ethernet 1/0/1.

- Configure the DHCP server so that users can obtain IP addresses from it.
- Configure Web authentication on Ethernet 1/0/1 to control the access of the user to the Internet.
- Configure a free IP address range, which can be accessed by the user before it passes the Web authentication.

Network diagram

Figure 1-1 Web authentication for user



Configuration procedure

Perform DHCP-related configuration on the DHCP server. (It is assumed that the user will automatically obtain an IP address through the DHCP server.)

Set the IP address and port number of the Web authentication server.

```
<Switch> system-view
```

```
[Switch] web-authentication web-server ip 10.10.10.10 port 8080
```

Configure a free IP address range, so that the user can access free resources before it passes the Web authentication.

```
[Switch] web-authentication free-ip 10.20.20.1 24
```

Enable Web authentication on Ethernet 1/0/1 and set the user access method to designated.

```
[Switch] interface Ethernet 1/0/1
```

```
[Switch-Ethernet1/0/1] web-authentication select method designated
```

Create RADIUS scheme radius1 and enter its view.

```
[Switch] radius scheme radius1
```

Set the IP address of the primary RADIUS authentication server.

```
[Switch-radius-radius1] primary authentication 10.10.10.164
```

Enable accounting optional.

```
[Switch-radius-radius1] accounting optional
```

Set the password that will be used to encrypt the messages exchanged between the switch and the RADIUS authentication server.

```
[Switch-radius-radius1] key authentication expert
```

Configure the system to strip domain name off a user name before transmitting the user name to the RADIUS server.

```
[Switch-radius-radius1] user-name-format without-domain
```

```
[Switch-radius-radius1] quit
```

Create ISP domain aabbcc.net for Web authentication users and enter the domain view.

```
[Switch] domain aabbcc.net
```

Configure domain aabbcc.net as the default user domain.

```
[Switch] domain default enable aabbcc.net
```

Reference scheme radius1 in domain aabbcc.net.

```
[Switch-isp-aabbcc.net] scheme radius-scheme radius1
```

Enable Web authentication globally. (It is recommended to take this step as the last step, so as to avoid the case that a valid user cannot access the network due to that some other related configurations are not finished.)

```
[Switch] web-authentication enable
```

Now, Web authentication takes effect. Before the user passes the Web authentication, it cannot access external networks and can only access the free resource.

The user can perform the following steps to access the Internet:

Step 1: Enter `http://10.10.10.10:8080` in the address column of IE. A page with the following prompt will be displayed: "Please input your name and the password!".

Step 2: Enter the correct user name and password and then click [login]. The following page will be displayed: "Authentication passed!".

Now the user can access external networks.

Table of Contents

1 MAC Address Authentication Configuration	1-1
MAC Address Authentication Overview	1-1
Performing MAC Address Authentication on a RADIUS Server	1-1
Performing MAC Address Authentication Locally	1-1
Related Concepts.....	1-2
MAC Address Authentication Timers	1-2
Quiet MAC Address.....	1-2
Configuring Basic MAC Address Authentication Functions	1-2
MAC Address Authentication Enhanced Function Configuration	1-4
MAC Address Authentication Enhanced Function Configuration Task List	1-4
Configuring a Guest VLAN	1-4
Configuring the Maximum Number of MAC Address Authentication Users Allowed to Access a Port	1-6
Displaying and Maintaining MAC Address Authentication Configuration	1-7
MAC Address Authentication Configuration Examples.....	1-7

1 MAC Address Authentication Configuration

When configuring MAC address authentication, go to these sections for information you are interested:

- [MAC Address Authentication Overview](#)
- [Related Concepts](#)
- [Configuring Basic MAC Address Authentication Functions](#)
- [MAC Address Authentication Enhanced Function Configuration](#)
- [Displaying and Maintaining MAC Address Authentication Configuration](#)
- [MAC Address Authentication Configuration Examples](#)

MAC Address Authentication Overview

MAC address authentication provides a way for authenticating users based on ports and MAC addresses, without requiring any client software to be installed on the hosts. Once detecting a new MAC address, it initiates the authentication process. During authentication, the user does not need to enter username or password manually.

For S3600 Series Ethernet switches, MAC address authentication can be implemented locally or on a RADIUS server.

After determining the authentication method, users can select one of the following types of user name as required:

- MAC address mode, where the MAC address of a user serves as the user name for authentication.
- Fixed mode, where user names and passwords are configured on a switch in advance. In this case, the user name, the password, and the limits on the total number of user names are the matching criterion for successful authentication. For details, refer to AAA of this manual for information about local user attributes.

Performing MAC Address Authentication on a RADIUS Server

When authentications are performed on a RADIUS server, the switch serves as a RADIUS client and completes MAC address authentication in cooperation with the RADIUS server.

- In MAC address mode, the switch sends the MAC addresses detected to the RADIUS server as both the user names and passwords, or sends the MAC addresses detected to the RADIUS server as the user names and uses the configured fixed password as the password.
- In fixed mode, the switch sends the user name and password previously configured for the user to the RADIUS server for authentication.

The RADIUS authentication process is the same as that of the 802.1x PAP authentication method. For details, refer to *802.1x and System-Guard Operation*.

A user can access a network upon passing the authentication performed by the RADIUS server.

Performing MAC Address Authentication Locally

When authentications are performed locally, users are authenticated by switches. In this case,

- In MAC address mode, the local user name to be configured is the MAC address of an access user, while the password may be the MAC address of the user or the fixed password configured (which is used depends on your configuration). Hyphens must or must not be included depending on the format configured with the **mac-authentication authmode usernameasmacaddress usernameformat** command; otherwise, the authentication will fail.
- In fixed mode, all users' MAC addresses are automatically mapped to the configured local passwords and usernames.
- The service type of a local user needs to be configured as lan-access.

Related Concepts

MAC Address Authentication Timers

The following timers function in the process of MAC address authentication:

- Offline detect timer: At this interval, the switch checks to see whether an online user has gone offline. Once detecting that a user becomes offline, the switch sends a stop-accounting notice to the RADIUS server.
- Quiet timer: Whenever a user fails MAC address authentication, the switch does not initiate any MAC address authentication of the user during a period defined by this timer.
- Server timeout timer: During authentication of a user, if the switch receives no response from the RADIUS server in this period, it assumes that its connection to the RADIUS server has timed out and forbids the user from accessing the network.

Quiet MAC Address

When a user fails MAC address authentication, the MAC address becomes a quiet MAC address, which means that any packets from the MAC address will be discarded simply by the switch until the quiet timer expires. This prevents an invalid user from being authenticated repeatedly in a short time.



Caution

If the quiet MAC is the same as the static MAC configured or an authentication-passed MAC, then the quiet function is not effective.

Configuring Basic MAC Address Authentication Functions

Follow these steps to configure basic MAC address authentication functions:

To do...	Use the command...		Remarks
Enter system view	system-view		—
Enable MAC address authentication globally	mac-authentication		Required Disabled by default
Enable MAC address authentication for the	In system view	mac-authentication interface <i>interface-list</i>	Use either method

To do...	Use the command...		Remarks
specified port(s) or the current port	In interface view	interface <i>interface-type interface-number</i>	Disabled by default
		mac-authentication	
		quit	
Set the user name in MAC address mode for MAC address authentication	mac-authentication authmode usernameasmacaddress [usernameformat { with-hyphen without-hyphen } { lowercase uppercase } fixedpassword <i>password</i>]		Optional By default, the MAC address of a user is used as the user name.
Set the user name in fixed mode for MAC address authentication	Set the user name in fixed mode for MAC address authentication	mac-authentication authmode usernamefixed	Optional By default, the user name is "mac" and no password is configured.
	Configure the user name	mac-authentication authusername <i>username</i>	
	Configure the password	mac-authentication authpassword <i>password</i>	
Specify an ISP domain for MAC address authentication	mac-authentication domain <i>isp-name</i>		Required The default ISP domain (default domain) is used by default.
Configure the MAC address authentication timers	mac-authentication timer { offline-detect <i>offline-detect-value</i> quiet <i>quiet-value</i> server-timeout <i>server-timeout-value</i> }		Optional The default timeout values are as follows: 300 seconds for offline detect timer; 60 seconds for quiet timer; and 100 seconds for server timeout timer



Caution

- If MAC address authentication is enabled on a port, you cannot configure the maximum number of dynamic MAC address entries for that port (through the **mac-address max-mac-count** command), and vice versa.
- If MAC address authentication is enabled on a port, you cannot configure port security (through the **port-security enable** command) on that port, and vice versa.
- You can configure MAC address authentication on a port before enabling it globally. However, the configuration will not take effect unless MAC address authentication is enabled globally.

MAC Address Authentication Enhanced Function Configuration

MAC Address Authentication Enhanced Function Configuration Task List

Complete the following tasks to configure MAC address authentication enhanced function:

Task	Remarks
Configuring a Guest VLAN	Optional
Configuring the Maximum Number of MAC Address Authentication Users Allowed to Access a Port	Optional

Configuring a Guest VLAN



Note

Different from Guest VLANs described in the *802.1x and System-Guard manual*, Guest VLANs mentioned in this section refer to Guests VLANs dedicated to MAC address authentication.

After completing configuration tasks in [Configuring Basic MAC Address Authentication Functions](#) for a switch, this switch can authenticate access users according to their MAC addresses or according to fixed user names and passwords. The switch will not learn MAC addresses of the clients failing in the authentication into its local MAC address table, thus prevent illegal users from accessing the network.

In some cases, if the clients failing in the authentication are required to access some restricted resources in the network (such as the virus library update server), you can use the Guest VLAN.

You can configure a Guest VLAN for each port of the switch. When a client connected to a port fails in MAC address authentication, this port will be added into the Guest VLAN automatically. The MAC address of this client will also be learned into the MAC address table of the Guest VLAN, and thus the user can access the network resources of the Guest VLAN.

After a port is added to a Guest VLAN, the switch will re-authenticate the first access user of this port (namely, the first user whose unicast MAC address is learned by the switch) periodically. If this user passes the re-authentication, this port will exit the Guest VLAN, and thus the user can access the network normally.

 Caution

- Guest VLANs are implemented in the mode of adding a port to a VLAN. For example, when multiple users are connected to a port, if the first user fails in the authentication, the other users can access only the contents of the Guest VLAN. The switch will re-authenticate only the first user accessing this port, and the other users cannot be authenticated again. Thus, if more than one client is connected to a port, you cannot configure a Guest VLAN for this port.
 - After users that are connected to an existing port failed to pass authentication, the switch adds the port to the Guest VLAN. Therefore, the Guest VLAN can separate unauthenticated users on an access port. When it comes to a trunk port or a hybrid port, if a packet itself has a VLAN tag and be in the VLAN that the port allows to pass, the packet will be forwarded perfectly without the influence of the Guest VLAN. That is, packets can be forwarded to the VLANs other than the Guest VLAN through the trunk port and the hybrid port, even users fail to pass authentication.
-

Follow these steps to configure a Guest VLAN:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the Guest VLAN for the current port	mac-authentication guest-vlan <i>vlan-id</i>	Required By default, no Guest VLAN is configured for a port by default.
Return to system view	quit	—
Configure the interval at which the switch re-authenticates users in Guest VLANs	mac-authentication timer guest-vlan-reauth <i>interval</i>	Optional By default, the switch re-authenticates the users in Guest VLANs at the interval of 30 seconds by default.



Caution

- If more than one client are connected to a port, you cannot configure a Guest VLAN for this port.
- When a Guest VLAN is configured for a port, only one MAC address authentication user can access the port. Even if you set the limit on the number of MAC address authentication users to more than one, the configuration does not take effect.
- The `undo vlan` command cannot be used to remove the VLAN configured as a Guest VLAN. If you want to remove this VLAN, you must remove the Guest VLAN configuration for it. Refer to the VLAN module in this manual for the description on the `undo vlan` command.
- Only one Guest VLAN can be configured for a port, and the VLAN configured as the Guest VLAN must be an existing VLAN. Otherwise, the Guest VLAN configuration does not take effect. If you want to change the Guest VLAN for a port, you must remove the current Guest VLAN and then configure a new Guest VLAN for this port.
- 802.1x authentication cannot be enabled for a port configured with a Guest VLAN.
- The Guest VLAN function for MAC address authentication does not take effect when port security is enabled.

Configuring the Maximum Number of MAC Address Authentication Users Allowed to Access a Port

You can configure the maximum number of MAC address authentication users for a port in order to control the maximum number of users accessing a port. After the number of access users has exceeded the configured maximum number, the switch will not trigger MAC address authentication for subsequent access users, and thus these subsequent access users cannot access the network normally.

Follow these steps to configure the maximum number of MAC address authentication users allowed to access a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the maximum number of MAC address authentication users allowed to access a port	mac-authentication max-auth-num <i>user-number</i>	Required By default, the maximum number of MAC address authentication users allowed to access a port is 256.



Caution

- If both the limit on the number of MAC address authentication users and the limit on the number of users configured in the port security function are configured for a port, the smaller value of the two configured limits is adopted as the maximum number of MAC address authentication users allowed to access this port. Refer to the *Port Security manual* for the description on the port security function.
- You cannot configure the maximum number of MAC address authentication users for a port if any user connected to this port is online.

Displaying and Maintaining MAC Address Authentication Configuration

To do...	Use the command...	Remarks
Display global or on-port information about MAC address authentication	display mac-authentication [interface <i>interface-list</i>]	Available in any view
Clear the statistics of global or on-port MAC address authentication	reset mac-authentication statistics [interface <i>interface-type</i> <i>interface-number</i>]	Available in user view

MAC Address Authentication Configuration Examples

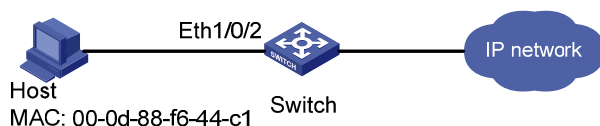
Network requirements

As illustrated in [Figure 1-1](#), a supplicant is connected to the switch through port Ethernet 1/0/2.

- MAC address authentication is required on port Ethernet 1/0/2 to control user access to the Internet.
- All users belong to domain aabbcc.net. The authentication performed is locally and the MAC address of the PC (00-0d-88-f6-44-c1) is used as both the user name and password.

Network Diagram

Figure 1-1 Network diagram for MAC address authentication configuration



Configuration Procedure

Enable MAC address authentication on port Ethernet 1/0/2.

```
<Sysname> system-view
```

```
[Sysname] mac-authentication interface Ethernet 1/0/2
```


Set the user name in MAC address mode for MAC address authentication, requiring hyphenated lowercase MAC addresses as the usernames and passwords.

```
[Sysname] mac-authentication authmode usernameasmacaddress usernameformat with-hyphen lowercase
```

Add a local user.

- Specify the user name and password.

```
[Sysname] local-user 00-0d-88-f6-44-c1
```

```
[Sysname-luser-00-0d-88-f6-44-c1] password simple 00-0d-88-f6-44-c1
```

- Set the service type to **lan-access**.

```
[Sysname-luser-00-0d-88-f6-44-c1] service-type lan-access
```

```
[Sysname-luser-00-0d-88-f6-44-c1] quit
```

Add an ISP domain named aabbcc.net.

```
[Sysname] domain aabbcc.net
```

New Domain added.

Specify to perform local authentication.

```
[Sysname-isp-aabbcc.net] scheme local
```

```
[Sysname-isp-aabbcc.net] quit
```

Specify aabbcc.net as the ISP domain for MAC address authentication

```
[Sysname] mac-authentication domain aabbcc.net
```

Enable MAC address authentication globally (This is usually the last step in configuring access control related features. Otherwise, a user may be denied of access to the networks because of incomplete configuration.)

```
[Sysname] mac-authentication
```

After doing so, your MAC address authentication configuration will take effect immediately. Only users with the MAC address of 00-0d-88-f6-44-c1 are allowed to access the Internet through port Ethernet 1/0/2.

Table of Contents

1 VRRP Configuration	1-1
VRRP Overview	1-1
Introduction to VRRP Group	1-2
Virtual Router Overview	1-4
VRRP Timer	1-5
VRRP Tracking	1-5
Operation Procedure of VRRP	1-6
Periodical sending of ARP packets in a VRRP Group	1-7
VRRP Configuration	1-7
Configuring Basic VRRP Functions	1-7
Configuring Advanced VRRP Functions	1-8
Displaying and Maintaining VRRP	1-10
VRRP Configuration Examples	1-10
Single-VRRP Group Configuration	1-10
VRRP Tracking Interface Configuration	1-13
Multiple-VRRP Group Configuration	1-15
Port Tracking Configuration Examples	1-16
Troubleshooting VRRP	1-18

1 VRRP Configuration

When configuring VRRP, go to these sections for information you are interested in:

- [VRRP Overview](#)
- [VRRP Configuration](#)
- [Displaying and Maintaining VRRP](#)
- [VRRP Configuration Examples](#)
- [Troubleshooting VRRP](#)



Note

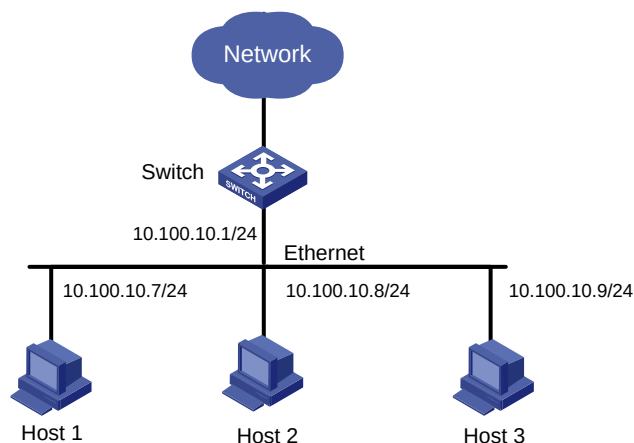
S3600-SI series Ethernet Switches support VRRP in Release 1702.

VRRP Overview

As shown in [Figure 1-1](#), the following occasions may occur in a stable network:

- All the hosts in a network set the same gateway as their next hop, whose IP address is also known as the next hop address of the default route (for example, the next hop address of the default route is 10.100.10.1 in [Figure 1-1](#)).
- The Switch in the figure acts as the gateway of all the hosts in the network, and forwards the hosts' packets destined for other network segments, so as to realize the communication between the hosts and the external network.
- If Switch fails, all the hosts on this segment taking Switch as the default gateway are cut off from the external network.

Figure 1-1 LAN networking



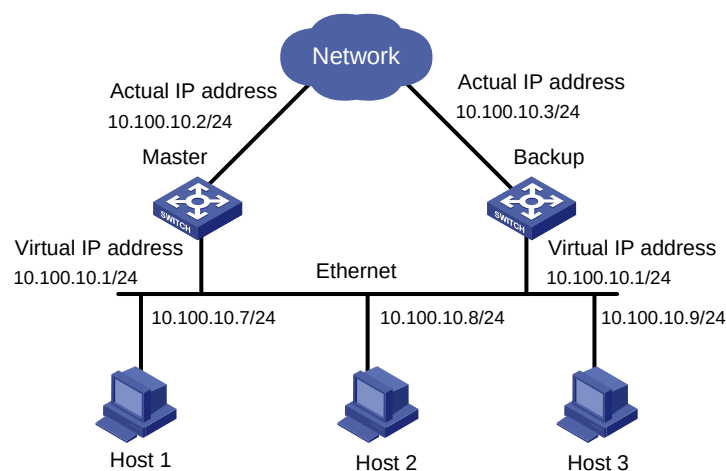
The networking illustrated in [Figure 1-1](#) requires high stability of the default gateway. Normally, adding egress gateways is used to improve the system reliability. In this case, how to route between multiple egresses needs to be solved.

Virtual Router Redundancy Protocol (VRRP), an error-tolerant protocol defined in RFC 2338, well solves the problem mentioned above through separating physical devices and logical devices. In LANs with multicast or broadcast capabilities (such as Ethernet), VRRP can avoid single point failure through establishing backup links without modifying the configuration of dynamic routing protocols and router discovery protocols.

Introduction to VRRP Group

VRRP allows you to combine a group of LAN switches (including a master and several backups) into a VRRP group. The VRRP group functions as a virtual router, forwarding packets as a gateway.

Figure 1-2 VRRP network diagram



As shown in [Figure 1-2](#), a VRRP group has the following features:

- The virtual router (the VRRP group) has its own IP address (10.100.10.1 in the above figure).
- The switches within the VRRP group must have their own IP addresses (such as 10.100.10.2 for the master and 10.100.10.3 for the backup).
- Hosts in the LAN use the IP address of the virtual router (that is, 10.100.10.1) as their default gateway.
- Hosts in 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 and 10.100.10.3 of the backup.

If the master in the VRRP group goes down, the backups in the VRRP group will reelect a master by priority. The backup with the highest priority functions as the new master to guarantee normal communication between the hosts and the external networks.

Priority of a switch in a VRRP group

You can configure the priority of a switch in a VRRP group. A master is elected from these VRRP-enabled switches by priority and the remaining switches are backups. The master in a VRRP group is the one currently with the highest priority.

Switch priority ranges from 0 to 255 (a larger number indicates a higher switch priority). Note that only 1 through 254 are available to users. Switch priorities 0 and 255 are reserved for special uses and the IP address owner respectively.

When a switch acts as the IP address owner, its priority is always 255. That is, if there is an IP address owner in a VRRP group, it acts as the master as long as it works properly.



Note

If two switches have the same VRRP priority, the one whose VLAN interface takes effect earlier becomes the master.

Preemptive mode and preemption delay of a switch in a VRRP group

You can configure an S3600 Ethernet switch to operate in preemptive mode.

- In non-preemptive mode, as long as a switch in a VRRP group becomes the master, it stays as the master as long as it operates normally, even if a backup is assigned a higher priority later.
- If all the switches in a VRRP group are set to operate in preemptive mode, a backup sends VRRP advertisements when it finds that its priority is higher than that of the current master. In this case a new election of master is triggered, and the backup becomes the master and the former master becomes a backup accordingly.

You can also set the preemption delay for an S3600 switch.

Setting a delay period aims at:

- In an unstable network, backups in a VRRP group possibly cannot receive VRRP advertisements from the master in time due to network congestions. In this case, the backup considers itself as the master and sends out VRRP advertisements to elect master. This causes the master of the VRRP group to be determined frequently.
- With preemption delay configured, if a backup does not receive VRRP advertisements from the master in time, it waits for a while before switching to a new master. The backup does not send VRRP advertisements if it receives VRRP advertisements from the master during the specified delay period.

Authentication type and authentication key of a switch in a VRRP group

VRRP provides the following authentication types:

- **simple**: Simple text authentication. In a network under possible security threat, the authentication type can be set to **simple**. With the **simple** authentication type configured, the switch adds an authentication key into a VRRP packet before transmitting it. The receiver then compares 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 illegal and discarded.
- **md5**: MD5 authentication. In a vulnerable network, the authentication type can be set to **md5**. The switch then uses the authentication type provided in the Authentication Header and the local MD5 algorithm to authenticate the VRRP packets. Packets that fail to pass the authentication are discarded. The switch then sends trap messages to the NMS.

Virtual Router Overview

VRRP group and virtual router IP address configuration

To create a VRRP group, you need to configure an IP address for the VRRP group virtual router. The VRRP group is automatically created after you configure the first IP address for the VRRP group virtual router. Other IP addresses configured for the virtual router after this one are just added to the IP address list of the virtual router.

The virtual router IP address has the following features:

- The IP address of the virtual router can be an unassigned IP address in the network segment where a member switch of the VRRP group resides.
- You can specify the virtual router IP address as the IP address used by a member switch in the VRRP group. In this case, the member switch is called an IP address owner.
- The virtual router IP address and the IP addresses used by the member switches in the VRRP group must belong to the same network segment. If not, the VRRP 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 VRRP group is removed after all its virtual router IP addresses are removed. In this case, all the configurations performed for the VRRP group are disabled.



Note

Do not configure a host IP address as the IP address of the virtual router. If your host IP address is the same as the virtual router IP address of the VRRP group, all the packets sent to the current network segment will be sent to your host. As a result, packets in the network segment cannot be forwarded properly.

Response of the virtual router to the ping operations

According to the standard VRRP, a running virtual router does not respond to the **ping** operations, so that you cannot use the **ping** command to check the network connectivity and whether the configuration of the IP address of a virtual router is successful.

For S3600 series Ethernet switches, you can specify whether the switches in a VRRP group respond to the **ping** operations destined for the virtual router IP addresses.

Mapping relationship between virtual router IP addresses and MAC addresses

You can set the mapping between the IP address of the virtual router and the MAC addresses of the member switches of a VRRP group, so that packets sent from the hosts in the network can be forwarded to the correct gateway according to the saved MAC address forwarding table.

There are two types of mapping between the virtual router IP address and the MAC addresses:

- Virtual router IP address-to-virtual MAC address mapping. By default, a virtual MAC address is automatically created after a virtual router IP address is configured. Hosts send packets to gateways for layer 3 forwarding according to this virtual MAC address. For S3600 series Ethernet switches, you can map multiple virtual router IP addresses of the VRRP group to one virtual MAC address.

- Virtual router IP address-to-real MAC address mapping. When there is an IP address owner in the VRRP group, a virtual router IP address may correspond to two MAC addresses, a real MAC address of the IP address owner and a virtual MAC address created by default. In this case, you can map virtual router IP addresses to the real MAC address. Then hosts send packets to the IP address owner for layer 3 forwarding according to the real MAC address.



Note

- You need to configure the mapping between the IP addresses of the VRRP group and the MAC address before enabling VRRP feature on an S3600 Ethernet switch. If VRRP is already enabled, the system does not support this configuration.
 - The number of virtual router IP addresses that can be mapped with the virtual router MAC address is determined by the chips of the switches in the VRRP group.
 - A switch can belong to multiple VRRP groups. However, the number of VRRP groups supported by a switch is determined by the chip it uses. Refer to device specification for details.
-

VRRP Timer

There are two types of VRRP timer, the VRRP advertisement interval timer and the VRRP preemption delay timer.

VRRP advertisement interval timer

- The master advertises its normal operation state to the switches within the VRRP group by sending VRRP packets once in each specified interval (determined by the *adver-interval* argument).
- You can adjust the interval for a master to send VRRP advertisements by setting the VRRP advertisement interval timer. If a backup does not receive the VRRP advertisements from the master after a period three times of the specified interval, it considers itself as the master and sends out VRRP advertisements to reelect the master.

VRRP preemption delay timer

- The backup may not receive a VRRP advertisement within a period three times of the specified interval due to excessive network traffic or network instability. In this case, you can configure the VRRP preemption delay for backups.
- If you configure the preemption delay for a backup, the switch preempts the master if it does not receive a VRRP advertisement from the master after it waits for a period three times of the advertisement interval and the period specified by the preemption delay.

VRRP Tracking



Note

- If an IP address owner exists in a VRRP group, you can configure a priority for the IP address owner. However your configuration will not take effect and the IP address owner will still be the master of the VRRP group because the system considers the priority of the IP address owner to be 255 always.
 - If an IP address owner exists in a VRRP group, the interface/port tracking function configured on the IP address owner cannot take effect.
-

Interface tracking function of the VRRP group

When the VLAN interface of the master goes down, if you want the specified backup to become the master, you can use the interface tracking function. With this function enabled for the VRRP group:

- If the tracked VLAN interface of the master goes down, the priority of the switch decreases automatically by a specified value.
- The decrease of the master priority makes the priority of the backup tracking the interface become higher, and thus the backup becomes the new master.

Port tracking function of the VRRP group

When a physical port of the master goes down, if you want the specified backup to become the master, you can use the port tracking function. With this function enabled for the VRRP group:

- If the tracked physical port of the master goes down, the priority of the master decreases automatically by a set value.
 - The decrease of the master priority makes the priority of the backup tracking the port become higher, and thus the backup becomes the new master.
-



Note

You can enable Auto Detect on the master switch in a VRRP group, use the Auto Detect function to detect the routes from the master switch to other networks, and use the detection results (reachable/unreachable) to control the priority of the master switch, so as to realize the automatic master-backup switchover. For details, please refer to *Auto Detect Operation* in this manual.

Operation Procedure of VRRP

- With VRRP enabled, the switches determine their respective roles in a VRRP group by priority. The switch with the highest priority acts as the master, which will forward packets to outside networks, and the switches with lower priorities act as backups. The master sends VRRP advertisements periodically to notify that it is operating normally.
- When a backup receives a VRRP advertisement, it compares its own priority with that in the advertisement. If its priority is lower, it remains as a backup. Otherwise, it becomes the master.
- A backup starts the advertisement interval timer after it receives the advertisement to wait for the next one from the master. If the backup does not receive VRRP advertisements from the master

after the timer expires, it considers that the master fails and starts the election process to elect a new master for forwarding packets.

Periodical sending of ARP packets in a VRRP Group

If a VRRP group exists on a network, the master sends gratuitous ARP packets periodically to hosts on the network, which then update their local ARP tables, ensuring that no device on this network uses the same IP address with the VRRP virtual router.

As you can create mappings between the IP address and MAC address of the VRRP virtual router, there are two cases:

- If the IP address of the virtual router corresponds to a virtual MAC address, the source MAC address in the gratuitous ARP packet will be the virtual MAC address.
- If the IP address of the virtual router corresponds to an actual MAC address, the source MAC address in the gratuitous ARP packet will be the VLAN interface's MAC address of the master in the VRRP group.



Note

For more information about ARP, refer to the ARP section in the part discussing ARP-MFF in this manual.

VRRP Configuration

Configuring Basic VRRP Functions

Follow these steps to configure the basic VRRP functions:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure response of the virtual router to the ping operations	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 VRRP group is mapped to the virtual MAC address.
Create a VLAN	vlan <i>vlan-id</i>	— This operation creates the VLAN to which the VRRP group corresponds. The <i>vlan-id</i> argument is the ID of the VLAN.
Return to system view	quit	—
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	—

To do...	Use the command...	Remarks
Create a VRRP group or add a virtual router IP address	vrrp vrid <i>virtual-router-id</i> virtual-ip <i>virtual-address</i>	Required
Configure the priority of the VRRP group	vrrp vrid <i>virtual-router-id</i> priority <i>priority</i>	Optional 100 by default.



Note

It is not recommended to configure features related to VRRP group on the Layer 3 interface of a remote-probe VLAN. Otherwise, packet mirroring may be affected.

Configuring Advanced VRRP Functions

Complete these tasks to configure advanced VRRP functions

Task		Remarks
Advanced VRRP configuration	Configuring the preemptive mode and preemption delay for a switch	Optional
	Configuring VRRP authentication type and authentication key for a member switch	Optional
	Configuring VRRP timer	Optional
	Configuring VRRP Tracking	Optional

Configuring the preemptive mode and preemption delay for a switch

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	—
Configure a virtual router IP address	vrrp vrid <i>virtual-router-id</i> virtual-ip <i>virtual-address</i>	Required
Configure the preemptive mode and preemption delay for the switches in the VRRP group	vrrp vrid <i>virtual-router-id</i> preempt-mode [timer delay <i>delay-value</i>]	Required By default, preemptive mode is set for the VRRP group and the preemption delay is 0 seconds.

Configuring VRRP authentication type and authentication key for a member switch

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	—

To do...	Use the command...	Remarks
Configure a virtual router IP address	vrrp vrid <i>virtual-router-id</i> virtual-ip <i>virtual-address</i>	Required
Configure the authentication type and authentication key	vrrp vrid <i>virtual-router-id</i> authentication-mode <i>authentication-type</i> <i>authentication-key</i>	Optional No authentication is performed by default.

Configuring VRRP timer

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface <i>Vlan-interface</i> <i>vlan-id</i>	—
Configure a virtual router IP address	vrrp vrid <i>virtual-router-id</i> virtual-ip <i>virtual-address</i>	Required
Configure the VRRP timer	vrrp vrid <i>virtual-router-id</i> timer advertise <i>adver-interval</i>	Optional 1 second by default.

Configuring VRRP Tracking

Follow these steps to configure VRRP tracking:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface <i>Vlan-interface</i> <i>vlan-id</i>	—
Configure a virtual router IP address	vrrp vrid <i>virtual-router-id</i> virtual-ip <i>virtual-address</i>	Required
Enable the interface tracking function	vrrp vrid <i>virtual-router-id</i> track interface <i>vlan-interface</i> <i>vlan-id</i> [reduced <i>value-reduced</i>]	Optional By default, the VLAN interface priority decreases by 10.
Return to system view	quit	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the port tracking function	vrrp <i>vlan-interface</i> <i>vlan-id</i> vrid <i>virtual-router-id</i> track [reduced <i>value-reduced</i>]	Required By default, the port priority decreases by 10.



Note

- The port to be tracked can be in the VLAN which the VLAN interface of the VRRP group belongs to.
- Up to eight ports can be tracked simultaneously through the port tracking function.
- You can enable Auto Detect on the master switch in a VRRP group, use the Auto Detect function to detect the routes from the master switch to other networks, and use the detection results (reachable/unreachable) to control the priority of the master switch, so as to realize the automatic master-backup switchover. For details, please refer to *Auto Detect Operation* in this manual.

Displaying and Maintaining VRRP

To do...	Use the command...	Remarks
Display VRRP statistics information	display vrrp statistics [interface vlan-interface <i>vlan-id</i> [vrid <i>virtual-router-id</i>]]	Available in any view
Display VRRP state information	display vrrp [verbose] [interface vlan-interface <i>vlan-id</i> [vrid <i>virtual-router-id</i>]]	
Clear VRRP statistics information	reset vrrp statistics [interface vlan-interface <i>vlan-id</i> [vrid <i>virtual-router-id</i>]]	Available in user view

VRRP Configuration Examples

Single-VRRP Group Configuration

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 group is as follows:

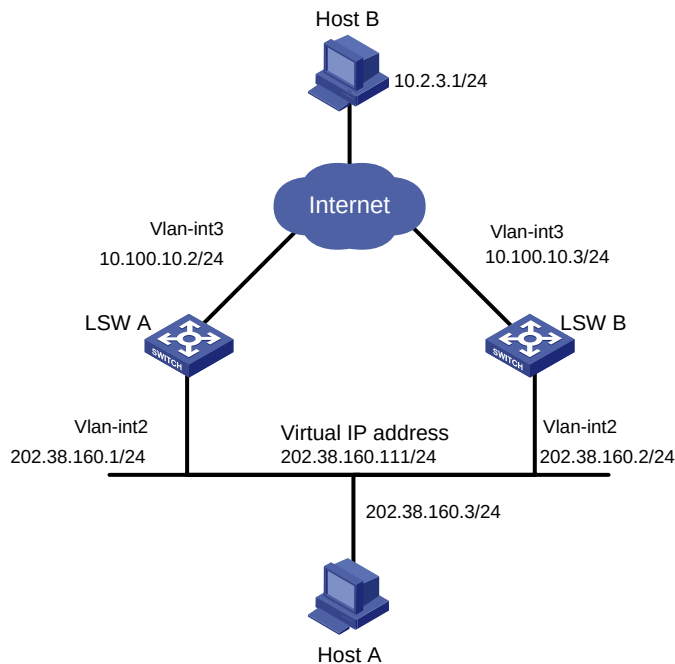
- VRRP group ID: 1
- Virtual router IP address: 202.38.160.111/24
- Master: Switch A
- Backup: Switch B
- Preemptive mode: enabled

Table 1-1 Network description

Switch	Ethernet port connecting to Host A	IP address of the VLAN interface	Switch priority in the VRRP 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

Network diagram

Figure 1-3 Network diagram for single-VRRP group configuration



Configuration procedure

- Configure Switch A.

Configure VLAN 3.

```
<LSW-A> system-view
[LSW-A] vlan 3
[LSW-A-vlan3] port Ethernet1/0/10
[LSW-A-vlan3] quit
[LSW-A] interface Vlan-interface 3
[LSW-A-Vlan-interface3] ip address 10.100.10.2 255.255.255.0
[LSW-A-Vlan-interface3] quit
```

Configure VLAN 2.

```
[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 VRRP group to respond to ping operations destined for its virtual router IP address.

```
[LSW-A] vrrp ping-enable
```

Create a VRRP group.

```
[LSW-A] interface Vlan-interface 2
[LSW-A-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Set the priority for Switch A in the VRRP group.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 priority 110
# Configure the preemptive mode for the VRRP group.
[LSW-A-Vlan-interface2] vrrp vrid 1 preempt-mode
```



Note

By default, a VRRP group adopts the preemptive mode.

- Configure Switch B.

Configure VLAN 3.

```
<LSW-B> system-view
[LSW-B] vlan 3
[LSW-B-vlan3] port Ethernet1/0/10
[LSW-B-vlan3] quit
[LSW-B] interface Vlan-interface 3
[LSW-B-Vlan-interface3] ip address 10.100.10.3 255.255.255.0
[LSW-B-Vlan-interface3] quit
```

Configure VLAN 2.

```
[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 VRRP group to respond to ping operations destined for its virtual router IP address.

```
[LSW-B] vrrp ping-enable
```

Create a VRRP 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 VRRP group.

```
[LSW-B-Vlan-interface2] vrrp vrid 1 preempt-mode
```

The IP address of the default gateway of Host A is configured as 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 after recovery.

VRP Tracking Interface Configuration

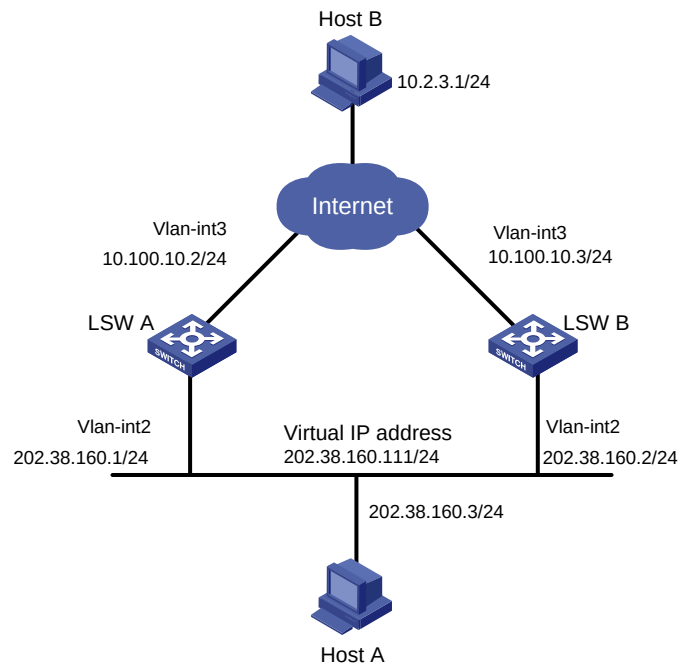
Network requirements

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 group ID is set to 1, with configurations of authorization key and timer.

Network diagram

Figure 1-4 Network diagram for interface tracking configuration



Configuration procedure

- Configure Switch A.

Configure VLAN 3.

```
<LSW-A> system-view
[LSW-A] vlan 3
[LSW-A-vlan3] port Ethernet1/0/10
[LSW-A-vlan3] quit
[LSW-A] interface Vlan-interface 3
[LSW-A-Vlan-interface3] ip address 10.100.10.2 255.255.255.0
[LSW-A-Vlan-interface3] quit
```

Configure VLAN 2.

```
[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 VRRP 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 VRRP group.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 priority 110
```

Set the authentication type for the VRRP group to **md5**, and the password to **abc123**.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 authentication-mode md5 abc123
```

Configure the master 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 interface Vlan-interface 3 reduced 30
```

- Configure switch B.

Configure VLAN 3.

```
<LSW-B> system-view
```

```
[LSW-B] vlan 3
```

```
[LSW-B-vlan3] port Ethernet1/0/10
```

```
[LSW-B-vlan3] quit
```

```
[LSW-B] interface Vlan-interface 3
```

```
[LSW-B-Vlan-interface3] ip address 10.100.10.3 255.255.255.0
```

```
[LSW-B-Vlan-interface3] quit
```

Configure VLAN 2.

```
[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 through.

```
[LSW-B] vrrp ping-enable
```

Create a VRRP 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 VRRP group.

```
[LSW-B-Vlan-interface2] vrrp vrid 1 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-interface 3 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-interface 3 recovers, switch A will resume its gateway function as the master.

Multiple-VRRP Group Configuration

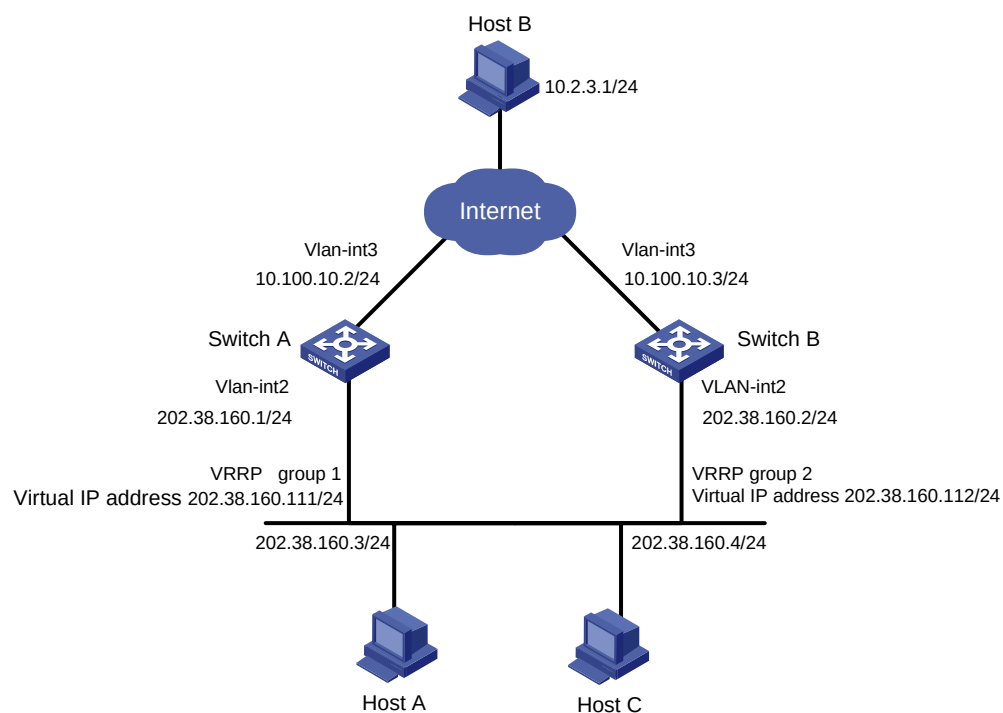
Network requirements

A switch can function as a backup of multiple VRRP groups.

Multiple-VRRP group configuration can implement load balancing. For example, Switch A acts as the master of VRRP group 1 and a backup in VRRP group 2. Similarly, Switch B acts as the master of VRRP group 2 and a backup in VRRP 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.

Network diagram

Figure 1-5 Network diagram for multiple-VRRP group configuration



Configuration procedure

- Configure Switch A.

Configure VLAN 3.

```
<LSW-A> system-view
[LSW-A] vlan 3
[LSW-A-vlan3] port Ethernet1/0/10
[LSW-A-vlan3] quit
[LSW-A] interface Vlan-interface 3
[LSW-A-Vlan-interface3] ip address 10.100.10.2 255.255.255.0
[LSW-A-Vlan-interface3] quit
```

Configure VLAN 2.

```
[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 VRRP group 1.
[LSW-A-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111

# Set the priority for VRRP group 1.
[LSW-A-Vlan-interface2] vrrp vrid 1 priority 150

# Create VRRP group 2.
[LSW-A-Vlan-interface2] vrrp vrid 2 virtual-ip 202.38.160.112

```

- Configure Switch B.

```

# Configure VLAN 3.
<LSW-B> system-view
[LSW-B] vlan 3
[LSW-B-vlan3] port Ethernet1/0/10
[LSW-B-vlan3] quit
[LSW-B] interface Vlan-interface 3
[LSW-B-Vlan-interface3] ip address 10.100.10.3 255.255.255.0
[LSW-B-Vlan-interface3] quit

# Configure VLAN 2.
[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 VRRP group 1.
[LSW-B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111

# Create VRRP group 2.
[LSW-B-Vlan-interface2] vrrp vrid 2 virtual-ip 202.38.160.112

# Set the priority for VRRP group 2.
[LSW-B-Vlan-interface2] vrrp vrid 2 priority 110

```



Note

Normally, multiple VRRP groups are used in actual use.

Port Tracking Configuration Examples

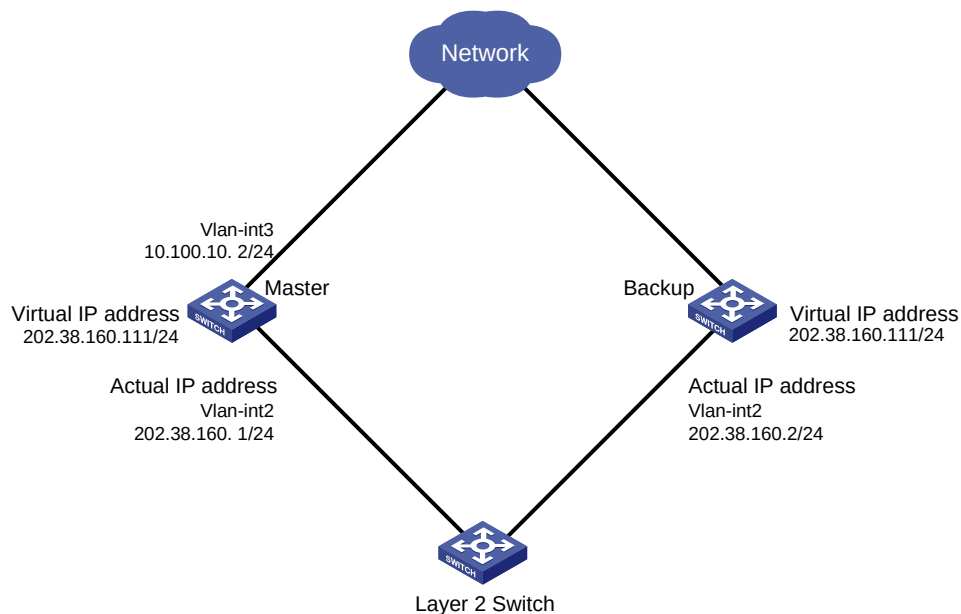
Network requirements

- VRRP group 1 comprises two switches, which act as the master and the backup.

- The actual IP addresses of the master and the backups are 10.100.10.2 and 10.100.10.3 respectively.
- The master is connected to the upstream network through its Ethernet 1/0/1 port. The backup is connected to the upstream network through its Ethernet 1/0/2 port.
- The virtual router IP address of the VRRP group is 10.100.10.1.
- Enable the port tracking function on Ethernet 1/0/1 port of the master and specify that the priority of the master decreases by 50 when Ethernet 1/0/1 port fails, which triggers new master being determined in the VRRP group 1.

Network diagram

Figure 1-6 Network diagram for VRRP port tracking configuration



Configuration procedure

- Configure the master switch.

Enter system view.

```
<Sysname> system-view
```

Create VLAN 3.

```
[Sysname] vlan 3
```

```
[Sysname-vlan3] port Ethernet1/0/1
```

```
[Sysname-vlan3] quit
```

Configure VLAN-interface 3.

```
[Sysname] interface Vlan-interface 3
```

```
[Sysname-Vlan-interface3] ip address 10.100.10.2 255.255.255.0
```

```
[Sysname-Vlan-interface3] quit
```

Create VLAN 2.

```
[Sysname] vlan 2
```

```
[Sysname-vlan2] port Ethernet1/0/2
```

```
[Sysname-vlan2] quit
```

Configure VLAN-interface 2.

```

[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
[Sysname-Vlan-interface2] quit

# Create a VRRP group.

[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111

# Enter Ethernet 1/0/1 port view and enable the VRRP tracking function.

[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] vrrp Vlan-interface 2 vrid 1 track reduced 50

```

Troubleshooting VRRP

You can locate VRRP problems through the configuration and debugging information. Here are some possible symptoms you might meet and the corresponding troubleshooting methods.

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 VRRP group, or the attempt of other devices sending illegal VRRP packets.

- The first possible fault can be solved through modifying the configuration.
- The second possibility is caused by the malicious attempt of some devices; non-technical measures should be taken to solve the problem.

Symptom 2: More than one master existing within a VRRP group

There are also 2 reasons. One is short coexistence of many masters, which is normal and needs no manual intervention. Another is long coexistence of many masters, which may be caused because the original master and other member switches in a VRRP 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.
- 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 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.

Symptom 3: VRRP state of a switch changing repeatedly

Such problems occur when the VRRP group timer interval is too short. They can be solved through prolonging the interval or configuring the preemption delay period.

Table of Contents

1 ARP Configuration	1-1
Introduction to ARP	1-1
ARP Function	1-1
ARP Message Format	1-1
ARP Table	1-3
ARP Process	1-3
Introduction to Gratuitous ARP	1-4
Configuring ARP	1-5
Configuring Gratuitous ARP	1-5
Displaying and Debugging ARP	1-6
ARP Configuration Examples	1-6
2 ARP Attack Defense Configuration	2-1
ARP Attack Defense Configuration	2-1
Introduction to Maximum Number of Dynamic ARP Entries a VLAN Interface Can Learn	2-1
Introduction to ARP Source MAC Address Consistency Check	2-1
Introduction to ARP Attack Detection	2-1
Introduction to ARP Packet Rate Limit	2-3
Introduction to ARP Packet Filtering Based on Gateway's Address	2-3
Configuring ARP Attack Defense	2-4
ARP Attack Defense Configuration Task List	2-4
Configuring the Maximum Number of Dynamic ARP Entries that a VLAN Interface Can Learn	2-5
Configuring ARP Source MAC Address Consistency Check	2-5
ARP Packet Filtering Based on Gateway's Address	2-5
Configuring ARP Attack Detection	2-6
Configuring the ARP Packet Rate Limit Function	2-7
ARP Attack Defense Configuration Example	2-8
ARP Attack Defense Configuration Example I	2-8
ARP Attack Defense Configuration Example II	2-10
ARP Attack Defense Configuration Example III	2-11
ARP Attack Defense Configuration Example IV	2-11
3 Proxy ARP Configuration	3-1
Proxy ARP Overview	3-1
Introduction to Proxy ARP	3-1
Work Mechanism of Common Proxy ARP	3-1
Local Proxy ARP	3-2
Configuring Proxy ARP	3-3
Proxy ARP Configuration Examples	3-3
Common Proxy ARP Configuration Example	3-3
Local Proxy ARP Configuration in Port Isolation Application	3-4
4 Resilient ARP Configuration	4-1
Introduction to Resilient ARP	4-1
Configuring Resilient ARP	4-1

Resilient ARP Configuration Example	4-2
5 MFF Configuration.....	5-1
MFF Overview	5-1
Application Background	5-1
Basic Concepts of MFF	5-2
How MFF Works	5-3
Protocols and Standards	5-4
MFF Configuration	5-4
Enabling MFF	5-4
Specifying the IP Addresses of Servers	5-5
Configuring User Port	5-5
Configuring Network Port	5-6
Displaying MFF Configuration	5-7
MFF Configuration Example	5-7
Troubleshooting MFF Configuration	5-11

1 ARP Configuration

When configuring ARP, go to these sections for information you are interested in:

- [Introduction to ARP](#)
- [Configuring ARP](#)
- [Configuring Gratuitous ARP](#)
- [Displaying and Debugging ARP](#)
- [ARP Configuration Examples](#)



Note

- Support for ARP attack defense is added. For details, refer to [2 ARP Attack Defense Configuration](#).
 - Support for local proxy ARP is added. For details, refer to [3 Proxy ARP Configuration](#).
 - Support for MAC-forced forwarding is added. For details, refer to [5 MFF Configuration](#).
-

Introduction to ARP

ARP Function

Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address.

An IP address is the address of a host at the network layer. To send a network layer packet to a destination host, the device must know the data link layer address (MAC address, for example) of the destination host or the next hop. To this end, the IP address must be resolved into the corresponding data link layer address.



Note

Unless otherwise stated, a data link layer address in this chapter refers to a 48-bit Ethernet MAC address.

ARP Message Format

ARP messages are classified as ARP request messages and ARP reply messages. [Figure 1-1](#) illustrates the format of these two types of ARP messages.

- As for an ARP request, all the fields except the hardware address of the receiver field are set. The hardware address of the receiver is what the sender requests for.

- As for an ARP reply, all the fields are set.

Figure 1-1 ARP message format

Hardware type (16 bits)	
Protocol type (16 bits)	
Length of hardware address	Length of protocol address
Operator (16 bits)	
Hardware address of the sender	
IP address of the sender	
Hardware address of the receiver	
IP address of the receiver	

[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	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 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

Value	Description
3	X.25
4	Proteon ProNET (Token Ring)
5	Chaos
6	IEEE802.X
7	ARC network

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 table, where the latest used IP address-to-MAC address mapping entries are stored. S3600 series Ethernet switches provide the **display arp** command to display the information about ARP mapping entries.

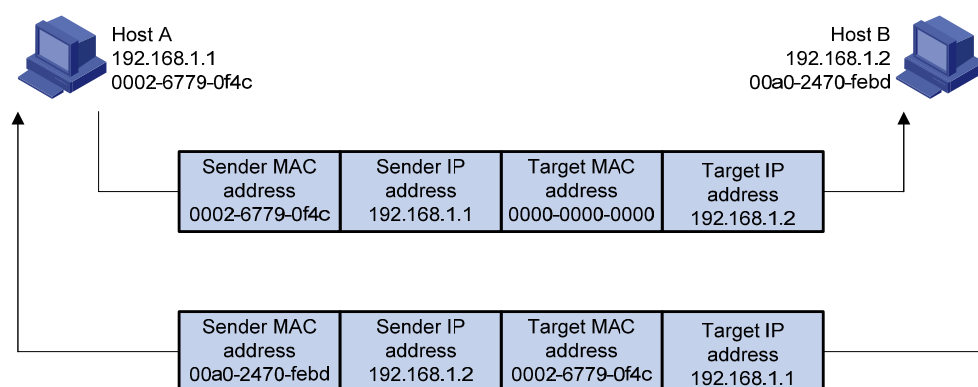
ARP entries in an S3600 series Ethernet switch can either be static entries or dynamic entries, as described in [Table 1-3](#).

Table 1-3 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.

ARP Process

Figure 1-2 ARP process



Suppose that Host A and Host B are on the same subnet and that Host A sends a message to Host B. The resolution process is as follows:

- Host A looks in its ARP mapping table to see whether there is an ARP entry for Host B. If Host A finds it, Host A uses the MAC address in the entry to encapsulate the IP packet into a data link layer frame and sends the frame to Host B.
- If Host A finds no entry for Host B, Host A buffers the packet and broadcasts an ARP request, in which the source IP address and source MAC address are respectively the IP address and MAC

address of Host A and the destination IP address and MAC address are respectively the IP address of Host B and an all-zero MAC address. Because the ARP request is sent in broadcast mode, all hosts on this subnet can receive the request, but only the requested host (namely, Host B) will process the request.

- 4) Host B compares its own IP address with the destination IP address in the ARP request. If they are the same, Host B saves the source IP address and source MAC address into its ARP mapping table, encapsulates its MAC address into an ARP reply, and unicasts the reply to Host A.
- 5) After receiving the ARP reply, Host A adds the MAC address of Host B into its ARP mapping table for subsequent packet forwarding. Meanwhile, Host A encapsulates the IP packet and sends it out.

Usually ARP dynamically implements and automatically seeks mappings from IP addresses to MAC addresses, without manual intervention.

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.

With the gratuitous ARP packet learning function enabled:

A device receiving a gratuitous ARP packet adds the information carried in the packet to its own dynamic ARP table if it finds no corresponding ARP entry for the ARP packet exists in the cache.

Periodical sending of gratuitous ARP packets

In an actual network, when the network load or the CPU occupancy of the receiving host is high, ARP packets may be lost or the host may be unable to timely process the ARP packets received. In such a case, the dynamic ARP entries on the receiving host may age out, and the traffic between the host and the sending device will get interrupted before the host learns the MAC address of the sending device again and installs a corresponding entry in the ARP table.

To address this issue, by default, the S3600 series allow VLAN interfaces to send gratuitous ARP packets periodically. That is, as long as a VLAN interface is in the Up state, it sends gratuitous ARP packets at an interval of 30 seconds so that the receiving host can refresh the MAC address of the switch in the ARP table timely, thereby preventing traffic interruption mentioned above.

Periodical sending of ARP packets in a VRRP backup group

If a VRRP backup group exists on a network, the master switch sends gratuitous ARP packets periodically to hosts on the network, which then update their local ARP tables, ensuring that no device on this network uses the same IP address with the VRRP virtual router.

As you can create mappings between the IP address and MAC address of the VRRP virtual router, there are two cases:

- If the IP address of the virtual router corresponds to a virtual MAC address, the source MAC address in the gratuitous ARP packet will be the virtual MAC address.

- If the IP address of the virtual router corresponds to an actual MAC address, the source MAC address in the gratuitous ARP packet will be the VLAN interface's MAC address of the master switch in the VRRP backup group.



Note

For details about VRRP backup group. Refer to the part discussing VRRP in this manual for details.

Configuring ARP

Follow these steps to configure ARP basic functions:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Add a static ARP entry	arp static <i>ip-address mac-address [vlan-id interface-type interface-number]</i>	Optional By default, the ARP mapping table is empty, and entries are created dynamically by ARP.
Configure the ARP aging timer	arp timer aging <i>aging-time</i>	Optional 20 minutes by default.
Enable the ARP entry checking function (that is, disable the switch from learning ARP entries with multicast MAC addresses)	arp check enable	Optional Enabled by default.



Caution

- Static ARP entries are valid as long as the Ethernet switch operates normally. But some operations, such as removing a VLAN, or removing a port from a VLAN, will make the corresponding ARP entries invalid and therefore removed automatically.
- 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 entries cannot be configured on the ports of an aggregation group.

Configuring Gratuitous ARP

Follow these steps to configure gratuitous ARP:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
Enable the gratuitous ARP packet learning function	gratuitous-arp-learning enable	Optional Enabled by default.
Enable the master switch of a VRRP backup group to send gratuitous ARP packets periodically	arp send-gratuitous enable vrrp	Optional Enabled by default.
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	—
Enable the VLAN interface to send gratuitous ARP packets periodically	gratuitous-arp period-resending enable	Optional Enabled by default.



Note

The sending of gratuitous ARP packets is enabled as long as an S3600 switch operates. No command is needed for enabling this function. That is, the device sends gratuitous ARP packets whenever a VLAN interface is enabled (such as when a link is enabled or an IP address is configured for the VLAN interface) or whenever the IP address of a VLAN interface is changed.

Displaying and Debugging ARP

To do...	Use the command...	Remarks
Display specific ARP mapping table entries	display arp [static dynamic <i>ip-address</i>]	Available in any view
Display the ARP mapping entries related to a specified string in a specified way	display arp [dynamic static] [{ begin include exclude } <i>regular-expression</i>]	
Display the number of the ARP entries of a specified type	display arp count [[dynamic static] [{ begin include exclude } <i>regular-expression</i>] [<i>ip-address</i>]	
Display the statistics about the untrusted ARP packets dropped by the specified port	display arp detection statistics interface <i>interface-type interface-number</i>	
Display the setting of the ARP aging timer	display arp timer aging	
Clear specific ARP entries	reset arp [dynamic static interface <i>interface-type interface-number</i>]	Available in user view

ARP Configuration Examples

Network requirements

- Disable ARP entry check on the switch.

- Disable VLAN-interface 1 of the switch from sending gratuitous ARP packets periodically.
- Set the aging time for dynamic ARP entries to 10 minutes.
- Add a static ARP entry, with the IP address being 192.168.1.1, the MAC address being 000f-e201-0000, and the outbound port being Ethernet 1/0/10 of VLAN 1.

Configuration procedure

```
<Sysname> system-view
[Sysname] undo arp check enable
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] undo gratuitous-arp period-resending enable
[Sysname-Vlan-interface1] quit
[Sysname] arp timer aging 10
[Sysname] arp static 192.168.1.1 000f-e201-0000 1 Ethernet 1/0/10
```

2 ARP Attack Defense Configuration

ARP Attack Defense Configuration

Although ARP is easy to implement, it provides no security mechanism and thus is prone to network attacks. Currently, ARP attacks and viruses are threatening LAN security. The device can provide multiple features to detect and prevent such attacks. This chapter mainly introduces these features.

Introduction to Maximum Number of Dynamic ARP Entries a VLAN Interface Can Learn

To prevent ARP flood attacks, you can limit the number of ARP entries learned by a VLAN interface on S3600 series Ethernet switches (operating as gateways). That is, you can set the maximum number of dynamic ARP entries that a VLAN interface can learn. If the number of ARP entries learned by the VLAN interface exceeds the specified upper limit, the VLAN interface stops learning ARP entries, thus to avoid ARP flood attacks.

Introduction to ARP Source MAC Address Consistency Check

An attacker may use the IP or MAC address of another host as the sender IP or MAC address of ARP packets. These ARP packets can cause other network devices to update the corresponding ARP entries incorrectly, thus interrupting network traffic.

To prevent such attacks, you can configure ARP source MAC address consistency check on S3600 series Ethernet switches (operating as gateways). With this function, the device can verify whether an ARP packet is valid by checking the sender MAC address of the ARP packet against the source MAC address in the Ethernet header.

- If they are consistent, the packet passes the check and the switch learns the ARP entry.
- If they are not consistent, the ARP packet is considered invalid and the corresponding ARP entry is not learned.

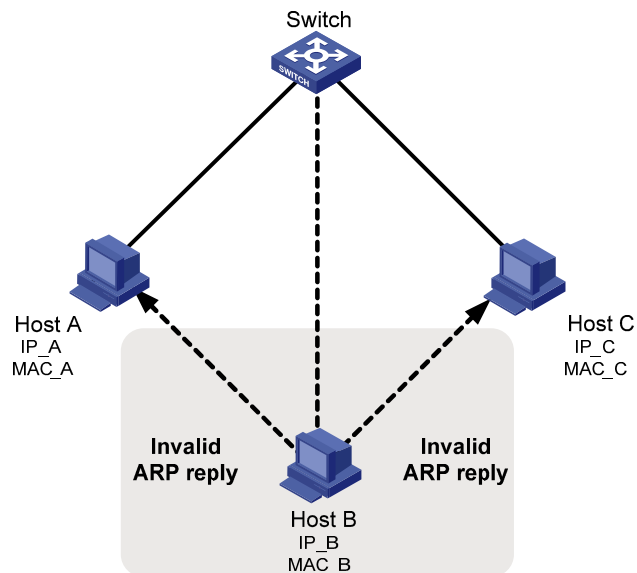
Introduction to ARP Attack Detection

Man-in-the-middle attack

According to the ARP design, after receiving an ARP response, a host adds the IP-to-MAC mapping of the sender into its ARP mapping table even if the MAC address is not the real one. This can reduce the ARP traffic in the network, but it also makes ARP spoofing possible.

In [Figure 2-1](#), Host A communicates with Host C through a switch. To intercept the traffic between Host A and Host C, the hacker (Host B) forwards invalid ARP reply messages to Host A and Host C respectively, causing the two hosts to update the MAC address corresponding to the peer IP address in their ARP tables with the MAC address of Host B. Then, the traffic between Host A and C will pass through Host B which acts like a “man-in-the-middle” that may intercept and modify the communication information. Such an attack is called man-in-the-middle attack.

Figure 2-1 Network diagram for ARP man-in-the-middle attack



ARP attack detection

To guard against the man-in-the-middle attacks launched by hackers or attackers, S3600 series Ethernet switches support the ARP attack detection function.

After you enable ARP attack detection for a VLAN,

- When receiving an ARP request or response packet from an ARP untrusted port, the device delivers the ARP packet to the CPU to check the validity of the packet. If the packet is considered to be valid, it is forwarded; otherwise, it is discarded.
- ARP packets received from a trusted port of the VLAN are forwarded without validity check.

After validity check, users are determined to be valid or invalid on the ports of the VLAN. Validity check can be based on DHCP-snooping entries, IP static binding entries, or IP-to-MAC mappings of authenticated 802.1x users, according to different network environments.

- If all the clients connected to the switch use IP addresses obtained through DHCP, you are recommended to enable DHCP snooping on the switch. The switch then checks validity of packets based on DHCP-snooping entries.
- If the clients connected to the switch use IP addresses configured manually and are few in number, you are recommended to configure IP static binding entries on the switch. The switch then checks validity of packets based on IP static binding entries.
- If a large number of 802.1x clients connected to the switch use IP addresses configured manually, you are recommended to enable ARP attack detection based on authenticated 802.1x clients on the switch. The switch then records mappings between IP addresses (both static and dynamic IP addresses) and MAC addresses of authenticated 802.1x clients and uses the mappings for ARP attack detection together with DHCP-snooping entries and IP static binding entries.



Note

- For details about DHCP Snooping and IP static binding, refer to *DHCP Operation*.
 - For details about 802.1x authentication, refer to *802.1x and System Guard Operation*.
-

ARP restricted forwarding

With the ARP restricted forwarding function enabled, ARP request packets coming from untrusted port are forwarded through trusted ports only; ARP response packets coming from untrusted port are forwarded according to the MAC addresses in the packets, or through trusted ports if the MAC address table contains no such destination MAC addresses.

Introduction to ARP Packet Rate Limit

To prevent the man-in-the-middle attack, a switch enabled with the ARP attack detection function delivers ARP packets to the CPU to check the validity of the packets. However, this causes a new problem: If an attacker sends a large number of ARP packets to a port of a switch, the CPU will get overloaded, causing other functions to fail, and even the whole device to break down. To guard against such attacks, S3600 series Ethernet switches support the ARP packets rate limit function, which will shut down the attacked port, thus preventing serious impact on the CPU.

With this function enabled on a port, the switch will count the ARP packets received on the port within each second. If the number of ARP packets received on the port per second exceeds the preconfigured value, the switch considers that the port is attacked by ARP packets. In this case, the switch will shut down the port. As the port does not receive any packet, the switch is protected from the ARP packet attack.

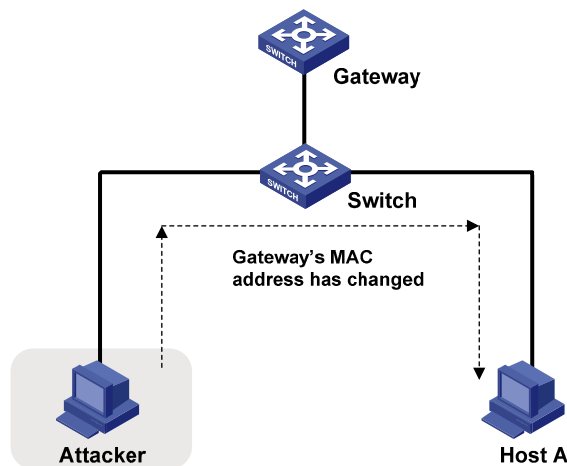
At the same time, the switch supports automatic recovery of port state. If a port is shut down by the switch due to high packet rate, the port will revert to the Up state after a configured period of time.

Introduction to ARP Packet Filtering Based on Gateway's Address

According to the ARP design, after receiving an ARP packet with the target IP address being that of the receiving interface, a device adds the IP-to-MAC mapping of the sender into its ARP mapping table even if the MAC address is not requested by itself. This can reduce the ARP traffic in the network, but it also makes ARP spoofing possible.

The most common ARP attack on campus networks is the gateway spoofing attack. An attacker sends an ARP packet with the gateway's IP address and a fake MAC address, and then a receiving host updates the IP-to-MAC binding of the gateway. As a result, the traffic sent from the host to the gateway will be redirected to the fake MAC address, and the client will be unable to access the external network.

Figure 2-2 Gateway spoofing attack



To prevent gateway spoofing attacks, an S3600 series Ethernet switch can work as an access device (usually with the upstream port connected to the gateway and the downstream ports connected to hosts) and filter ARP packets based on the gateway's address.

- To filter ARP attack packets arriving on a downstream port, you can bind the gateway's IP address to the downstream port (directly connected to hosts) of the switch. After that, the port will discard ARP packets with the gateway's IP address as the sender IP address, and permit other ARP packets to pass.
- To filter ARP attack packets arriving on the upstream port, you can bind the IP and MAC addresses of the gateway to the cascaded port or upstream port of the access switch. After that, the port will discard ARP packets with the sender IP address as the gateway's IP address but with the sender MAC address different from the gateway's MAC address, and permit other ARP packets to pass.

 Note

An ARP trusted port has higher priority comparing with support for ARP packet filtering based on gateway's address. That is, if you configure a cascaded port or an upstream port as an ARP trusted port, the gateway's IP and MAC addresses configured on the port are ineffective.

Configuring ARP Attack Defense

ARP Attack Defense Configuration Task List

Complete the following tasks to configure ARP attack defense:

Task	Remarks
Configuring the Maximum Number of Dynamic ARP Entries that a VLAN Interface Can Learn	Optional The switch serves as a gateway.
Configuring ARP Source MAC Address Consistency Check	Optional The switch serves as a gateway or an access device.

Task	Remarks
ARP Packet Filtering Based on Gateway's Address	Optional The switch serves as an access device.
Configuring ARP Attack Detection	Optional The switch serves as a gateway or an access device.
Configuring the ARP Packet Rate Limit Function	Optional The switch serves as a gateway or an access device.

Configuring the Maximum Number of Dynamic ARP Entries that a VLAN Interface Can Learn

Follow these steps to configure the maximum number of dynamic ARP entries that a VLAN interface can learn:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface vlan-interface <i>vlan-id</i>	—
Configure the maximum number of dynamic ARP entries that the VLAN interface can learn	arp max-learning-num <i>number</i>	Optional For an S3600-EI switch the value is 4031, and for an S3600-SI switch the value is 2048 by default.

Configuring ARP Source MAC Address Consistency Check

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable ARP source MAC address consistency check	arp anti-attack valid-check enable	Required Disabled by default.

ARP Packet Filtering Based on Gateway's Address

Follow these steps to configure ARP packet filtering based on gateway's IP address:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure ARP packet filtering based on the gateway's IP address	arp filter source <i>ip-address</i>	Required Not configured by default.

Follow these steps to configure ARP packet filtering based on gateway's IP and MAC address:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure ARP packet filtering based on the gateway's IP and MAC addresses	arp filter binding <i>ip-address</i> <i>mac-address</i>	Required Not configured by default.



Note

The **arp filter source** and **arp filter binding** commands are mutually exclusive on an Ethernet port. That is, you can only configure ARP packet filtering based on gateway's IP address, or based on gateway's IP and MAC addresses on an Ethernet port. Generally, ARP packet filtering based on gateway's IP address is configured on the switch's port directly connected to a host, and ARP packet filtering based on gateway's IP and MAC addresses is configured on the cascaded port or upstream port.

Configuring ARP Attack Detection

Follow these steps to configure the ARP attack detection function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a static binding	interface <i>interface-type</i> <i>interface-number</i>	Required Use at least one of the commands. By default, no IP static binding is created, and the DHCP snooping function and ARP attack detection based on authenticated 802.1x clients are disabled.
	ip source static binding <i>ip-address ip-address</i> [<i>mac-address mac-address</i>]	
Enable DHCP snooping	dhcp-snooping	
Enable ARP attack detection based on IP-to-MAC bindings of authenticated 802.1x clients	ip source static import dot1x	
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Specify the current port as a trusted port	dhcp-snooping trust	Optional After DHCP snooping is enabled, you need to configure the upstream port connected to the DHCP server as a trusted port.

To do...	Use the command...	Remarks
Configure the port as an ARP trusted port	arp detection trust	Optional By default, a port is an ARP untrusted port. Generally, the upstream port of a switch is configured as a trusted port.
Quit to system view	quit	—
Enter VLAN view	vlan <i>vlan-id</i>	—
Enable the ARP attack detection function	arp detection enable	Required By default, ARP attack detection is disabled on all ports.
Enable ARP restricted forwarding	arp restricted-forwarding enable	Optional Disabled by default.



Note

- When most clients acquire IP addresses through DHCP and some clients use static IP addresses, you need to enable DHCP snooping and configure static IP binding entries on the switch. These functions can cooperate with ARP attack detection to check the validity of packets.
- You need to use ARP attack detection based on authenticated 802.1x clients together with functions of both MAC-based 802.1x authentication and ARP attack detection.
- Currently, the VLAN ID of an IP-to-MAC binding configured on a port of an S3600 series Ethernet switch is the same as the default VLAN ID of the port. If the VLAN tag of an ARP packet is different from the default VLAN ID of the receiving port, the ARP packet cannot pass the ARP attack detection based on the IP-to-MAC bindings.
- Before enabling ARP restricted forwarding, make sure you have enabled ARP attack detection and configured ARP trusted ports.
- You are not recommended to configure ARP attack detection on the ports of a fabric or an aggregation group.

Configuring the ARP Packet Rate Limit Function

Follow these steps to configure the ARP packet rate limit function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the ARP packet rate limit function	arp rate-limit enable	Required By default, the ARP packet rate limit function is disabled on a port.

To do...	Use the command...	Remarks
Configure the maximum ARP packet rate allowed on the port	arp rate-limit <i>rate</i>	Optional By default, the maximum ARP packet rate allowed on a port is 15 pps.
Quit to system view	quit	—
Enable the port state auto-recovery function	arp protective-down recover enable	Optional Disabled by default.
Configure the port state auto-recovery interval	arp protective-down recover interval <i>interval</i>	Optional By default, when the port state auto-recovery function is enabled, the port state auto-recovery interval is 300 seconds.



Note

- You need to enable the port state auto-recovery feature before you can configure the port state auto-recovery interval.
- You are not recommended to configure the ARP packet rate limit function on the ports of a fabric or an aggregation group.

ARP Attack Defense Configuration Example

ARP Attack Defense Configuration Example I

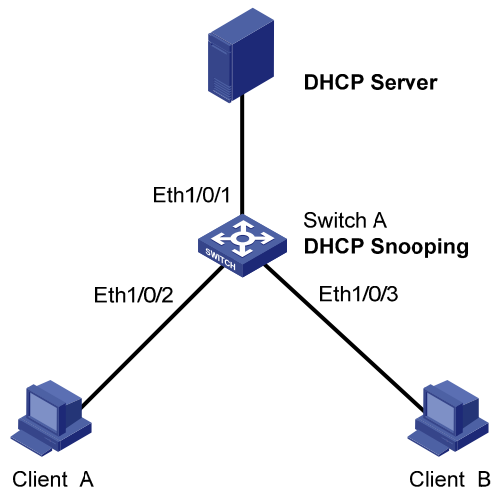
Network requirements

As shown in [Figure 2-3](#), Ethernet 1/0/1 of Switch A connects to DHCP Server; Ethernet 1/0/2 connects to Client A, Ethernet 1/0/3 connects to Client B. Ethernet 1/0/1, Ethernet 1/0/2 and Ethernet 1/0/3 belong to VLAN 1.

- Enable DHCP snooping on Switch A and specify Ethernet 1/0/1 as the DHCP snooping trusted port.
- Enable ARP attack detection in VLAN 1 to prevent ARP man-in-the-middle attacks, and specify Ethernet 1/0/1 as the ARP trusted port.
- Enable the ARP packet rate limit function on Ethernet 1/0/2 and Ethernet 1/0/3 of Switch A, so as to prevent Client A and Client B from attacking Switch A through ARP traffic.
- Enable the port state auto recovery function on the ports of Switch A, and set the recovery interval to 200 seconds.

Network diagram

Figure 2-3 ARP attack detection and packet rate limit configuration



Configuration procedure

Enable DHCP snooping on Switch A.

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

Specify Ethernet 1/0/1 as the DHCP snooping trusted port and the ARP trusted port.

```
[SwitchA] interface Ethernet 1/0/1
[SwitchA-Ethernet1/0/1] dhcp-snooping trust
[SwitchA-Ethernet1/0/1] arp detection trust
[SwitchA-Ethernet1/0/1] quit
```

Enable ARP attack detection on all ports in VLAN 1.

```
[SwitchA] vlan 1
[SwitchA-vlan1] arp detection enable
```

Enable the ARP packet rate limit function on Ethernet 1/0/2, and set the maximum ARP packet rate allowed on the port to 20 pps.

```
[SwitchA] interface Ethernet 1/0/2
[SwitchA-Ethernet1/0/2] arp rate-limit enable
[SwitchA-Ethernet1/0/2] arp rate-limit 20
[SwitchA-Ethernet1/0/2] quit
```

Enable the ARP packet rate limit function on Ethernet 1/0/3, and set the maximum ARP packet rate allowed on the port to 50 pps.

```
[SwitchA] interface Ethernet 1/0/3
[SwitchA-Ethernet1/0/3] arp rate-limit enable
[SwitchA-Ethernet1/0/3] arp rate-limit 50
[SwitchA-Ethernet1/0/3] quit
```

Configure the port state auto recovery function, and set the recovery interval to 200 seconds.

```
[SwitchA] arp protective-down recover enable
[SwitchA] arp protective-down recover interval 200
```

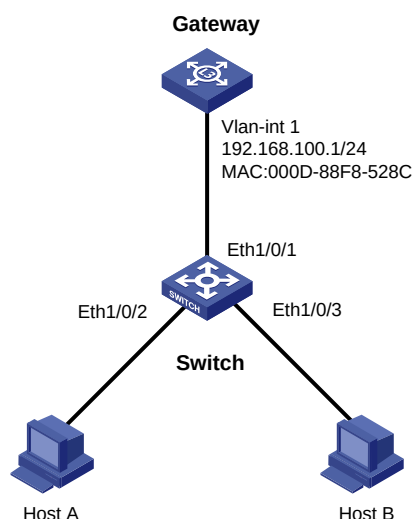
ARP Attack Defense Configuration Example II

Network Requirements

As shown in [Figure 2-4](#), Host A and Host B are connected to Gateway through an access switch (Switch). The IP and MAC addresses of Gateway are 192.168.100.1/24 and 000D-88F8-528C. To prevent gateway spoofing attacks from Host A and Host B, configure ARP packet filtering based on the gateway's IP and MAC addresses on Switch.

Network Diagram

Figure 2-4 Network diagram for defense against gateway spoofing



Configuration Procedures

Enter system view.

```
<Switch> system-view
```

Configure ARP packet filtering based on the gateway's IP and MAC addresses on Ethernet 1/0/1.

```
[Switch] interface Ethernet 1/0/1
```

```
[Switch-Ethernet1/0/1] arp filter binding 192.168.100.1 000d-88f8-528c
```

```
[Switch-Ethernet1/0/1] quit
```

Configure ARP packet filtering based on the gateway's IP address on Ethernet 1/0/2.

```
[Switch] interface Ethernet 1/0/2
```

```
[Switch-Ethernet1/0/2] arp filter source 192.168.100.1
```

```
[Switch-Ethernet1/0/2] quit
```

Configure ARP packet filtering based on the gateway's IP address on Ethernet 1/0/3.

```
[Switch] interface Ethernet 1/0/3
```

```
[Switch-Ethernet1/0/3] arp filter source 192.168.100.1
```

```
[Switch-Ethernet1/0/3] quit
```

ARP Attack Defense Configuration Example III

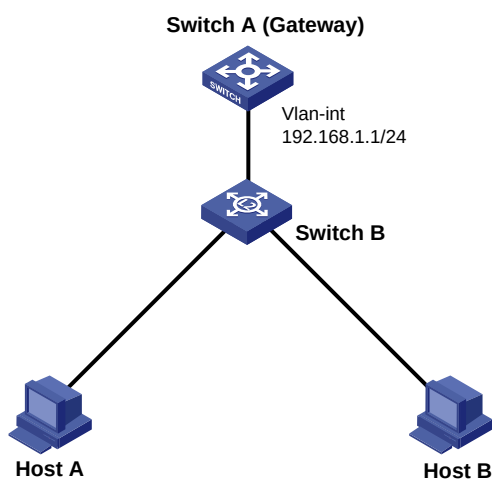
Network Requirements

As shown in [Figure 2-5](#), Host A and Host B are connected to Gateway (Switch A) through a Layer 2 switch (Switch B). To prevent ARP attacks such as ARP flooding:

- Enable ARP packet source MAC address consistency check on Switch A to block ARP packets with the sender MAC address different from the source MAC address in the Ethernet header.
- Limit the number of dynamic ARP entries learned on VLAN-interface 1.

Network Diagram

Figure 2-5 Network diagram for ARP attack defense



Configuration Procedures

Enter system view.

```
<SwitchA> system-view
```

Enable ARP source MAC address consistency check.

```
[SwitchA] arp anti-attack valid-check enable
```

Enter VLAN-interface 1 view.

```
[SwitchA] interface vlan-interface 1
```

Configure an IP address for VLAN-interface 1.

```
[SwitchA-Vlan-interface1] ip address 192.168.1.1 24
```

Configure the maximum number of ARP entries that can be learned by VLAN-interface 1 as 500.

```
[SwitchA-Vlan-interface1] arp max-learning-num 500
```

```
[SwitchA-Vlan-interface1] quit
```

ARP Attack Defense Configuration Example IV

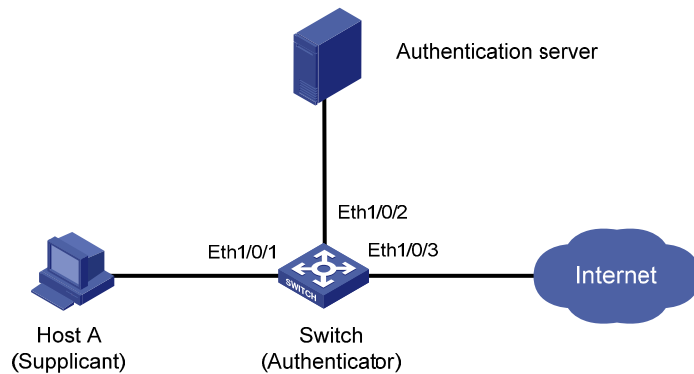
Network Requirements

- Host A is assigned with an IP address statically and installed with an 802.1x client.
- A CAMS authentication, authorization and accounting server serves as the authentication server.

- Enable ARP attack detection based on bindings of authenticated 802.1x clients on the switch to prevent ARP attacks.

Network Diagram

Figure 2-6 Network diagram for 802.1x based ARP attack defense



Configuration Procedures

Enter system view.

```
<Switch> system-view
```

Enable 802.1x authentication globally.

```
[Switch] dot1x
```

Enable ARP attack detection for VLAN 1.

```
[Switch] vlan 1
```

```
[Switch-vlan1] arp detection enable
```

```
[Switch-vlan1] quit
```

Configure Ethernet 1/0/2 and Ethernet 1/0/3 as ARP trusted ports.

```
[Switch] interface Ethernet 1/0/2
```

```
[Switch-Ethernet1/0/2] arp detection trust
```

```
[Switch-Ethernet1/0/2] quit
```

```
[Switch] interface Ethernet 1/0/3
```

```
[Switch-Ethernet1/0/3] arp detection trust
```

```
[Switch-Ethernet1/0/3] quit
```

Enable ARP attack detection based on IP-to-MAC mappings of authenticated 802.1x clients.

```
[Switch] ip source static import dot1x
```

Enable 802.1x on Ethernet 1/0/1.

```
[Switch] interface ethernet 1/0/1
```

```
[Switch-Ethernet1/0/1] dot1x
```

3 Proxy ARP Configuration

When configuring proxy ARP, go to these sections for information you are interested in:

- [Proxy ARP Overview](#)
- [Configuring Proxy ARP](#)
- [Proxy ARP Configuration Examples](#)

Proxy ARP Overview

Introduction to Proxy ARP

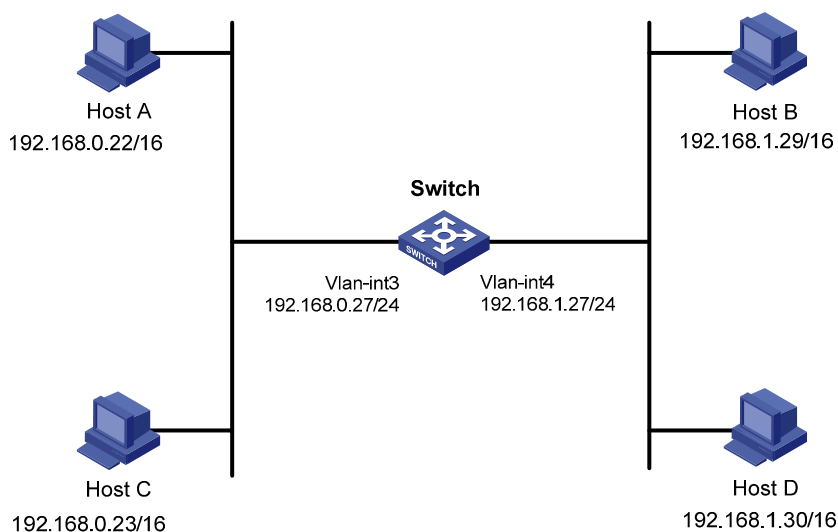
If a host sends an ARP request for the MAC address of another host that actually resides on another network (but the sending host considers the requested host is on the same network according to the destination IP address and mask), the device in between must be able to respond to the request with the MAC address of the receiving interface to allow Layer 3 communication between the two hosts. This is achieved by proxy ARP. Proxy ARP hides the physical details of the network.

If the target IP address in an incoming ARP request and the receiving interface of the proxy ARP enabled device reside on the same network, proxy ARP is called local proxy ARP. If not, it is called common proxy ARP.

- Common proxy ARP applies where the two communication parties connect to different Layer 3 interfaces of a device, and they are not on the same broadcast domain.
- Local proxy ARP applies where the two communication parties connect to the same Layer 3 interface of a device, and they are not on the same broadcast domain.

Work Mechanism of Common Proxy ARP

Figure 3-1 Work mechanism of common proxy ARP



As shown in [Figure 3-1](#):

Host A and Host D are on different sub networks. When Host A (192.168.0.22/16) needs to send packets to Host D (192.168.1.30/16), because the mask of the two hosts are both 16 bits, Host A regards Host D to be on its directly connected sub network, and thus Host A will broadcast an ARP request to request the MAC address of Host D.

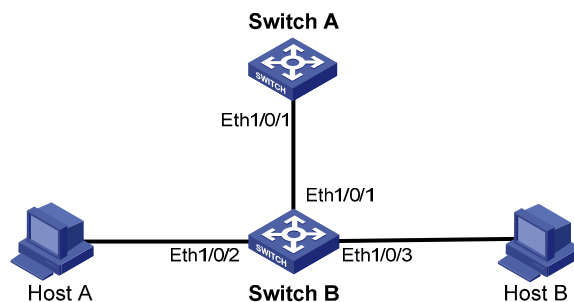
- When the common proxy ARP feature is not enabled on the switch, because Host A and Host D are in different VLANs, the ARP request sent by Host A cannot reach Host D, and the two hosts cannot communicate.
- With common proxy ARP enabled on the switch, when VLAN-interface 3 receives the ARP request, if the switch finds a route to the destination IP address (encapsulated in the ARP request) in the routing table, the switch sends host A the MAC address of VLAN-interface 3 in an ARP response (with the source IP address being the destination IP address of the ARP request). After receiving the ARP response, Host A creates an ARP entry, in which the destination IP address is the IP address of Host D (192.168.1.30/16), and the MAC address is that of VLAN-interface 3. The following packets sent from Host A to Host D will all be sent to VLAN-interface 3 of the switch, and then the switch forwards the packets in Layer 3 to Host D, so as to realize the Layer 3 connectivity between Host A and Host D.

If IP hosts on a network have no default gateway configured or have no routing capability, you can use common proxy ARP to address this issue.

Local Proxy ARP

The following gives a local proxy ARP application scenario. Host A and Host B belong to the same VLAN, and they respectively connect to Switch B' Layer 2 ports Ethernet 1/0/2 and Ethernet 1/0/3, which are isolated at Layer 2. To allow the two hosts to communicate at Layer 3, you can enable local proxy ARP on Switch A.

Figure 3-2 Local proxy ARP application



In one of the following cases, you need to enable local proxy ARP:

- Hosts connecting to different isolated Layer 2 ports in the same VLAN need to communicate at Layer 3.
- After Isolate-user-VLAN function is configured on a device attached to a S3600 series Ethernet switch, hosts belonging to different secondary VLANs need to communicate at Layer 3.

Configuring Proxy ARP

Follow these steps to configure proxy ARP:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface vlan-interface <i>vlan-id</i>	—
Enable common proxy ARP	arp proxy enable	Required Disabled by default.
Enable local proxy ARP	local-proxy-arp enable [ip-range startIP to endIP]	Required Disabled by default.
Display common and local proxy ARP configuration	display arp proxy [interface vlan-interface <i>vlan-id</i>]	Available in any view

Proxy ARP Configuration Examples

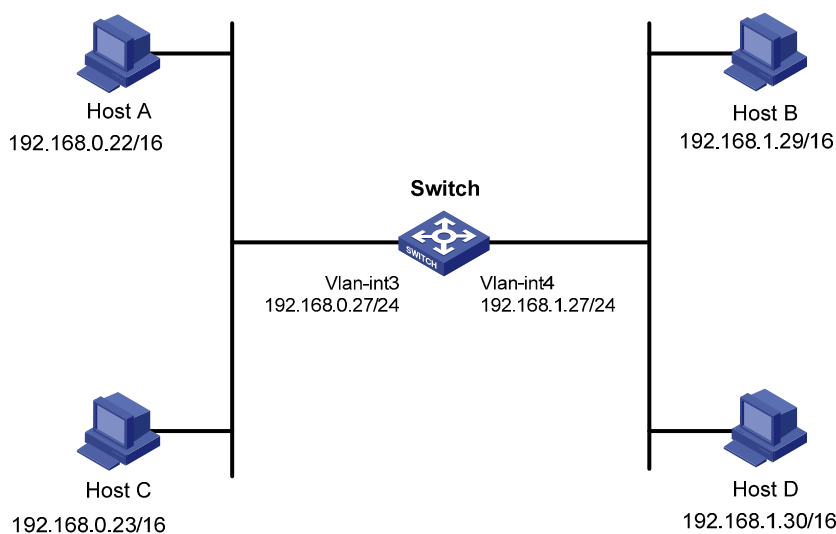
Common Proxy ARP Configuration Example

Network requirements

- The IP address of Host A is 192.168.0.22/16, and that of Host D is 192.168.1.30/16.
- Create VLAN 3 and VLAN 4 on the switch.
- The IP address of VLAN-interface 3 is 192.168.0.27/24, and that of VLAN-interface 4 is 192.168.1.27/24.
- Enable common proxy ARP on VLAN-interface 3 and VLAN-interface 4 to realize the communication between Host A and Host D.

Network diagram

Figure 3-3 Network diagram for common proxy ARP



Configuration procedure

Configure the IP address of VLAN-interface 3 to be 192.168.0.27/24.

```

<Switch> system-view
[Switch] interface Vlan-interface 3
[Switch-Vlan-interface3] ip address 192.168.0.27 24
[Switch-Vlan-interface3] quit

# Configure the IP address of VLAN-interface 4 to be 192.168.1.27/24.
[Switch] interface Vlan-interface 4
[Switch-Vlan-interface4] ip address 192.168.1.27 24
[Switch-Vlan-interface4] quit

# Enter VLAN-interface 3 view, and enable common proxy ARP on it.
[Switch] interface Vlan-interface 3
[Switch-Vlan-interface3] arp proxy enable
[Switch-Vlan-interface3] quit

# Enter VLAN-interface 4 view, and enable common proxy ARP on it.
[Switch] interface Vlan-interface 4
[Switch-Vlan-interface4] arp proxy enable
[Switch-Vlan-interface4] quit

```

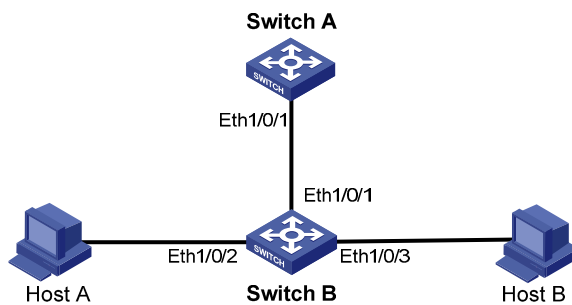
Local Proxy ARP Configuration in Port Isolation Application

Network requirements

- Switch A (a S3600 series Ethernet switch) is connected to Switch B through Ethernet 1/0/1.
- Ethernet 1/0/2 and Ethernet 1/0/3 on Switch B belong to VLAN 1, and are connected to Host A and Host B respectively.
- Host A and Host B isolated at Layer 2 can communicate at Layer 3 through Switch A.

Network diagram

Figure 3-4 Network diagram for local proxy ARP configuration in port isolation application



Configuration procedure

1) Configure Switch B

Add Ethernet 1/0/2 and Ethernet 1/0/3 into an isolation group, disabling Host A and Host B from communicating with each other at Layer 2.

For details about port isolation, refer to the part discussing port isolation.

```

<SwitchB> system-view
[SwitchB] interface Ethernet 1/0/2
[SwitchB-Ethernet1/0/2] port isolate

```

```
[SwitchB-Ethernet1/0/2] quit
[SwitchB] interface Ethernet 1/0/3
[SwitchB-Ethernet1/0/3] port isolate
[SwitchB-Ethernet1/0/3] quit
```

2) Configure Switch A

Configure local proxy ARP on VLAN-interface 1, enabling Host A and Host B to communicate at Layer 3.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] local-proxy-arp enable
[SwitchA-Vlan-interface1] quit
```

4 Resilient ARP Configuration

When configuring resilient ARP, go to these sections for information you are interested in:

- [Introduction to Resilient ARP](#)
- [Configuring Resilient ARP](#)
- [Resilient ARP Configuration Example](#)



Note

The features in this chapter apply to S3600-EI series switches only.

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.

Configuring Resilient ARP

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.

Follow these steps to configure the Resilient ARP function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the Resilient ARP function	resilient-arp enable	Required Enabled by default.
Configure the VLAN interface through which Resilient packets are sent	resilient-arp interface vlan-interface <i>vlan-id</i>	Optional By default, Resilient ARP packets are sent through the interface of VLAN 1 (VLAN-interface 1).
Display information about the Resilient ARP state	display resilient-arp [unit <i>unit-id</i>]	Available in any view

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.

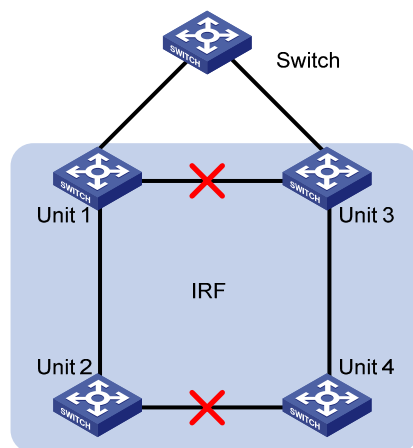
Resilient ARP Configuration Example

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.

Network diagram

Figure 4-1 Network diagram for Resilient ARP



Configuration procedure

Enable the Resilient ARP function.

```
<Sysname> system-view
```

```
[Sysname] resilient-arp enable
```

Configure the Resilient ARP packets to be sent through the VLAN-interface 2.

[Sysname] resilient-arp interface Vlan-interface 2

5 MFF Configuration

MFF Overview

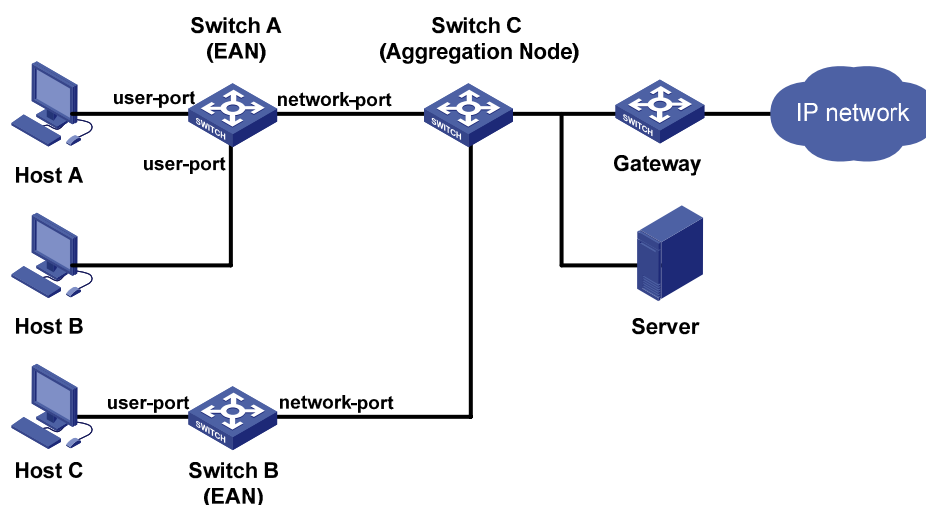
Application Background

In traditional Ethernet networking, typically VLANs are created on a switch to implement Layer 2 isolation and provide Layer 3 interoperability among clients. If a large number of users are to be isolated at Layer 2, however, this type of networking consumes many VLAN resources. Moreover, to provide Layer 3 interoperability among clients, you need to plan a different IP network segment for each VLAN and configure an IP address for each VLAN interface. Therefore, an excessive number of VLANs will make IP address allocation less efficient.

Access-layer switches support MAC-forced forwarding (MFF), which provides a solution for Layer 2 isolation and Layer 3 interoperability among clients within the same broadcast domain.

An MFF enabled device intercepts an ARP request and then returns the MAC address of a gateway to the sender. In this way, the sender is forced to send all packets to the gateway for traffic monitoring and attack prevention.

Figure 5-1 Ethernet-based access network



As shown in [Figure 5-1](#), Switch A and Switch B, serving as Ethernet access nodes (EANs), interconnect the hosts and the aggregation node Switch C. After port isolation and MFF are enabled on the EANs, all the data packets exchanged among the hosts will be forwarded through the gateway, thus providing Layer 3 interoperability among the hosts while ensuring Layer 2 isolation of data. That is, the client hosts will have no knowledge of one another's MAC addresses.

The MFF feature is typically used in combination with port isolation, IP filtering, and ARP intrusion detection. It is used on access-layer switches to implement traffic filtering, Layer 2 isolation, and Layer 3 interoperability among the hosts, thereby enhancing access-layer network security. For details about port isolation, IP filtering, and ARP intrusion detection, refer to the sections covering port isolation, DHCP, and ARP in this manual.

Basic Concepts of MFF

User port

An MFF user port is directly connected to a host; it processes packets as follows:

- Allows DHCP packets and multicast packets to pass.
- Delivers ARP packets to the CPU.
- After learning gateways' MAC addresses, a user port allows only the unicast packets with the gateways' MAC addresses as the destination MAC addresses to pass. If no gateways' MAC addresses are learned, a user port discards all received unicast packets.



Note

- IP filtering must be enabled on a port before the port can be configured as a user port. IP filtering cannot be disabled on an as-configured user port.
 - To ensure Layer 2 isolation among clients connected to the same switch, the corresponding user ports must be added to a port isolation group.
-

Network port

An MFF network port is connected to a networking device, such as an access switch, a distribution switch or a gateway. A network port processes packets as follows:

- Allows multicast packets and DHCP packets to pass.
- Delivers ARP packets to the CPU.
- Denies broadcast packets.



Note

- You need to configure the following ports as network ports: upstream ports connected to a gateway, ports connected to the downstream MFF devices, and ports between devices in a ring network.
 - A network port is not always an upstream port.
 - To ensure the correct implementation of MFF, the network port is typically configured as a DHCP snooping trusted port and an ARP intrusion detection trusted port.
-

Gateway

For an access layer switch enabled with MFF, each VLAN corresponds to an MFF gateway. All the traffic from the clients of a VLAN will be forwarded by the corresponding gateway, to implement Layer 2 isolation and traffic monitoring.

The IP address of an MFF gateway can be configured manually or obtained automatically. For details, refer to [How MFF Works](#).



Note

If a VLAN interface and its IP address are configured incorrectly, or the IP address of the gateway is not on the same network segment as that of the VLAN interface, the gateway's MAC address may not be learned correctly.

How MFF Works

Manual mode

If a host's IP address is manually assigned, you can enable the MFF manual mode on the access layer switch connected to it.

If the MFF manual mode is enabled, you need to specify gateways. Upon receiving an ARP request for a host's MAC address from a specified gateway, the switch directly sends the host's MAC address to the gateway based on the static binding entry or the DHCP snooping entry.

Automatic mode

If all the hosts connected to an access layer switch obtain IP addresses through DHCP, you can enable MFF automatic mode on the switch, provided that DHCP snooping has been enabled.

With MFF automatic mode enabled, a DHCP snooping device, upon receiving a DHCP-ACK message, resolves Option 3 in the message (Router IP option) to obtain a gateway for the client's IP-MAC snooping entry. If the DHCP-ACK message contains multiple gateway addresses, only the first one is recorded for the entry. If the message contains no gateway IP address, the first gateway recorded by the current VLAN is used.

To get a gateway's MAC address, MFF uses the IP and MAC addresses in the first client snooping entry corresponding to the gateway to forge an ARP request, and sends the ARP request to the gateway.



Note

- In MFF automatic mode, a VLAN can learn and maintain up to 20 gateways. The gateway IP addresses will not be updated, that is, the gateway information does not age unless MFF is disabled.
 - If the source MAC address of an incoming ARP packet from a gateway is different from the one recorded, the MFF device will use the new MAC to replace the old MAC for the gateway.
 - After you enable MFF manual mode, the hosts that obtain IP address dynamically can get the gateway's IP address based on DHCP snooping entries.
-

ARP reply mechanism

Like proxy ARP, the ARP reply mechanism is used for Layer 3 communication between hosts, which helps reduce the number of broadcast messages.

An MFF device processes ARP packets as follows:

- After receiving an ARP request from a host, the MFF device sends the MAC address of the corresponding gateway to the host. In this way, hosts in the network have to communicate at Layer 3 through a gateway.
- After receiving an ARP request from a gateway, the MFF device sends the requested host's MAC address to the gateway if the corresponding entry is available; if the entry is not available, the MFF device will forward the ARP request.
- The MFF device forwards ARP replies between hosts and gateways.
- If the source MAC addresses of ARP requests from gateways are different from those recorded, the MFF device updates and broadcasts the IP and MAC addresses of the gateways.

Protocols and Standards

RFC4562: MAC-Forced Forwarding

MFF Configuration

Table 5-1 Configure MFF

Operation	Remarks
Enabling MFF	Required
Specifying the IP Addresses of Servers	Optional
Configuring User Port	Required
Configuring Network Port Configuring Network Port	Required



Note

If VLAN mapping is enabled on an MFF-capable access-layer switch, to ensure that the MFF gateway and the access-layer switch operate normally, you need to configure the MFF gateway and the VLAN interfaces of the access-layer switch to belong to a network-side VLAN and manually configure the VLAN interface IP addresses to be on the same network segment as the MFF gateway IP address.

Enabling MFF

Follow these steps to enable MFF:

Operation	Command	Remarks
Enter system view	system-view	—
Enter VLAN view	vlan <i>vlan-id</i>	—
Enable MFF and specify an MFF operating mode	arp mac-forced-forwarding { auto default-gateway gateway-ip }	Required Disabled by default.

Specifying the IP Addresses of Servers

For communication between hosts connected to an MFF enabled switch and a server, you need to specify the server's IP address in either manual or automatic MFF mode. The server can be a DHCP server or a server providing some other service. After you specify a server's IP address and then an ARP request from the server is received, the MFF device will reply with the corresponding MAC address to the server. In this way, packets from a host to a server are forwarded by the gateway, while packets from a server to a host are not forwarded by the gateway.

Follow these steps to specify the IP addresses of servers:

Operation	Command	Remarks
Enter system view	system-view	—
Enter VLAN view	vlan <i>vlan-id</i>	—
Specify the IP addresses of servers	arp mac-forced-forwarding server <i>server-ip</i> &<1-10>	Required Not specified by default



Note

- If MFF automatic mode is enabled, and the gateway and DHCP server do not run on the same device, you need to use this command to specify the IP address of the DHCP server.
- If a VRRP group serves as an MFF gateway, you need to use this command to specify all the IP addresses of the switches in the VRRP group.

Configuring User Port

Configuration prerequisites

Before configuring a port as an MFF user port, enable DHCP snooping on the access-layer switch and verify the following:

- ARP intrusion detection is enabled in the VLAN to which the port belongs.
- IP filtering is enabled on the port.
- The port is a member of a port isolation group.

Configuration procedure

Follow these steps to configure an MFF user port:

Operation	Command	Remarks
Enter system view	system-view	—
Enable DHCP snooping	dhcp-snooping	Required Disabled by default
Enter VLAN view	vlan <i>vlan-id</i>	—
Enable ARP intrusion detection	arp detection enable	Required Disabled by default
Return to system view	quit	—

Operation	Command	Remarks
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable IP filtering on the port	ip check source ip-address [mac-address]	Required Disabled by default
Add the port to the isolation group	port isolate	Required By default, an Ethernet port is not added to any isolation group.
Configure the port as an MFF user port	arp mac-forced-forwarding user-port	Required No user port configured by default



Note

- On a port configured as an MFF user port or MFF network port, aggregation synchronization will not occur. To ensure proper MFF implementation, you need to perform manual configurations to ensure that all the ports in an aggregation group are MFF user ports or MFF network ports.
- If several access-layer switches are connected in series in the network and multiple VLANs are created on the downstream switches, to ensure proper MFF operation, the downstream user port on the upstream switch must be configured as an ARP trusted port.

Configuring Network Port

Configuration prerequisites

Before configuring a port as the MFF network port on an access-layer switch, enable DHCP snooping on the switch and verify the following:

- ARP intrusion detection is enabled in the VLAN to which the port belongs.
- The port is configured as an ARP intrusion detection trusted port and a DHCP snooping trusted port.



Note

In case multiple access-layer switches are connected in series in the actual networking environment, if a downstream port of the upstream access-layer switch is an MFF network port, the port cannot be configured as a DHCP snooping trusted port.

Configuration procedure

Follow these steps to configure an MFF network port:

Operation	Command	Remarks
Enter system view	system-view	—
Enable DHCP snooping	dhcp-snooping	Required Disabled by default
Enter VLAN view	vlan <i>vlan-id</i>	—
Enable ARP intrusion detection	arp detection enable	Required Disabled by default
Return to system view	quit	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the port as a DHCP snooping trusted port	dhcp-snooping trust	Optional By default, after DHCP snooping is enabled, all the ports of the device are untrusted ports.
Configure the port as an ARP intrusion detection trusted port	arp detection trust	Required By default, a port is not an ARP intrusion detection trusted port.
Configure the port as an MFF network port	arp mac-forced-forwarding network-port	Required No MFF network port configured by default

Displaying MFF Configuration

After the above-mentioned configuration, you can use the following **display** commands in any view to display the MFF operating status, so as to verify configuration result.

Follow these steps to display MFF configuration:

Operation	Command	Remarks
Display the MFF user port and MFF network port configuration information	display arp mac-forced-forwarding interface	Available in any view
Display MFF gateway configuration information	display arp mac-forced-forwarding vlan	

MFF Configuration Example

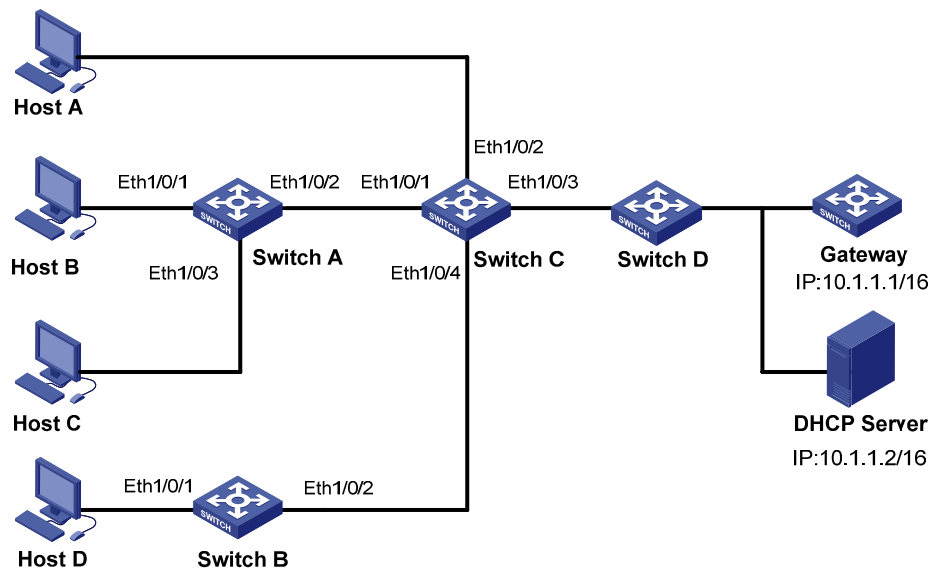
Network requirements

All the hosts are in VLAN 1. Assign a static IP address to Host A, and configure Host B, Host C, and Host D to obtain IP addresses dynamically through DHCP.

Enable MFF on Switch A, Switch B and Switch C respectively, implementing Layer 2 isolation and Layer 3 communication among the hosts through Gateway.

Network diagram

Figure 5-2 MFF network diagram



Configuration procedure

1) Configure Gateway.

Configure the VLAN interface IP address of the gateway.

```
<Gateway> system-view
[Gateway] interface Vlan-interface 1
[Gateway-Vlan-interface1] ip address 10.1.1.1 16
```

2) Configure the DHCP server

```
<DHCPServer> system-view
[DHCPServer] dhcp enable
[DHCPServer] dhcp server ip-pool 1
[DHCPServer-dhcp-pool-1] network 10.1.1.0 mask 255.255.0.0
[DHCPServer-dhcp-pool-1] gateway-list 10.1.1.1
[DHCPServer-dhcp-pool-1] quit
[DHCPServer] interface Vlan-interface 1
[DHCPServer-Vlan-interface1] ip address 10.1.1.2 16
```

3) Configure Switch A.

Enable DHCP snooping.

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

Enable ARP intrusion detection in VLAN 1.

```
[SwitchA] vlan 1
[SwitchA-vlan1] arp detection enable
```

Enable MFF.

```
[SwitchA-vlan-1] arp mac-forced-forwarding auto
```

Specify the IP address of the DHCP server.

```
[SwitchA-vlan-1] arp mac-forced-forwarding server 10.1.1.2
```

Configure Ethernet 1/0/2 as an ARP detection trusted port and an DHCP snooping trusted port.

```
[SwitchA] interface ethernet 1/0/2
```

```
[SwitchA-Ethernet1/0/2] arp detection trust
```

```
[SwitchA-Ethernet1/0/2] dhcp-snooping trust
```

Configure Ethernet 1/0/2 as an MFF network port.

```
[SwitchA-Ethernet1/0/2] arp mac-forced-forwarding network-port
```

Enable IP filtering on Ethernet 1/0/1, add it to the port isolation group, and then configure it as an MFF user port.

```
[SwitchA] interface ethernet 1/0/1
```

```
[SwitchA-Ethernet1/0/1] port isolate
```

```
[SwitchA-Ethernet1/0/1] ip check source ip-address
```

```
[SwitchA-Ethernet1/0/1] arp mac-forced-forwarding user-port
```

```
[SwitchA-Ethernet1/0/1] quit
```

Enable IP filtering on Ethernet 1/0/3, add it to the port isolation group, and then configure it as an MFF user port.

```
[SwitchA] interface ethernet 1/0/3
```

```
[SwitchA-Ethernet1/0/3] port isolate
```

```
[SwitchA-Ethernet1/0/3] ip check source ip-address
```

```
[SwitchA-Ethernet1/0/3] arp mac-forced-forwarding user-port
```

```
[SwitchA-Ethernet1/0/3] quit
```

4) Configure Switch B.

Enable DHCP snooping.

```
<SwitchB> system-view
```

```
[SwitchB] dhcp-snooping
```

Enable ARP intrusion detection on VLAN 1.

```
[SwitchB] vlan 1
```

```
[SwitchB-vlan1] arp detection enable
```

Enable MFF.

```
[SwitchB-vlan-1] arp mac-forced-forwarding auto
```

Specify the IP address of the DHCP server.

```
[SwitchB-vlan-1] arp mac-forced-forwarding server 10.1.1.2
```

Configure Ethernet 1/0/2 as an ARP intrusion detection trusted port and an DHCP snooping trusted port.

```
[SwitchB] interface ethernet 1/0/2
```

```
[SwitchB-Ethernet1/0/2] arp detection trust
```

```
[SwitchB-Ethernet1/0/2] dhcp-snooping trust
```

Configure Ethernet 1/0/2 as an MFF network port.

```
[SwitchB-Ethernet1/0/2] arp mac-forced-forwarding network-port
```

Enable IP filtering on Ethernet 1/0/1, add it to the port isolation group, and then configure it as an MFF user port.

```

[SwitchB] interface ethernet 1/0/1
[SwitchB-Ethernet1/0/1] port isolate
[SwitchB-Ethernet1/0/1] ip check source ip-address
[SwitchB-Ethernet1/0/1] arp mac-forced-forwarding user-port
[SwitchB-Ethernet1/0/1] quit
5) Configure Switch C.
# Enable DHCP snooping.
<SwitchC> system-view
[SwitchC] dhcp-snooping

# Enable ARP detection in VLAN 1.
[SwitchC] vlan 1
[SwitchC-vlan-1] arp detection enable

# Enable MFF.
[SwitchC-vlan-1] arp mac-forced-forwarding default-gateway 10.1.1.1

# Specify the IP address of the DHCP server.
[SwitchC-vlan-1] arp mac-forced-forwarding server 10.1.1.2

# Configure Ethernet 1/0/3 as an ARP detection trusted port.
[SwitchC] interface ethernet 1/0/3
[SwitchC-Ethernet1/0/3] arp detection trust

# Configure Ethernet 1/0/3 as a DHCP snooping trusted port.
[SwitchC-Ethernet1/0/3] dhcp-snooping trust

# Configure Ethernet 1/0/3 as an MFF network port.
[SwitchC-Ethernet1/0/3] arp mac-forced-forwarding network-port
[SwitchC-Ethernet1/0/3] quit

# Configure a static binding and enable IP filtering on Ethernet 1/0/2, and then configure it as an MFF
user port.
[SwitchC] interface ethernet1/0/2
[SwitchC-Ethernet1/0/2] ip source static binding ip-address 10.1.1.100 mac-address
0001-0001-0001
[SwitchC-Ethernet1/0/2] ip check source ip-address mac-address
[SwitchC-Ethernet1/0/2] arp mac-forced-forwarding user-port
[SwitchC-Ethernet1/0/2] quit

# Configure Ethernet 1/0/1 and Ethernet 1/0/4 as MFF network ports.
[SwitchC] interface ethernet1/0/1
[SwitchC-Ethernet1/0/1] arp mac-forced-forwarding network-port
[SwitchC-Ethernet1/0/1] quit
[SwitchC] interface ethernet1/0/4
[SwitchC-Ethernet1/0/4] arp mac-forced-forwarding network-port
[SwitchC-Ethernet1/0/4] quit

```



Note

- To ensure that the access-layer switches in the network can correctly learn the DHCP snooping entries from the downstream access-layer switches, after the configuration on all the access-layer switches, you need to disable and then enable the VLAN interfaces of all the access-layer switches. In addition, you need to configure the hosts to obtain IP addresses once again.
 - MFF ensures Layer 3 interoperability among Host A, Host B, Host C and Host D, but not Layer 3 interoperability between these hosts and the access-layer switches Switch A and Switch B.
 - To ensure that user multicast packets are received normally, use the related command, such as **igmp snooping**, on the access-layer switch to make it multicast capable. Otherwise, multicast packets may be discarded by MFF.
-

Troubleshooting MFF Configuration

- Hosts configured with static IP addresses cannot access the network. This is because MFF manual mode is not enabled on the corresponding VLAN of the device connected to these hosts.
- Hosts configured with static IP addresses cannot access the network. This is because the static bindings of the hosts are not configured on the port of the device connected to these hosts.
- Some ARP packets on a user port or a network port cannot be processed correctly and network traffic is interrupted. This is because ARP detection is not enabled on the VLANs to which the user port or network port belongs, or because the network port is not configured as an ARP detection trusted port.
- An access-layer switch and hosts connected to it cannot obtain IP addresses. This is because the corresponding network port is not configured as a DHCP snooping trusted port.
- Packets cannot pass IP filtering or ARP intrusion detection and network traffic is interrupted. This is because DHCP snooping is not enabled on the access-layer switches, or because DHCP snooping is not enabled until the hosts and access-layer switches obtain IP addresses.
- Multicast traffic is interrupted. This is because no multicast command, such as **igmp snooping**, is configured on access-layer switches.

Table of Contents

1 DHCP Overview	1-1
Introduction to DHCP	1-1
DHCP IP Address Assignment	1-2
IP Address Assignment Policy	1-2
Obtaining IP Addresses Dynamically	1-2
Updating IP Address Lease	1-3
DHCP Packet Format	1-3
Protocol Specification	1-4
2 DHCP Server Configuration	2-1
Introduction to DHCP Server	2-1
Usage of DHCP Server	2-1
DHCP Address Pool	2-1
DHCP IP Address Preferences	2-3
IRF Support	2-3
DHCP Server Configuration Task List	2-4
Enabling DHCP	2-4
Configuring the Global Address Pool Based DHCP Server	2-5
Configuration Task List	2-5
Enabling the Global Address Pool Mode on Interface(s)	2-5
Creating a DHCP Global Address Pool	2-6
Configuring an Address Allocation Mode for the Global Address Pool	2-6
Configuring a Domain Name Suffix for the DHCP Client	2-9
Configuring DNS Servers for the DHCP Client	2-9
Configuring WINS Servers for the DHCP Client	2-10
Configuring Gateways for the DHCP Client	2-11
Configuring BIMS Server Information for the DHCP Client	2-11
Configuring Option 184 Parameters for the Client with Voice Service	2-11
Configuring the TFTP Server and Bootfile Name for the DHCP Client	2-14
Configuring a Self-Defined DHCP Option	2-14
Configuring the Interface Address Pool Based DHCP Server	2-15
Configuration Task List	2-15
Enabling the Interface Address Pool Mode on Interface(s)	2-16
Configuring an Address Allocation Mode for an Interface Address Pool	2-17
Configuring a Domain Name Suffix for the DHCP Client	2-19
Configuring DNS Servers for the DHCP Client	2-19
Configuring WINS Servers for the DHCP Client	2-20
Configuring BIMS Server Information for the DHCP Client	2-21
Configuring Option 184 Parameters for the Client with Voice Service	2-21
Configuring the TFTP Server and Bootfile Name for the DHCP Client	2-22
Configuring a Self-Defined DHCP Option	2-23
Configuring DHCP Server Security Functions	2-24
Prerequisites	2-24

Enabling Unauthorized DHCP Server Detection	2-24
Configuring IP Address Detecting	2-24
Configuring DHCP Accounting Functions	2-25
Introduction to DHCP Accounting	2-25
DHCP Accounting Fundamentals	2-25
DHCP Accounting Configuration	2-26
Enabling the DHCP Server to Process Option 82	2-26
Displaying and Maintaining the DHCP Server	2-26
DHCP Server Configuration Examples	2-27
DHCP Server Configuration Example	2-28
DHCP Server with Option 184 Support Configuration Example	2-29
DHCP Accounting Configuration Example	2-31
Troubleshooting a DHCP Server	2-32
3 DHCP Relay Agent Configuration	3-1
Introduction to DHCP Relay Agent	3-1
Usage of DHCP Relay Agent	3-1
DHCP Relay Agent Fundamentals	3-1
Option 82 Support on DHCP Relay Agent	3-2
DHCP Inform Message Handling Feature Used in IRF System	3-3
Configuring the DHCP Relay Agent	3-4
DHCP Relay Agent Configuration Task List	3-4
Enabling DHCP	3-4
Correlating a DHCP Server Group with a Relay Agent Interface	3-5
Configuring DHCP Relay Agent Security Functions	3-6
Configuring the DHCP Relay Agent to Support Option 82	3-9
Configuring DHCP Inform Message Handling Feature Used in IRF System	3-9
Displaying and Maintaining DHCP Relay Agent Configuration	3-10
DHCP Relay Agent Configuration Example	3-10
Troubleshooting DHCP Relay Agent Configuration	3-11
4 DHCP Snooping Configuration	4-1
DHCP Snooping Overview	4-1
Introduction to DHCP Snooping	4-1
Introduction to DHCP-Snooping Option 82	4-2
Introduction to IP Filtering	4-4
Configuring DHCP Snooping	4-5
Configuring DHCP Snooping	4-5
Configuring DHCP Snooping to Support Option 82	4-6
Configuring IP Filtering	4-9
Displaying and Maintaining DHCP Snooping Configuration	4-11
DHCP Snooping Configuration Examples	4-11
DHCP-Snooping Option 82 Support Configuration Example	4-11
IP Filtering Configuration Example	4-12
QoS Profile and IP Filtering Association Configuration Example	4-14
5 DHCP Packet Rate Limit Configuration	5-1
Introduction to DHCP Packet Rate Limit	5-1
Configuring DHCP Packet Rate Limit	5-1

Configuring DHCP Packet Rate Limit.....	5-1
Rate Limit Configuration Example	5-2
6 DHCP/BOOTP Client Configuration	6-1
Introduction to DHCP Client	6-1
Introduction to BOOTP Client	6-1
Configuring a DHCP/BOOTP Client.....	6-2
DHCP Client Configuration Example.....	6-2
BOOTP Client Configuration Example	6-3
Displaying DHCP/BOOTP Client Configuration	6-3

1 DHCP Overview

When configuring DHCP, go to these sections for information you are interested in:

- [Introduction to DHCP](#)
- [DHCP IP Address Assignment](#)
- [DHCP Packet Format](#)
- [Protocol Specification](#)



Note

- The **qos-profile** keyword and IP filtering based on authenticated 802.1x clients are added. For details, refer to [Configuring IP Filtering](#).
 - The function of removing DHCP snooping entries is added in this manual. For details, refer to [Displaying and Maintaining DHCP Snooping Configuration](#).
 - The function of DHCP Inform Message Handling Feature Used in IRF System is added in this manual. For details, refer to [Configuring DHCP Inform Message Handling Feature Used in IRF System](#).
-

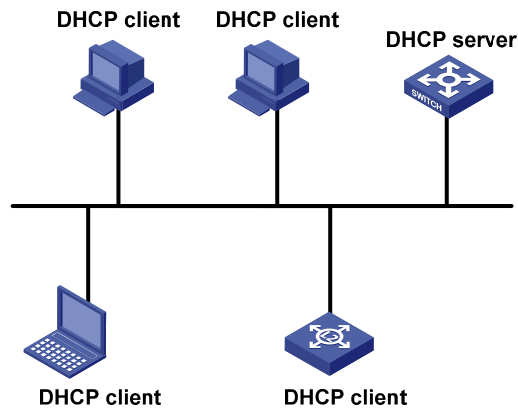
Introduction to DHCP

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 to solve these issues.

DHCP adopts a client/server model, where the DHCP clients send requests to DHCP servers for configuration parameters; and the DHCP servers return the corresponding configuration information such as IP addresses to implement dynamic allocation of network resources.

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



DHCP IP Address Assignment

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 configures static IP-to-MAC bindings for some special clients, such as a 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.

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 from the DHCP client, it chooses an unassigned IP address from the address pool 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 [DHCP Packet Format](#) for details.
- 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

- After the client receives the DHCP-ACK message, it will probe whether the IP address assigned by the server is in use by broadcasting a gratuitous ARP packet. If the client receives no response within specified time, the client can use this IP address. Otherwise, the client sends a DHCP-DECLINE message to the server and requests an IP address again.
 - If there are multiple DHCP servers, IP addresses offered by other DHCP servers are assignable to other clients.
-

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.

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

0	7	15	23	31
op (1)	htype (1)		hlen (1)	hops (1)
xid (4)				
secs (2)		flags (2)		
ciaddr (4)				
yiaddr (4)				
siaddr (4)				
giaddr (4)				
chaddr (16)				
sname (64)				
file (128)				
options (variable)				

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 relay agents which a DHCP packet passes. For each DHCP relay agent 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, used to identify that the DHCP response packet is a unicast (set to 0) or broadcast (set to 1). 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 agent that the DHCP client passes after it sent the request packet.
- 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.

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
- RFC3046: DHCP Relay Agent Information option

2 DHCP Server Configuration

When configuring the DHCP server, go to these sections for information you are interested in:

- [Introduction to DHCP Server](#)
- [DHCP Server Configuration Task List](#)
- [Enabling DHCP](#)
- [Configuring the Global Address Pool Based DHCP Server](#)
- [Configuring the Interface Address Pool Based DHCP Server](#)
- [Configuring DHCP Server Security Functions](#)
- [Configuring DHCP Accounting Functions](#)
- [Enabling the DHCP Server to Process Option 82](#)
- [Displaying and Maintaining the DHCP Server](#)
- [DHCP Server Configuration Examples](#)
- [Troubleshooting a DHCP Server](#)



Note

- The contents of this chapter are only applicable to the S3600-EI series among S3600 series switches.
 - Currently, the interface-related DHCP server configurations can only be made on VLAN interfaces.
-

Introduction to DHCP Server

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.

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.

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.

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.



Note

The IP address lease does not enjoy the inheritance attribute.

Principles of address pool selection

The DHCP server observes the following principles to select an address pool to assign an IP address to a client:

- 1) If the receiving interface works in the global address pool mode, the DHCP server assigns an IP address from the global address pool to the DHCP client.
- 2) If the receiving interface works in the interface address pool mode, the DHCP server assigns an IP address from the interface address pool to the DHCP client directly connected to the interface. If there is no available IP address in the interface address pool, the DHCP server selects an IP address from the global address pool that contains the interface address pool's network segment for the client.

The DHCP server assigns an IP address to the client in the following order from an interface address pool or a global address pool:

- 3) If there is an address pool where an IP address is statically bound to the MAC address or ID of the client, the DHCP server will select this address pool and assign the statically bound IP address to the client.
- 4) Otherwise, the DHCP server observes the following principles to select a dynamic address pool.
 - If the client and the server reside in the same network segment, the smallest address pool that contains the IP address of the receiving interface will be selected.
 - If the client and the server do not reside in the same network segment (that is, a DHCP relay agent is in-between), the smallest address pool that contains the IP address specified in the giaddr field of the client's request will be selected.
 - If no assignable IP address is available in the selected address pool, the DHCP server will not assign any IP address to the client because it cannot assign an IP address from the parent address pool to the client.

DHCP IP Address Preferences

A DHCP server assigns IP addresses in interface address pools or global address pools to DHCP clients in the following sequence:

- 1) IP addresses that are statically bound to the MAC addresses of DHCP clients or client IDs.
- 2) The IP address that was ever assigned to the client
- 3) The IP address designated by the Option 50 field in a DHCP-DISCOVER message
- 4) The first assignable IP address found in a proper DHCP address pool
- 5) 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.

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 or 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.

DHCP Server Configuration Task List

Complete the following tasks to configure the DHCP server:

Task		Remarks
Enabling DHCP		Required
Configure address pool based DHCP server	Configuring the Global Address Pool Based DHCP Server	One of the two options is required
	Configuring the Interface Address Pool Based DHCP Server	
Configuring DHCP Server Security Functions		Optional
Configuring DHCP Accounting Functions		Optional
Enabling the DHCP Server to Process Option 82		Optional

Enabling DHCP

You need to enable DHCP to make other related configurations take effect.

Follow these steps to enable DHCP:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable DHCP	dhcp enable	Optional By default, DHCP is enabled.



Note

To improve security and avoid malicious attacks to unused sockets, S3600 Ethernet switches provide the following functions:

- UDP port 67 and UDP port 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP port 67 and UDP port 68 ports are disabled when DHCP is disabled.

The corresponding implementation is as follows:

- After DHCP is enabled with the **dhcp enable** command, if the DHCP server and DHCP relay agent functions are not configured, UDP port 67 and UDP port 68 ports are kept disabled; if the DHCP server or DHCP relay agent function is configured, UDP port 67 and UDP port 68 ports are enabled.
- After DHCP is disabled with the **undo dhcp enable** command, even if the DHCP server or DHCP relay function is configured, UDP port 67 and UDP port 68 ports will be disabled.

Configuring the Global Address Pool Based DHCP Server

Configuration Task List

Complete the following tasks to configure the global address pool based DHCP server:

Task		Remarks
Enabling the Global Address Pool Mode on Interface(s)		Required
Creating a DHCP Global Address Pool		Required
Configuring an Address Allocation Mode for the Global Address Pool	Configuring the static IP address allocation mode	One of the two options is required
	Configuring the dynamic IP address allocation mode	Only one mode can be selected for the same global address pool.
Configuring a Domain Name Suffix for the DHCP Client		Optional
Configuring DNS Servers for the DHCP Client		Optional
Configuring WINS Servers for the DHCP Client		Optional
Configuring Gateways for the DHCP Client		Optional
Configuring BIMS Server Information for the DHCP Client		Optional
Configuring Option 184 Parameters for the Client with Voice Service		Optional
Configuring the TFTP Server and Bootfile Name for the DHCP Client		Optional
Configuring a Self-Defined DHCP Option		Optional

Enabling the 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.

Follow these steps to configure the global address pool mode on interface(s):

To do...		Use the command...	Remarks
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 <i>interface-type interface-number</i>	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 <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>] all }	

Creating a DHCP Global Address Pool

Follow these steps to create a DHCP address pool:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a DHCP global address pool and enter its view	dhcp server ip-pool <i>pool-name</i>	Required Not created by default.

Configuring an Address Allocation Mode for the Global Address Pool



Note

You can configure either the static IP address allocation mode or the dynamic IP address allocation mode for a global address pool, and only one mode can be configured for one DHCP global address pool.

For dynamic IP address allocation, 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.

Configuring the static IP address allocation mode

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 requests 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. If the bindings of client IDs and IP addresses are configured on the DHCP server, when such a client requests an IP address, the DHCP server will find the corresponding IP address based on the client ID and assign it to the DHCP client.

Currently, only one IP address in a global DHCP address pool can be statically bound to a MAC address or a client ID.

Follow these steps to configure the static IP address allocation mode:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enter DHCP address pool view		dhcp server ip-pool <i>pool-name</i>	—
Configure an IP address to be statically bound		static-bind ip-address <i>ip-address [mask mask]</i>	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 <i>mac-address</i>	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 <i>client-identifier</i>	



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.

Configuring the dynamic IP address allocation mode

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 address conflicts, the DHCP server automatically excludes IP addresses (used by the gateway, FTP server and so forth) specified with the **dhcp server forbidden-ip** command from dynamic allocation.

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.

Follow these steps to configure the dynamic IP address allocation mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter DHCP address pool view	dhcp server ip-pool <i>pool-name</i>	—
Set the IP address segment whose IP address are to be assigned dynamically	network <i>network-address</i> [mask <i>mask</i>]	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 <i>day</i> [hour <i>hour</i> [minute <i>minute</i>]] unlimited }	Optional The default lease time is one day
Return to system view	quit	—
Specify the IP addresses that are not dynamically assigned	dhcp server forbidden-ip <i>low-ip-address</i> [<i>high-ip-address</i>]	Optional By default, except the IP addresses of DHCP server interfaces, all IP addresses in a DHCP address pool are assignable.



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 or ID has been bound.

Configuring a Domain Name Suffix for the DHCP Client

You can configure a domain name suffix in each DHCP address pool on the DHCP server. The DHCP server will provide the domain name suffix together with an IP address to the DHCP client.

With this suffix assigned, the client needs only input part of the domain name, and the system will add the domain name suffix for name resolution. For details about DNS, refer to *DNS Operation* in this manual.

Follow these steps to configure a domain name suffix for the DHCP client:

To do...	Use the command...	Remarks
Enter system view	<code>system-view</code>	—
Enter DHCP address pool view	dhcp server ip-pool <i>pool-name</i>	—
Configure a domain name suffix for the client	domain-name <i>domain-name</i>	Required Not configured by default.

Configuring DNS Servers for the DHCP Client

If a client accesses a host on the Internet through domain name, DNS (domain name system) is needed to translate the domain name into the corresponding IP address. To enable DHCP clients to access hosts on 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.

Follow these steps to configure DNS servers for the DHCP client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter DHCP address pool view	dhcp server ip-pool <i>pool-name</i>	—
Configure DNS server addresses for DHCP clients	dns-list <i>ip-address&<1-8></i>	Required By default, no DNS server address is configured.

Configuring WINS Servers for the DHCP Client

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.

To implement host name-to-IP address translation for DHCP clients, you should enable the DHCP server to assign WINS server addresses when assigning IP addresses to DHCP clients. 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.

Follow these steps to configure WINS servers for the DHCP client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter DHCP address pool view	dhcp server ip-pool <i>pool-name</i>	—
Configure WINS server addresses for DHCP clients	nbns-list <i>ip-address</i> &<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.



Note

If b-node is specified for the client, you don't need to specify any WINS server address.

Configuring Gateways for the DHCP Client

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 global address pools on a DHCP server. Currently, you can configure up to eight gateway addresses for a DHCP address pool.

Follow these steps to configure gateways for the DHCP client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter DHCP address pool view	dhcp server ip-pool <i>pool-name</i>	—
Configure gateway addresses for DHCP clients	gateway-list <i>ip-address&<1-8></i>	Required By default, no gateway address is configured.

Configuring BIMS Server Information for the DHCP Client

A DHCP client performs regular software update and backup using configuration files obtained from a branch intelligent management system (BIMS) server. Therefore, the DHCP server needs to offer DHCP clients the BIMS server IP address, port number, shared key from the DHCP address pool.

Follow these steps to configure BIMS server information for the DHCP client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter DHCP address pool view	dhcp server ip-pool <i>pool-name</i>	—
Configure the BIMS server information to be assigned to the DHCP client	bims-server ip <i>ip-address</i> [port <i>port-number</i>] sharekey <i>key</i>	Required By default, no BIMS server information is configured.

Configuring Option 184 Parameters for the Client with Voice Service

Option 184 is a reserved option, and the information it carries can be customized. You can define four sub-options for this option after enabling the DHCP server. Thus, besides obtaining an IP address, the DHCP client with voice services can obtain voice related parameters from the DHCP address pool.

Basic concept

The four sub-options of Option 184 mainly carry information about voice. The following lists the sub-options and the carried information:

- Sub-option 1: IP address of the network call processor (NCP-IP).
- Sub-option 2: IP address of the alternate server (AS-IP).
- Sub-option 3: Voice VLAN configuration.

- Sub-option 4: Fail-over call routing.

Meanings of the sub-options for Option 184

Table 2-1 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
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 need to configure the DHCP server to add sub-option 1.

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 on the 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.

Configuring Option 184 Parameters for the DHCP Client with Voice Service

Follow these steps to configure Option 184 parameters for the DHCP client with voice service:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter DHCP address pool view	dhcp server ip-pool <i>pool-name</i>	—
Specify the IP address of the primary network calling processor	voice-config ncp-ip <i>ip-address</i>	Required Not specified by default.
Specify the IP address of the backup network calling processor	voice-config as-ip <i>ip-address</i>	Optional Not specified by default.
Configure the voice VLAN	voice-config voice-vlan <i>vlan-id</i> { disable enable }	Optional Not configured by default.
Specify the failover IP address	voice-config fail-over <i>ip-address dialer-string</i>	Optional No failover IP address is specified by default.



Note

Specify an IP address for the network calling processor before performing other configuration.

Configuring the TFTP Server and Bootfile Name for the DHCP Client

This task is to specify the IP address and name of a TFTP server and the bootfile name in the DHCP global address pool. The DHCP clients use these parameters to contact the TFTP server, requesting the configuration file used for system initialization, which is called auto-configuration. The request process of the client is described below:

- 1) When a switch starts up without loading any configuration file, the system sets the specified interface (VLAN-interface 1) as the DHCP client to request from the DHCP server parameters such as the IP address and name of a TFTP server, and bootfile name.
- 2) After getting related parameters, the DHCP client will send a TFTP request to obtain the configuration file from the specified TFTP server for system initialization. If the client cannot get related parameters, it will perform system initialization without loading any configuration file.

To implement auto-configuration, you need to specify the IP address and name of a TFTP server and the bootfile name on the DHCP server, but you do not need to perform any configuration on the DHCP client.

When Option 55 in a client's request contains parameters of Option 66, Option 67, or Option 150, the DHCP server will return the IP address and name of the specified TFTP server, bootfile name and an IP address to the client, which uses such information to complete auto-configuration.

Follow these steps to configure the TFTP server and bootfile name for the DHCP client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter DHCP address pool view	dhcp server ip-pool <i>pool-name</i>	—
Specify the TFTP server	tftp-server ip-address <i>ip-address</i>	Optional Not specified by default.
Specify the name of the TFTP server	tftp-server domain-name <i>domain-name</i>	Optional Not specified by default.
Specify the bootfile name	bootfile-name <i>bootfile-name</i>	Optional Not specified by default.

Configuring a Self-Defined DHCP Option

By configuring self-defined DHCP options, you can:

- Define new DHCP options. New configuration options will come out with DHCP development. To support new options, you can add them into the attribute list of the DHCP server.
- Extend existing DHCP options. When the current DHCP options cannot meet customers' requirements (for example, you cannot use the **dns-list** command to configure more than eight DNS server addresses), you can configure a self defined option for extension.

Follow these steps to configure a self-defined DHCP option:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter DHCP address pool view	dhcp server ip-pool <i>pool-name</i>	—
Configure a self-defined DHCP option	option code { ascii <i>ascii-string</i> hex <i>hex-string</i><1-10> ip-address <i>ip-address</i><1-8> }	Required Not configured by default.



Caution

Be cautious when configuring self-defined DHCP options because such configuration may affect the DHCP operation process.

Configuring the Interface Address Pool Based DHCP Server



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 network 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 on the same network segment, so the clients cannot communicate with each other.

Therefore, in the interface address pool mode, if the DHCP clients in a VLAN need to obtain IP addresses from the same network segment, the number of DHCP clients cannot exceed the number of the IP addresses assignable in the VLAN interface address pool.

Configuration Task List

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.

Complete the following tasks to configure the interface address pool based DHCP server:

Task		Remarks
Enabling the Interface Address Pool Mode on Interface(s)		Required
Configuring an Address Allocation Mode for an Interface Address Pool	Configuring the static IP address allocation mode	One of the two options is required. And these two options can be configured at the same time.
	Configuring the dynamic IP address allocation mode	
Configuring a Domain Name Suffix for the DHCP Client		Optional
Configuring DNS Servers for the DHCP Client		Optional
Configuring WINS Servers for the DHCP Client		Optional
Configuring BIMS Server Information for the DHCP Client		Optional
Configuring Option 184 Parameters for the Client with Voice Service		Optional
Configuring the TFTP Server and Bootfile Name for the DHCP Client		Optional
Configuring a Self-Defined DHCP Option		Optional



Note

When an S3600-EI Ethernet switch works in the interface address pool mode as a DHCP server, the only gateway address it can assign to a client is the primary IP address of the interface.

Enabling the Interface Address Pool Mode on Interface(s)

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.

Follow these steps to configure interface address pool mode on interface(s):

To do...		Use the command...	Remarks
Enter system view		system-view	—
Configure interface address pool mode	On the current interface	interface <i>interface-type interface-number</i>	Required By default, a DHCP server assigns the IP addresses of the global address pool to DHCP clients.
		dhcp select interface	
		quit	
	On multiple interfaces in system view	dhcp select interface { interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>] all }	

You need to configure an IP address for the interface before enabling the interface address pool mode on it.



Note

To improve security and avoid malicious attack to the unused sockets, S3600 Ethernet switches provide the following functions:

- UDP port 67 and UDP port 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP port 67 and UDP port 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 port 67 and UDP port 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 port 67 and UDP port 68 ports used by DHCP are disabled accordingly.

Configuring an Address Allocation Mode for an Interface Address Pool

IP addresses of an interface address pool can be statically bound to DHCP clients or dynamically allocated to DHCP clients.

Configuring the static IP address allocation mode

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.

Follow these steps to configure the static IP address allocation mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure static binding	dhcp server static-bind ip-address <i>ip-address</i> { client-identifier <i>client-identifier</i> mac-address <i>mac-address</i> }	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 network 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.

Configuring the dynamic IP address allocation mode

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 address conflicts, the DHCP server automatically excludes IP addresses (used by the gateway, FTP server and so forth) specified with the **dhcp server forbidden-ip** command from dynamic allocation.

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.

Follow these steps to configure the dynamic IP address allocation mode:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Configure the lease time	Configure for the current interface	interface <i>interface-type interface-number</i>	Optional The default lease time is one day.
		dhcp server expired { day <i>day</i> [hour <i>hour</i> [minute <i>minute</i>]] unlimited }	
		quit	
	Configure multiple interfaces in system view	dhcp server expired { day <i>day</i> [hour <i>hour</i> [minute <i>minute</i>]] unlimited } { interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>] all }	

To do...	Use the command...	Remarks
Specify the IP addresses that are not dynamically assigned	dhcp server forbidden-ip <i>low-ip-address [high-ip-address]</i>	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 or client ID has been bound.

Configuring a Domain Name Suffix for the DHCP Client

You can configure a suffix for the domain name in each DHCP interface address pool on the DHCP server. The DHCP server provides the domain name suffix together with an IP address for a requesting DHCP client.

Follow these steps to configure a domain name suffix for the client:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Configure a domain name suffix for the clients	In the current interface address pool	interface <i>interface-type interface-number</i>	Required Not configured by default.
		dhcp server domain-name <i>domain-name</i>	
		quit	
	In multiple interface address pools in system view	dhcp server domain-name <i>domain-name</i> { all interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>] }	

Configuring DNS Servers for the DHCP Client

If a client accesses a host on the Internet through domain name, DNS is needed to translate the domain name into the corresponding IP address. To enable DHCP clients to access hosts on 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.

Follow these steps to configure DNS servers for the DHCP client:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Configure DNS server addresses for DHCP clients	Configure the current interface	interface <i>interface-type interface-number</i>	Required By default, no DNS server address is configured.
		dhcp server dns-list <i>ip-address&<1-8></i>	
		quit	
	Configure multiple interfaces in system view	dhcp server dns-list <i>ip-address&<1-8></i> { interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>] all }	

Configuring WINS Servers for the DHCP Client

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.

To implement host name-to-IP address translation for DHCP clients, you should enable the DHCP server to assign WINS server addresses when assigning IP addresses to DHCP clients. 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.

Follow these steps to configure WINS servers for the DHCP client:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Configure WINS server addresses for DHCP clients	Configure the current interface	interface <i>interface-type interface-number</i>	Required By default, no WINS server address is
		dhcp server nbns-list <i>ip-address&<1-8></i>	
		quit	

To do...		Use the command...	Remarks
	Configure multiple interfaces in system view	dhcp server nbns-list <i>ip-address</i> <1-8> { interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>] all }	configured.
Configure a NetBIOS node type for DHCP clients	Configure the current interface	interface <i>interface-type interface-number</i>	Required By default, no NetBIOS node type is specified.
		dhcp server netbios-type { b-node h-node m-node p-node }	
	Configure multiple interfaces in system view	quit dhcp server netbios-type { b-node h-node m-node p-node } { interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>] all }	



Note

If b-node is specified for the client, you don't need to specify any WINS server address.

Configuring BIMS Server Information for the DHCP Client

A DHCP client performs regular software update and backup using configuration files obtained from a BIMS server. Therefore, the DHCP server needs to offer DHCP clients the BIMS server IP address, port number, shared key from the DHCP address pool.

Follow these steps to configure BIMS server information for the DHCP client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the BIMS server information to be assigned to the DHCP client	dhcp server bims-server ip <i>ip-address</i> [port <i>port-number</i>] sharekey <i>key</i> { interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>] all }	Required By default, no BIMS server information is configured.

Configuring Option 184 Parameters for the Client with Voice Service

For details about Option 184, refer to [Configuring Option 184 Parameters for the Client with Voice Service](#).

Follow these steps to configure Option 184 parameters for the client with voice service:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Configure Option 184 in the current interface address pool	Enter interface view	interface interface-type interface-number	—
	Specify the primary network calling processor	dhcp server voice-config ncp-ip ip-address	Required Not specified by default.
	Specify the backup network calling processor	dhcp server voice-config as-ip ip-address	Optional Not specified by default.
	Configure the voice VLAN	dhcp server voice-config voice-vlan vlan-id { disable enable }	Optional Not configured by default.
	Specify the failover IP address	dhcp server voice-config fail-over ip-address dialer-string	Optional Not specified by default.
	Return to system view	quit	—
Configure Option 184 in multiple interface address pools	Specify the primary network calling processor	dhcp server voice-config ncp-ip ip-address { all interface interface-type interface-number [to interface-type interface-number] }	Required Not specified by default.
	Specify the backup network calling processor	dhcp server voice-config as-ip ip-address { all interface interface-type interface-number [to interface-type interface-number] }	Optional Not specified by default.
	Configure the voice VLAN	dhcp server voice-config voice-vlan vlan-id { disable enable } { all interface interface-type interface-number [to interface-type interface-number] }	Optional Not specified by default.
	Specify the failover IP address	dhcp server voice-config fail-over ip-address dialer-string { all interface interface-type interface-number [to interface-type interface-number] }	Optional Not specified by default.



Note

Specify an IP address for the network calling processor before performing other configuration.

Configuring the TFTP Server and Bootfile Name for the DHCP Client

For related principles, refer to [Configuring the TFTP Server and Bootfile Name for the DHCP Client](#).

Follow these steps to configure the TFTP server and bootfile name for the DHCP client:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Specify the IP address and name of the TFTP server and the bootfile name in the current interface address pool	Enter interface view	interface <i>interface-type interface-number</i>	—
	Specify the TFTP server	dhcp server tftp-server ip-address <i>ip-address</i>	Optional Not specified by default.
	Specify the TFTP server name	dhcp server tftp-server domain-name <i>domain-name</i>	
	Specify the bootfile name	dhcp server bootfile-name <i>bootfile-name</i>	
	Return to system view	quit	—
Specify the IP address and name of the TFTP server and the bootfile name in the specified interface address pool	Specify the TFTP server	dhcp server tftp-server ip-address <i>ip-address { all interface interface-type interface-number }</i>	Optional Not specified by default.
	Specify the TFTP server name	dhcp server tftp-server domain-name <i>domain-name { all interface interface-type interface-number }</i>	
	Specify the bootfile name	dhcp server bootfile-name <i>bootfile-name { all interface interface-type interface-number }</i>	

Configuring a Self-Defined DHCP Option

By configuring self-defined DHCP options, you can:

- Define new DHCP options. New configuration options will come out with DHCP development. To support new options, you can add them into the attribute list of the DHCP server.
- Extend existing DHCP options. When the current DHCP options cannot meet customers' requirements (for example, you cannot use the **dns-list** command to configure more than eight DNS server addresses), you can configure a self defined option for extension.

Follow these steps to customize the DHCP service:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Configure customized options	Configure the current interface	interface <i>interface-type interface-number</i>	Required By default, no customized option is configured.
		dhcp server option code { ascii <i>ascii-string</i> hex <i>hex-string</i> &<1-10> ip-address <i>ip-address</i> &<1-8> }	
		quit	
	Configure multiple interfaces in system view	dhcp server option code { ascii <i>ascii-string</i> hex <i>hex-string</i> &<1-10> ip-address <i>ip-address</i> &<1-8> } { interface <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>] all }	



Caution

Be cautious when configuring self-defined DHCP options because such configuration may affect the DHCP operation process.

Configuring DHCP Server Security Functions

DHCP security configuration is needed to ensure the security of DHCP service.

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).

Enabling Unauthorized DHCP Server Detection

If there is an unauthorized DHCP server in the network, when a client applies for an IP address, the unauthorized DHCP server may assign an incorrect IP address to the client.

With this feature enabled, when receiving a DHCP message with the siaddr field not being 0 from a client, the DHCP server will record the value of the siaddr field and the receiving interface. The administrator can use such information to check out any DHCP unauthorized servers.

Follow these steps to enable unauthorized DHCP server detection:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the unauthorized DHCP server detecting function	dhcp server detect	Required Disabled by default.



Note

With the unauthorized DHCP server detection enabled, the relay agent will log all DHCP servers, including authorized ones, and each server is recorded only once. The administrator needs to find unauthorized DHCP servers from the system log information.

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.

The DHCP server pings the IP address to be assigned using ICMP. If the server gets a response within the specified period, the server will ping another IP address; otherwise, the server will ping the IP addresses once again until the specified number of ping packets are sent. If still no response, the server

will assign the IP address to the requesting client (The DHCP client probes the IP address by sending gratuitous ARP packets).

Follow these steps to configure IP address detecting:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify the number of ping packets	dhcp server ping packets <i>number</i>	Optional Two ping packets by default.
Configure a timeout waiting for ping responses	dhcp server ping timeout <i>milliseconds</i>	Optional 500 ms by default.

Configuring DHCP Accounting Functions

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.

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 *AAA Operation* 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, 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.



Note

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.

DHCP Accounting Configuration

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.

Configuring DHCP Accounting

Follow these steps to configure DHCP accounting:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter address pool view	dhcp server ip-pool <i>pool-name</i>	Required
Enable DHCP accounting	accounting domain <i>domain-name</i>	Required The domain identified by the <i>domain-name</i> argument can be created by using the domain command.

Enabling the DHCP Server to Process Option 82

If a DHCP server is enabled to process Option 82, after the DHCP server receives packets containing Option 82, the DHCP server adds Option 82 into the responses when assigning IP addresses and other configuration information to the clients.

If a DHCP server is configured to ignore Option 82, after the DHCP server receives packets containing Option 82, the DHCP server will not add Option 82 into the responses when assigning IP addresses and other configuration information to the clients.

For details of Option 82, see section [Option 82 Support on DHCP Relay Agent](#).

Follow these steps to configure the DHCP server to process Option 82:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the DHCP server to process Option 82	dhcp server relay information enable	Optional By default, the DHCP server supports Option 82.

Displaying and Maintaining the DHCP Server

To do...	Use the command...	Remarks
Display the statistics on IP address conflicts	display dhcp server conflict { all ip <i>ip-address</i> }	Available in any view

To do...	Use the command...	Remarks
Display lease expiration information	display dhcp server expired { ip <i>ip-address</i> pool [<i>pool-name</i>] interface [<i>interface-type</i> <i>interface-number</i>] all }	
Display the free IP addresses	display dhcp server free-ip	
Display information about address binding	display dhcp server ip-in-use { ip <i>ip-address</i> pool [<i>pool-name</i>] interface [<i>interface-type</i> <i>interface-number</i>] all }	
Display the statistics on a DHCP server	display dhcp server statistics	
Display information about DHCP address pool tree	display dhcp server tree { pool [<i>pool-name</i>] interface [<i>interface-type</i> <i>interface-number</i>] all }	
Clear IP address conflict statistics	reset dhcp server conflict { all ip <i>ip-address</i> }	Available in user view
Clear dynamic address binding information	reset dhcp server ip-in-use { ip <i>ip-address</i> pool [<i>pool-name</i>] interface [<i>interface-type</i> <i>interface-number</i>] 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.

DHCP Server Configuration Examples

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 agent. Note that DHCP server configuration is the same in both scenarios.

DHCP Server Configuration Example

Network requirements

- The DHCP server (Switch A) assigns IP address to clients in subnet 10.1.1.0/24, which is subnetted into 10.1.1.0/25 and 10.1.1.128/25.
- The IP addresses of VLAN-interface 1 and VLAN-interface 2 on Switch A are 10.1.1.1/25 and 10.1.1.129/25 respectively.
- In the address pool 10.1.1.0/25, the address lease duration is ten days and twelve hours, domain name suffix aabbcc.com, DNS server address 10.1.1.2, gateway 10.1.1.126, and WINS server 10.1.1.4.
- In the address pool 10.1.1.128/25, the address lease duration is five days, domain name suffix aabbcc.com, DNS server address 10.1.1.2, and gateway address 10.1.1.254, and there is no WINS server address.



Note

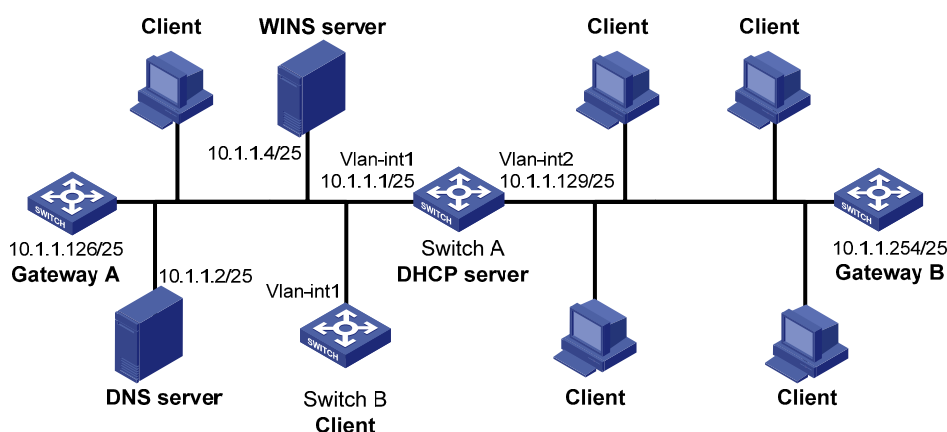
If you use the inheriting relation of parent and child address pools, make sure that the number of the assigned IP addresses does not exceed the number of the IP addresses in the child address pool; otherwise extra IP addresses will be obtained from the parent address pool, and the attributes (for example, gateway) also are based on the configuration of the parent address pool.

For example, in the network to which VLAN-interface 1 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-interface 1 is recommended to be less than or equal to 122 and the number of clients applying for IP addresses from VLAN-interface 2 is recommended to be less than or equal to 124.

Network diagram

Figure 2-1 Network diagram for DHCP configuration



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.

```
<SwitchA> system-view
```

```
[SwitchA] dhcp enable
```

Configure the IP addresses that are not dynamically assigned. (That is, the IP addresses of the DNS server, WINS server, and gateways.)

```
[SwitchA] dhcp server forbidden-ip 10.1.1.2
```

```
[SwitchA] dhcp server forbidden-ip 10.1.1.4
```

```
[SwitchA] dhcp server forbidden-ip 10.1.1.126
```

```
[SwitchA] dhcp server forbidden-ip 10.1.1.254
```

Configure DHCP address pool 0, including address range, domain name suffix of the clients, and domain name server address.

```
[SwitchA] dhcp server ip-pool 0
```

```
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

```
[SwitchA-dhcp-pool-0] domain-name aabbcc.com
```

```
[SwitchA-dhcp-pool-0] dns-list 10.1.1.2
```

```
[SwitchA-dhcp-pool-0] quit
```

Configure DHCP address pool 1, including address range, gateway, WINS server address and lease time.

```
[SwitchA] dhcp server ip-pool 1
```

```
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
```

```
[SwitchA-dhcp-pool-1] gateway-list 10.1.1.126
```

```
[SwitchA-dhcp-pool-1] expired day 10 hour 12
```

```
[SwitchA-dhcp-pool-1] nbns-list 10.1.1.4
```

```
[SwitchA-dhcp-pool-1] quit
```

Configure DHCP address pool 2, including address range, gateway and lease time.

```
[SwitchA] dhcp server ip-pool 2
```

```
[SwitchA-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
```

```
[SwitchA-dhcp-pool-2] expired day 5
```

```
[SwitchA-dhcp-pool-2] gateway-list 10.1.1.254
```

DHCP Server with Option 184 Support Configuration Example

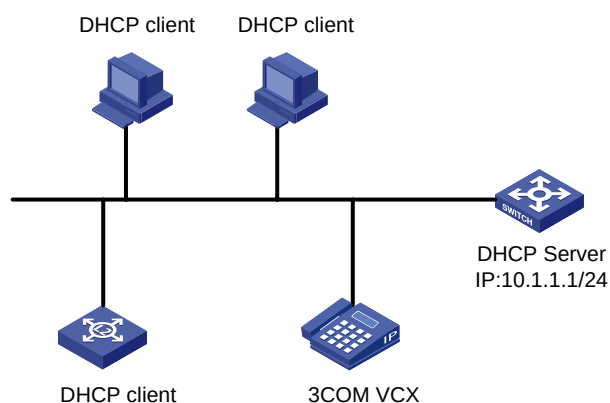
Network requirements

A 3COM VCX device operating as a DHCP client requests the DHCP server for all sub-options of Option 184. An H3C series switch operates as the DHCP server. The Option 184 support 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*

Network diagram

Figure 2-2 Network diagram for Option 184 support configuration



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.

```
<Sysname> system-view
```

Add Ethernet 1/0/1 to VLAN 2 and configure the IP address of VLAN 2 interface to be 10.1.1.1/24.

```
[Sysname] vlan 2
```

```
[Sysname-vlan2] port ethernet 1/0/1
```

```
[Sysname-vlan2] quit
```

```
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
```

```
[Sysname-Vlan-interface2] quit
```

Configure VLAN-interface 2 to operate in the DHCP server mode.

```
[Sysname] dhcp select global interface vlan-interface 2
```

Enter DHCP address pool view.

```
[Sysname] dhcp server ip-pool 123
```

Configure sub-options of Option 184 in global DHCP address pool view.

```
[Sysname-dhcp-pool-123] network 10.1.1.1 mask 255.255.255.0
```

```
[Sysname-dhcp-pool-123] voice-config ncp-ip 3.3.3.3
```

```
[Sysname-dhcp-pool-123] voice-config as-ip 2.2.2.2
```

```
[Sysname-dhcp-pool-123] voice-config voice-vlan 3 enable
```

```
[Sysname-dhcp-pool-123] voice-config fail-over 1.1.1.1 99*
```

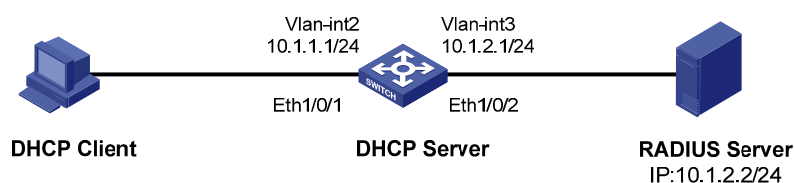
DHCP Accounting Configuration Example

Network requirements

- The DHCP server connects to a DHCP client and a RADIUS server respectively through Ethernet 1/0/1 and Ethernet 1/0/2.
- Ethernet 1/0/1 belongs to VLAN 2; Ethernet 1/0/2 belongs to VLAN 3.
- The IP address of VLAN-interface 1 is 10.1.1.1/24, and that of VLAN-interface 2 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. The DHCP server operates as a RADIUS client and adopts AAA for authentication.

Network diagram

Figure 2-3 Network diagram for DHCP accounting configuration



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

Create VLAN 2.

```
[Sysname] vlan 2
```

```
[Sysname-vlan2] quit
```

Create VLAN 3.

```
[Sysname] vlan 3
```

```
[Sysname-vlan3] quit
```

Enter Ethernet 1/0/1 port view and add the port to VLAN 2.

```
[Sysname] interface ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] port access vlan 2
```

```
[Sysname-Ethernet1/0/1] quit
```

Enter Ethernet 1/0/2 port view and add the port to VLAN 3.

```
[Sysname] interface ethernet 1/0/2
```

```
[Sysname-Ethernet1/0/2] port access vlan 3
```

```
[Sysname-Ethernet1/0/2] quit
```

Enter VLAN 2 interface view and assign the IP address 10.1.1.1/24 to the VLAN interface.

```
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] ip address 10.1.1.1 24
```

```
[Sysname-Vlan-interface2] quit
```

Enter VLAN 3 interface view and assign the IP address 10.1.2.1/24 to the VLAN interface.

```
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] ip address 10.1.2.1 24
[Sysname-Vlan-interface3] quit

# Create a domain and a RADIUS scheme. Associate the domain with the RADIUS scheme.

[Sysname] radius scheme 123
[Sysname-radius-123] primary authentication 10.1.2.2
[Sysname-radius-123] primary accounting 10.1.2.2
[Sysname] domain 123
[Sysname-isp-123] scheme radius-scheme 123
[Sysname-isp-123] quit

# Create an address pool on the DHCP server.

[Sysname] dhcp server ip-pool test
[Sysname-dhcp-pool-test] network 10.1.1.0 mask 255.255.255.0

# Enable DHCP accounting.

[Sysname-dhcp-pool-test] accounting domain 123
```

Troubleshooting a DHCP Server

Symptom

The IP address dynamically assigned by a DHCP server to a client conflicts with the IP address of another host.

Analysis

With DHCP enabled, IP address conflicts are usually caused by IP addresses that are manually configured on hosts.

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.

3 DHCP Relay Agent Configuration

When configuring the DHCP relay agent, go to these sections for information you are interested in:

- [Introduction to DHCP Relay Agent](#)
- [Configuring the DHCP Relay Agent](#)
- [Displaying and Maintaining DHCP Relay Agent Configuration](#)
- [DHCP Relay Agent Configuration Example](#)
- [Troubleshooting DHCP Relay Agent Configuration](#)



Note

Currently, the interface-related DHCP relay agent configurations can only be made on VLAN interfaces.

Introduction to DHCP Relay Agent

Usage of DHCP Relay Agent

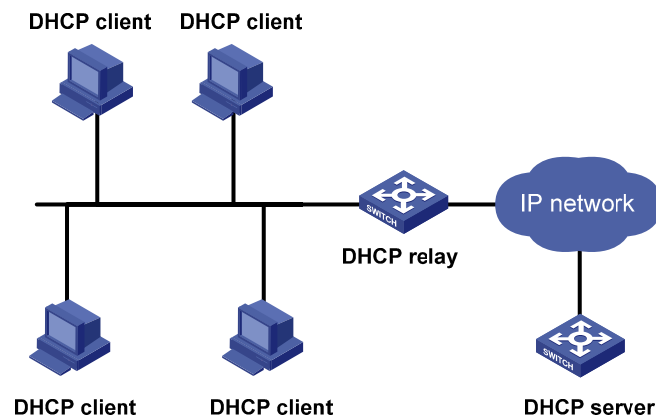
Since the packets are broadcasted in the process of obtaining IP addresses, DHCP is only applicable to the situation that DHCP clients and DHCP servers are in the same network segment, that is, you need to deploy at least one DHCP server for each network segment, which is far from economical.

DHCP relay agent 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.

DHCP Relay Agent Fundamentals

[Figure 3-1](#) illustrates a typical DHCP relay agent application.

Figure 3-1 Typical DHCP relay agent application



In the process of dynamic IP address assignment through the DHCP relay agent, the DHCP client and DHCP server interoperate with each other in a similar way as they do without the DHCP relay agent. The following sections only describe the forwarding process of the DHCP relay agent. For the interaction process of the packets, see section [Obtaining IP Addresses Dynamically](#).

- 1) After receiving the DHCP-DISCOVER or DHCP-REQUEST broadcast from the client, the network device providing the DHCP relay agent function unicasts the message to the designated DHCP server based on the configuration.
- 2) The DHCP server selects an IP address and other parameters and sends the configuration information to the DHCP relay agent that relays the information to the client (the sending mode is decided by the flag filed in the client's DHCP-DISCOVER packet, refer to section [DHCP Packet Format](#) for details).

Option 82 Support on DHCP Relay Agent

Introduction to Option 82

Option 82 is the relay agent information option in the DHCP message. It records the location information of the DHCP client. With this option, the administrator can locate the DHCP client to further implement security control and accounting. The Option 82 supporting server can also use such information to define individual assignment policies of IP address and other parameters for the clients.

Option 82 involves at most 255 sub-options. If Option 82 is defined, at least one sub-option must be defined. Currently the DHCP relay agent supports two sub-options: sub-option 1 (circuit ID sub-option) and sub-option 2 (remote ID sub-option).

Padding content of Option 82

Option 82 has no unified definition in RFC 3046. Its padding information varies with vendors. Currently, S3600 Series Ethernet Switches that operate as DHCP relay agents support the extended padding format of Option 82 sub-options. By default, the sub-options of Option 82 are padded as follows, as shown in [Figure 3-2](#) and [Figure 3-3](#). (The content in brackets is the fixed value of each field.)

- sub-option 1: Padded with the port index (smaller than the physical port number by 1) and VLAN ID of the port that received the client's request.
- sub-option 2: Padded with the bridge MAC address of the DHCP relay agent device that received the client's request.

Figure 3-2 Padding contents for sub-option 1 of Option 82

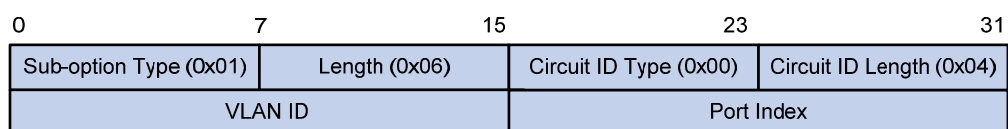
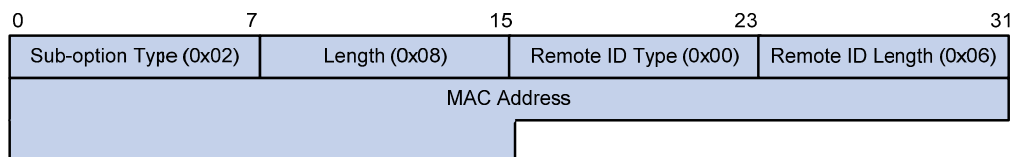


Figure 3-3 Padding contents for sub-option 2 of Option 82



Mechanism of Option 82 supported on DHCP relay agent

The procedure for a DHCP client to obtain an IP address from a DHCP server through a DHCP relay agent 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 support on DHCP relay agent.

- 1) Upon receiving a DHCP request, the DHCP relay agent checks whether the packet contains Option 82 and processes the packet accordingly.
 - If the request packet contains Option 82, the DHCP relay agent 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.
 - If the request packet does not contain Option 82, the DHCP relay agent adds Option 82 to the packet and forwards the packet to the DHCP server.
- 2) Upon receiving the packet returned from the DHCP server, the DHCP relay agent 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 agent adds Option 82 to both types of packets to accommodate to DHCP servers of different manufacturers.

DHCP Inform Message Handling Feature Used in IRF System

Some DHCP clients, after obtaining IP addresses, send DHCP Inform messages to the DHCP server to request other configuration parameters (such as DNS server and default gateway addresses).

If an S3600 series switch belongs to a fabric, you need to enable UDP Helper and then DHCP relay agent on it. Then, upon receiving a DHCP Inform message from a DHCP client, the switch will replace

the XID (Transaction ID, a random value selected by the client to uniquely identify an address allocation process) in the message, and then forward the message to the DHCP server.

After receiving the message, the DHCP server returns a DHCP-ACK message to the client:

- If the DHCP-ACK message is unicast, the DHCP relay agent directly forwards the message to the client without replacing the XID in the message.
- If the DHCP-ACK message is broadcast, the DHCP relay agent delivers the message to the CPU to replace the XID, and then forwards the message to the client.

A DHCP client can only handle a DHCP-ACK message which has the same XID as that in the DHCP Inform message sent by the client. Therefore, to ensure clients to obtain configuration parameters successfully, S3600 series Ethernet switches support the DHCP Inform message handling feature. With this feature enabled, an S3600 series switch that functions as a DHCP relay agent in a fabric can replace the XID in DHCP Inform messages before forwarding them to the DHCP server. If this feature is disabled, the switch does not replace the XID.

Configuring the DHCP Relay Agent



Note

- If a switch belongs to an IRF fabric, you need to enable the UDP Helper function on it before configuring it as a DHCP relay agent.
- If an S3600 Ethernet switch is configured with DHCP Relay Agent, the clients connected to it cannot dynamically obtain IP addresses through BOOTP.

DHCP Relay Agent Configuration Task List

Complete the following tasks to configure the DHCP relay agent:

Task	Remarks
Enabling DHCP	Required
Correlating a DHCP Server Group with a Relay Agent Interface	Required
Configuring DHCP Relay Agent Security Functions	Optional
Configuring the DHCP Relay Agent to Support Option 82	Optional
Configuring DHCP Inform Message Handling Feature Used in IRF System	Optional

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.

Follow these steps to enable DHCP:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable DHCP	dhcp enable	Required Enabled by default.

Note that: Among S3600 series switches, only S3600-EI switches support this command. DHCP is always enabled on S3600-SI series switches.

Correlating a DHCP Server Group with a Relay Agent Interface

To enhance reliability, you can set multiple DHCP servers on the same network. These DHCP servers form a DHCP server group. When an interface of the relay agent establishes a correlation with the DHCP server group, the interface will forward received DHCP packets to all servers in the server group.

Follow these steps to correlate a DHCP server group with a relay agent interface:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the DHCP server IP address(es) in a specified DHCP server group	dhcp-server group <i>No ip ip-address&<1-8></i>	Required By default, no DHCP server IP address is configured in a DHCP server group.
Map an interface to a DHCP server group	interface <i>interface-type interface-number</i>	Required By default, a VLAN interface is not mapped to any DHCP server group.
	dhcp-server group <i>No</i>	



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 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.

Configuring DHCP Relay Agent Security Functions

Configuring address checking



Note

Among S3600 series switches, only S3600-EI series switches support the DHCP relay agent address checking function.

After relaying an IP address from the DHCP server to a DHCP client, the DHCP relay agent can automatically record the client's IP-to-MAC binding and generate a dynamic address entry. It also supports static bindings, which means you can manually configure IP-to-MAC bindings on the DHCP relay agent, so that users can access external network using fixed IP addresses.

The purpose of the address checking function on DHCP relay agent is to prevent unauthorized users from statically configuring IP addresses to access external networks. With this function enabled, a DHCP relay agent 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 agent and the manually configured static entries) in the user address table on the DHCP relay agent.

Follow these steps to configure address checking:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a static IP-to-MAC binding	dhcp-security static <i>ip-address mac-address</i>	Optional Not created by default. (Only S3600-EI series switches among S3600 series switches support this configuration.)
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	—

To do...	Use the command...	Remarks
Enable the address checking function	address-check enable	Required Disabled by default. (Only S3600-EI series switches among S3600 series switches support this configuration.)



Note

- The **address-check enable** command is independent of other commands of the DHCP relay agent. That is, the invalid address check takes effect when this command is executed, regardless of whether other commands (such as the command to enable DHCP) are used.
- Before executing the **address-check enable** command on the interface connected to the DHCP server, you need to configure the static binding of the IP address to the MAC address of the DHCP server. Otherwise, the DHCP client will fail to obtain an IP address.

Configuring the dynamic client address entry updating function



Note

Among S3600 series switches, only S3600-EI series switches support the DHCP relay agent handshake and dynamic client address entry updating functions.

After relaying an IP address from the DHCP server to the DHCP client, the DHCP relay agent can automatically record the client's IP-to-MAC binding and generate a dynamic address entry. But as a DHCP relay agent 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. You can solve this problem by enabling the DHCP relay agent handshake function and configuring the dynamic client address entry updating interval.

After the handshake function is enabled, the DHCP relay agent sends the handshake packet (the DHCP-REQUEST packet) periodically to the DHCP server using a client's IP address and its own MAC address.

- If the DHCP relay agent receives the DHCP-ACK packet from the DHCP server, or receives no response from the server within a specified period, the IP address can be assigned. The DHCP relay agent ages out the corresponding entry in the client address table.
- If the DHCP relay agent receives the DHCP-NAK packet from the DHCP server, the lease of the IP address does not expire. The DHCP relay agent does not age out the corresponding entry.

Follow these steps to configure the dynamic user address entry updating function:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
Enable the DHCP relay agent handshake function	dhcp relay hand enable	Optional Enabled by default. (Only S3600-EI series switches among S3600 series switches support this configuration.)
Set the interval at which the DHCP relay agent dynamically updates the client address entries	dhcp-security tracker { <i>interval</i> auto }	Optional By default, auto is adopted, that is, the interval is automatically calculated. (Only S3600-EI series switches among S3600 series switches support this configuration.)



Note

Currently, the DHCP relay agent handshake function on a S3600-EI series switch can only interoperate with a Windows 2000 DHCP server.

Enabling unauthorized DHCP server detection

If there is an unauthorized DHCP server in the network, when a client applies for an IP address, the unauthorized DHCP server may assign an incorrect IP address to the DHCP client.

With this feature enabled, upon receiving a DHCP message with the siaddr field (IP addresses of the servers offering IP addresses to the client) not being 0 from a client, the DHCP relay agent will record the value of the siaddr field and the receiving interface. The administrator can use this information to check out any DHCP unauthorized servers.

Follow these steps to enable unauthorized DHCP server detection:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable unauthorized DHCP server detection	dhcp-server detect	Required Disabled by default.



Note

With the unauthorized DHCP server detection enabled, the relay agent will log all DHCP servers, including authorized ones, and each server is recorded only once until such information is removed and is recorded again. The administrator needs to find unauthorized DHCP servers from the system log information.

Configuring the DHCP Relay Agent to Support Option 82

Prerequisites

Before configuring Option 82 support on a DHCP relay agent, 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 agent and the DHCP server are reachable.

Enabling Option 82 support on a DHCP relay agent

Follow these steps to enable Option 82 support on a DHCP relay agent:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable Option 82 support on the DHCP relay agent	dhcp relay information enable	Required Disabled by default.
Configure the strategy for the DHCP relay agent 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 support function enabled on the DHCP relay agent, the DHCP relay agent will adopt the replace strategy to process the request packets containing Option 82. However, if other strategies are configured before, then enabling the 82 support on the DHCP relay agent 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 agent.

Configuring DHCP Inform Message Handling Feature Used in IRF System

Follow these steps to enable the DHCP relay agent to replace the XID in DHCP Inform messages:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable UDP Helper	udp-helper enable	Required Disabled by default.
Enable the DHCP relay agent to replace the XID in DHCP Inform messages	dhcp relay inform replace enable	Optional Enabled by default.



Note

Before enabling the DHCP relay agent to replace the XID in DHCP Inform messages, make sure that UDP Helper is enabled on the switch.

Displaying and Maintaining DHCP Relay Agent Configuration

To do...	Use the command...	Remarks
Display the information about a specified DHCP server group	display dhcp-server <i>groupNo</i>	Available 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 <i>vlan-id</i>	
Display the specified client address entries on the DHCP relay agent	display dhcp-security [<i>ip-address</i> dynamic static tracker]	
Clear the statistics information of the specified DHCP server group	reset dhcp-server <i>groupNo</i>	Available in user view



Note

Among S3600 series Ethernet switches, only S3600-EI series switches support the **display dhcp-security** command.

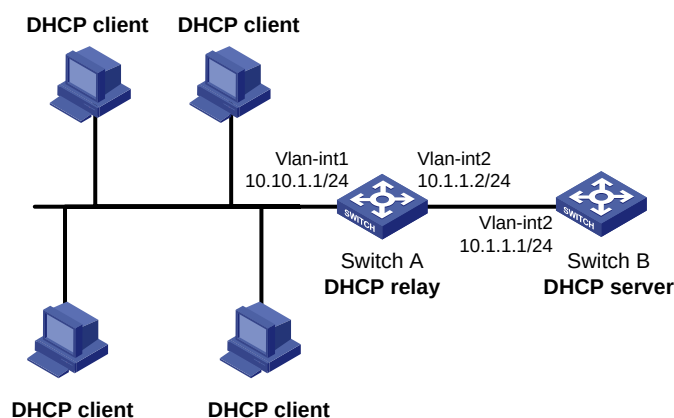
DHCP Relay Agent Configuration Example

Network requirements

VLAN-interface 1 on the DHCP relay agent (Switch A) connects to the network where DHCP clients reside. The IP address of VLAN-interface 1 is 10.10.1.1/24 and IP address of VLAN-interface 2 is 10.1.1.2/24 that communicates with the DHCP server 10.1.1.1/24. As shown in the figure below, Switch A forwards messages between DHCP clients and the DHCP server to assign IP addresses in subnet 10.10.1.0/24 to the clients.

Network diagram

Figure 3-4 Network diagram for DHCP relay agent



Configuration procedure

Create DHCP server group 1 and configure an IP address of 10.1.1.1 for it.

```
<SwitchA> system-view
```

```
[SwitchA] dhcp-server 1 ip 10.1.1.1
```

Map VLAN-interface 1 to DHCP server group 1.

```
[SwitchA] interface Vlan-interface 1
```

```
[SwitchA-Vlan-interface1] dhcp-server 1
```



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.
- The DHCP relay agent and DHCP server must be reachable to each other.

Troubleshooting DHCP Relay Agent Configuration

Symptom

A client fails to obtain configuration information through a DHCP relay agent.

Analysis

This problem may be caused by improper DHCP relay agent configuration. When a DHCP relay agent 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.)

Solution

- Check if DHCP is enabled on the DHCP server and the DHCP relay agent.
- 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 agent and the DHCP server.
- Check the DHCP relay agent. 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.
- If the **address-check enable** command is configured on the interface connected to the DHCP server, verify the DHCP server's IP-to-MAC address binding entry is configured on the DHCP relay agent; otherwise the DHCP client cannot obtain an IP address.

4 DHCP Snooping Configuration

When configuring DHCP snooping, go to these sections for information you are interested in:

- [DHCP Snooping Overview](#)
- [Configuring DHCP Snooping](#)
- [Displaying and Maintaining DHCP Snooping Configuration](#)
- [DHCP Snooping Configuration Examples](#)

DHCP Snooping Overview

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.

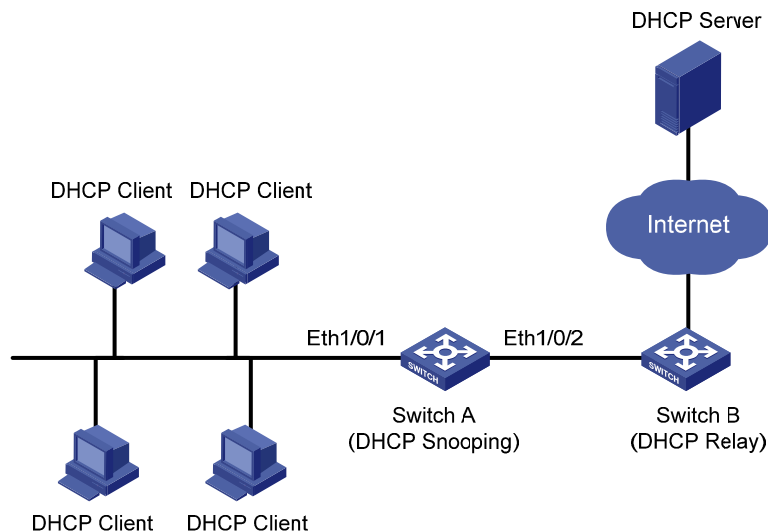
- Switches can track DHCP clients' IP addresses through the security function of the DHCP relay agent operating at the network layer.
- Switches can track DHCP clients' IP addresses through the DHCP snooping function at the data link layer.

When an unauthorized DHCP server exists in the network, a DHCP client may obtain 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: A trusted port is connected to an authorized DHCP server directly or indirectly. It forwards DHCP messages to guarantee that DHCP clients can obtain valid IP addresses.
- Untrusted: An untrusted port is connected to an unauthorized DHCP server. The DHCP-ACK or DHCP-OFFER packets received from the port are discarded, preventing DHCP clients from receiving invalid IP addresses.

[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



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-REQUEST packet
- DHCP-ACK packet

Introduction to DHCP-Snooping Option 82

Introduction to Option 82

For details about Option 82, refer to [Option 82 Support on DHCP Relay Agent](#).

Padding content and frame format of Option 82

There is no specification for what should be padded in Option 82. Manufacturers can pad it as required. By default, the sub-options of Option 82 for S3600 Series Ethernet Switches (enabled with DHCP snooping) are padded as follows:

- sub-option 1 (circuit ID sub-option): Padded with the port index (smaller than the physical port number by 1) and VLAN ID of the port that received the client's request.
- sub-option 2 (remote ID sub-option): Padded with the bridge MAC address of the DHCP snooping device that received the client's request.

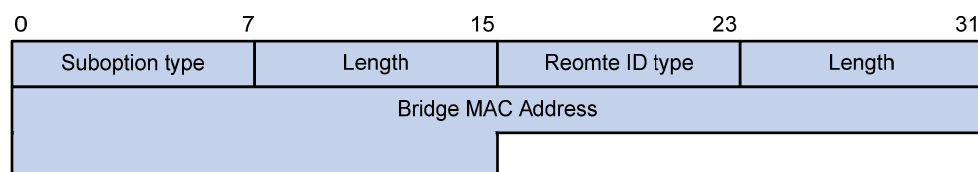
By default, when S3600 Series Ethernet Switches serve as DHCP snooping devices, Option 82 adopts the extended format. Refer to [Figure 4-2](#) and [Figure 4-3](#) for the extended format of the sub-options (with the default padding contents). That is, the circuit ID or remote ID sub-option defines the type and length of a circuit ID or remote ID.

The remote ID type field and circuit ID type field are determined by the option storage format. They are both set to **0** in the case of HEX format and to **1** in the case of ASCII format.

Figure 4-2 Extended format of the circuit ID sub-option

0	7	15	23	31	
Suboption type		Length		Circuit ID type	Length
VLAN ID				Port Index	

Figure 4-3 Extended format of the remote ID sub-option



In practice, some network devices do not support the type and length identifiers of the Circuit ID and Remote ID sub-options. To interwork with these devices, S3600 Series Ethernet Switches support Option 82 in the standard format. Refer to [Figure 4-4](#) and [Figure 4-5](#) for the standard format of the sub-options (with the default padding contents). In the standard format, the Circuit ID or Remote ID sub-option does not contain the two-byte type and length fields of the circuit ID or remote ID.

Figure 4-4 Standard format of the circuit ID sub-option

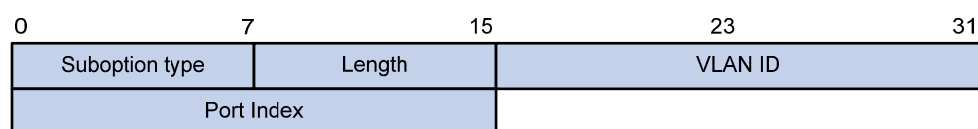
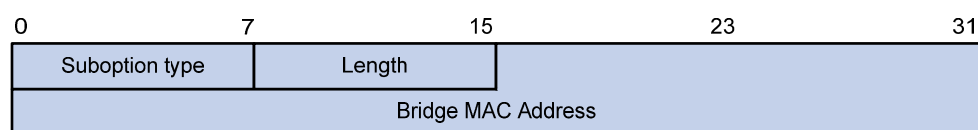


Figure 4-5 Standard format of the remote ID sub-option



Mechanism of DHCP-snooping Option 82

With DHCP snooping and DHCP-snooping Option 82 support enabled, when the DHCP snooping device receives a DHCP client's request containing Option 82, it will handle the packet according to the handling policy and the configured contents in sub-options. For details, see [Table 4-1](#).

Table 4-1 Ways of handling a DHCP packet with Option 82

Handling policy	Sub-option configuration	The DHCP Snooping device will...
Drop	—	Drop the packet.
Keep	—	Forward the packet without changing Option 82.
Replace	Neither of the two sub-options is configured	Forward the packet after replacing the original Option 82 with the default content. The storage format of Option 82 content is the one specified with the dhcp-snooping information format command or the default HEX format if this command is not executed.

Handling policy	Sub-option configuration	The DHCP Snooping device will...
	Circuit ID sub-option is configured	Forward the packet after replacing the circuit ID sub-option of the original Option 82 with the configured circuit ID sub-option in ASCII format.
	Remote ID sub-option is configured	Forward the packet after replacing the remote ID sub-option of the original Option 82 with the configured remote ID sub-option in ASCII format.

When receiving a DHCP client's request without Option 82, the DHCP snooping device will add the option field with the configured sub-option and then forward the packet. For details, see [Table 4-2](#).

Table 4-2 Ways of handling a DHCP packet without Option 82

Sub-option configuration	The DHCP-Snooping device will ...
Neither of the two sub-options is configured.	Forward the packet after adding Option 82 with the default contents. The format of Option 82 is the one specified with the dhcp-snooping information format command or the default HEX format if this command is not executed.
Circuit ID sub-option is configured.	Forward the packet after adding Option 82 with the configured circuit ID sub-option in ASCII format.
Remote ID sub-option is configured.	Forward the packet after adding Option 82 with the configured remote ID sub-option in ASCII format.



Note

The circuit ID and remote ID sub-options in Option 82, which can be configured simultaneously or separately, are independent of each other in terms of configuration sequence.

When the DHCP snooping device receives a DHCP response packet from the DHCP server, the DHCP snooping device will delete the Option 82 field, if contained, before forwarding the packet, or will directly forward the packet if the packet does not contain the Option 82 field.

Introduction to IP Filtering

A denial-of-service (DoS) attack means an attempt of an attacker sending a large number of forged address requests with different source IP addresses to the server so that the network cannot work normally. The specific effects are as follows:

- The resources on the server are exhausted, so the server does not respond to other requests.

- After receiving such type of packets, a switch needs to send them to the CPU for processing. Too many request packets cause high CPU usage rate. As a result, the CPU cannot work normally.

The switch can filter invalid IP packets through the DHCP-snooping table and , IP static binding table, or IP-to-MAC mappings of authenticated 802.1x clients.

DHCP-snooping table

After DHCP snooping is enabled on a switch, a DHCP-snooping table is generated. It is used to record IP addresses obtained from the DHCP server, MAC addresses, the number of the port through which a client is connected to the DHCP-snooping-enabled device, and the number of the VLAN to which the port belongs to. These records are saved as entries in the DHCP-snooping table.

IP static binding table

The DHCP-snooping table only records information about clients that obtains IP address dynamically through DHCP. If a fixed IP address is configured for a client, the IP address and MAC address of the client cannot be recorded in the DHCP-snooping table. Consequently, this client cannot pass the IP filtering of the DHCP-snooping table, thus it cannot access external networks.

To solve this problem, the switch supports the configuration of static binding table entries, that is, the binding relationship between IP address, MAC address, and the port connecting to the client, so that packets of the client can be correctly forwarded.

IP-to-MAC mappings of authenticated 802.1x clients

If most clients are assigned with static IP addresses, you need to configure an IP static binding for each client. The configuration is a heavy workload and causes errors easily.

To ensure security, in actual networks, clients are usually connected to networks through 802.1x authentication. With the authenticated 802.1x client-based IP filtering function enabled, the switch can record and query the IP-to-MAC mappings of authenticated 802.1x clients to defend against IP attacks.

IP filtering

IP filtering can be implemented based on the DHCP-snooping table, IP static binding table, or IP-to-MAC mappings of authenticated 802.1x clients, according to actual network requirements. The switch can filter IP packets in the following modes:

- Filtering packets based on their source IP addresses. If the source IP address in a packet and the number of the port that receives the packet match an entry or mapping, the switch regards the packet as a valid packet and forwards it; otherwise, the switch drops it directly.
- Filtering packets based on their source IP and MAC addresses. If the source IP address and source MAC address in the packet, and the number of the port that receives the packet match an entry or mapping, the switch regards the packet as a valid packet and forwards it; otherwise, the switch drops it directly.
- Filtering packets based on their source IP and MAC addresses, and traffic limit defined in a QoS profile. You can associate IP filtering with the traffic limit function on the switch for security filtering and precise packet limit.

Configuring DHCP Snooping

Configuring DHCP Snooping

Follow these steps to configure DHCP snooping:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable DHCP snooping	dhcp-snooping	Required By default, the DHCP snooping function is disabled.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Specify the current port as a trusted port	dhcp-snooping trust	Required By default, after DHCP snooping is enabled, all ports of a switch are untrusted ports.



Note

- If an S3600 Ethernet switch is enabled with DHCP snooping, the clients connected to it cannot dynamically obtain IP addresses through BOOTP.
- You need to specify the ports connected to the valid DHCP servers as trusted to ensure that DHCP clients can obtain valid IP addresses. The trusted port and the port connected to the DHCP client must be in the same VLAN.
- To enable DHCP snooping on an S3600 switch that belongs to an IRF fabric, do not configure the ports connecting to the DHCP clients and DHCP server to belong to different units of the fabric; otherwise, the switch cannot record DHCP snooping entries although the clients can obtain IP addresses.
- You are not recommended to configure both the DHCP snooping and selective Q-in-Q function on the switch, which may result in the DHCP snooping to function abnormally.

Configuring DHCP Snooping to Support Option 82



Note

Enable DHCP snooping and specify trusted ports on the switch before configuring DHCP snooping to support Option 82.

Complete the following tasks to configure the DHCP snooping to support Option 82:

Task	Remarks
Enabling DHCP-snooping Option 82 support	Required
Configuring a handling policy for DHCP packets with Option 82	Optional
Configuring the storage format of Option 82	Optional
Configuring the circuit ID sub-option	Optional

Task	Remarks
Configuring the remote ID sub-option	Optional
Configuring the padding format for Option 82	Optional

Enabling DHCP-snooping Option 82 support

Follow these steps to enable DHCP-snooping Option 82 support:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable DHCP-snooping Option 82 support	dhcp-snooping information enable	Required Disabled by default.

Configuring a handling policy for DHCP packets with Option 82

Follow these steps to configure a handling policy for DHCP packets with Option 82:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a global handling policy for requests that contain Option 82	dhcp-snooping information strategy { drop keep replace }	Optional The default handling policy is replace .
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure a handling policy for requests that contain Option 82 received on the specified interface	dhcp-snooping information strategy { drop keep replace }	Optional The default policy is replace .



Note

If a handling policy is configured on a port, this configuration overrides the globally configured handling policy for requests received on this port, while the globally configured handling policy applies on those ports where a handling policy is not natively configured.

Configuring the storage format of Option 82

S3600 Series Ethernet Switches support the HEX or ASCII format for the Option 82 field.

Follow these steps to configure a storage format for the Option 82 field:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a storage format for the Option 82 field	dhcp-snooping information format { hex ascii }	Optional By default, the format is hex .



Note

The **dhcp-snooping information format** command applies only to the default content of the Option 82 field. If you have configured the circuit ID or remote ID sub-option, the format of the sub-option is ASCII, instead of the one specified with the **dhcp-snooping information format** command.

Configuring the circuit ID sub-option

Follow these steps to configure the circuit ID sub-option:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the circuit ID sub-option in Option 82	dhcp-snooping information [vlan <i>vlan-id</i>] circuit-id <i>string</i>	Optional By default, the circuit ID sub-option contains the VLAN ID and port index related to the port that receives DHCP request packets from DHCP clients



Note

- If you have configured a circuit ID with the **vlan** *vlan-id* argument specified, and the other one without the argument in Ethernet port view, the former circuit ID applies to the DHCP messages from the specified VLAN; while the latter one applies to DHCP messages from other VLANs.
- In a port aggregation group, you can use this command to configure the primary and member ports respectively. When Option 82 is added, however, the circuit ID sub-option is subject to the one configured on the primary port.
- The circuit ID sub-option configured on a port will neither be synchronized in the case of port aggregation nor support IRF .

Configuring the remote ID sub-option

You can configure the remote ID sub-option in system view or Ethernet port view:

- In system view, the remote ID takes effect on all interfaces. You can configure Option 82 as the system name (sysname) of the device or any customized character string in the ASCII format.
- In Ethernet port view, the remote ID takes effect only on the current interface. You can configure Option 82 as any customized character string in the ASCII format for different VLANs. That is to say, you can add different configuration rules for packets from different VLANs.

Follow these steps to configure the remote ID sub-option in Option 82:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the remote ID sub-option in system view	dhcp-snooping information remote-id { sysname string string }	Optional By default, the remote ID sub-option is the MAC address of the DHCP snooping device that received the DHCP client's request.
Enter Ethernet port view	interface <i>interface-type interface-number</i>	—
Configure the remote ID sub-option in Ethernet port view	dhcp-snooping information [vlan <i>vlan-id</i>] remote-id string string	Optional By default, the remote ID sub-option is the MAC address of the DHCP snooping device that received the client's request.



Note

- If you configure a remote ID sub-option in both system view and on a port, the remote ID sub-option configured on the port applies when the port receives a packet, and the global remote ID applies to other interfaces that have no remote ID sub-option configured.
- If you have configured a remote ID with the **vlan *vlan-id*** argument specified, and the other one without the argument in Ethernet port view, the former remote ID applies to the DHCP messages from the specified VLAN, while the latter one applies to DHCP messages from other VLANs.
- In a port aggregation group, you can use this command to configure the primary and member ports respectively. When Option 82 is added, however, the remote ID is subject to the one configured on the primary port.
- The remote ID configured on a port will neither be synchronized in the case of port aggregation nor support IRF.

Configuring the padding format for Option 82

Follow these steps to configure the padding format for Option 82:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the padding format	dhcp-snooping information packet-format { extended standard }	Optional By default, the padding format is in extended format.

Configuring IP Filtering

Follow these steps to configure IP filtering:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enter Ethernet port view		interface <i>interface-type</i> <i>interface-number</i>	—
Create a static binding		ip source static binding ip-address <i>ip-address</i> [mac-address <i>mac-address</i>]	Optional By default, no IP static binding entry is created.
Enable IP filtering	Enable IP filtering based on the DHCP-snooping table and the IP static binding table	ip check source ip-address [mac-address] [qos-profile <i>string</i>]	Either command is required By default, this function is disabled.
	Enable IP filtering based on authenticated 802.1x clients	ip check dot1x enable	



Note

- For details about 802.1x authentication, refer to *802.1x and System Guard Operation*.
- You are not recommended to configure IP filtering on the ports of an aggregation group.
- Enable DHCP snooping and specify trusted ports on the switch before configuring IP filtering based on the DHCP-snooping table.
- To implement IP filtering based on IP-to-MAC bindings of authenticated 802.1x clients, the device assigns an ACL to each of such bindings. If an ACL fails to be assigned to a binding, the corresponding authenticated 802.1x client is forced to go offline.
- IP filtering based on IP-to-MAC bindings of authenticated 802.1x clients requires to be associated with 802.1x based on MAC address authentication, and requires 802.1x clients to provide IP addresses; otherwise, the IP addresses of 802.1x clients cannot be obtained. To ensure IP addresses of DHCP clients can be updated for corresponding IP-to-MAC entries, you are recommended to enable 802.1x authentication handshake function; otherwise, you need to disable 802.1x authentication triggered by DHCP, ensuring normal receiving and forwarding of multicast authentication packets.
- To create a static binding after IP filtering is enabled with the **mac-address** keyword specified on a port, the *mac-address* argument must be specified; otherwise, the packets sent from this IP address cannot pass the IP filtering.
- A static entry has a higher priority than the dynamic DHCP snooping entry that has the same IP address as the static one. That is, if the static entry is configured after the dynamic entry is recorded, the static entry overwrites the dynamic entry; if the static entry is configured before DHCP snooping is enabled, no DHCP client can obtain the IP address of the static entry, that is, the dynamic DHCP snooping entry cannot be generated.
- The VLAN ID of the IP static binding configured on a port is the VLAN ID of the port.

Displaying and Maintaining DHCP Snooping Configuration

To do...	Use the command...	Remarks
Display the user IP-to-MAC address mapping entries recorded by the DHCP snooping function	display dhcp-snooping [<i>unit unit-id</i>]	Available in any view
Display the (enabled/disabled) state of the DHCP snooping function and the trusted ports	display dhcp-snooping trust	
Display the IP static binding table	display ip source static binding [<i>vlan vlan-id</i> interface <i>interface-type interface-number</i>]	
Remove DHCP snooping entries	reset dhcp-snooping [<i>ip-address</i>]	Available in user view

DHCP Snooping Configuration Examples

DHCP-Snooping Option 82 Support Configuration Example

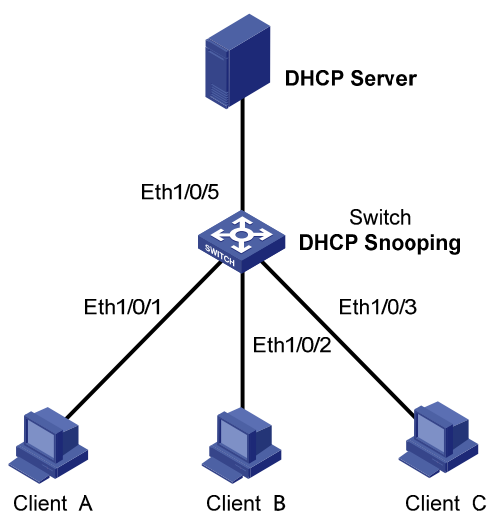
Network requirements

As shown in [Figure 4-6](#), Ethernet 1/0/5 of the switch is connected to the DHCP server, and Ethernet 1/0/1, Ethernet 1/0/2, and Ethernet 1/0/3 are respectively connected to Client A, Client B, and Client C.

- Enable DHCP snooping on the switch.
- Specify Ethernet 1/0/5 on the switch as a trusted port for DHCP snooping.
- Enable DHCP-snooping Option 82 support on the switch and set the remote ID field in Option 82 to the system name of the switch. Set the circuit ID sub-option to **abcd** in DHCP packets from VLAN 1 on Ethernet 1/0/3.

Network diagram

Figure 4-6 Network diagram for DHCP-snooping Option 82 support configuration



Configuration procedure

Enable DHCP snooping on the switch.

```
<Switch> system-view
```

```
[Switch] dhcp-snooping
```

Specify Ethernet 1/0/5 as the trusted port.

```
[Switch] interface ethernet 1/0/5
```

```
[Switch-Ethernet1/0/5] dhcp-snooping trust
```

```
[Switch-Ethernet1/0/5] quit
```

Enable DHCP-snooping Option 82 support.

```
[Switch] dhcp-snooping information enable
```

Set the remote ID sub-option in Option 82 to the system name (sysname) of the DHCP snooping device.

```
[Switch] dhcp-snooping information remote-id sysname
```

Set the circuit ID sub-option in DHCP packets from VLAN 1 to **abcd** on Ethernet 1/0/3.

```
[Switch] interface ethernet 1/0/3
```

```
[Switch-Ethernet1/0/3] dhcp-snooping information vlan 1 circuit-id string abcd
```

IP Filtering Configuration Example

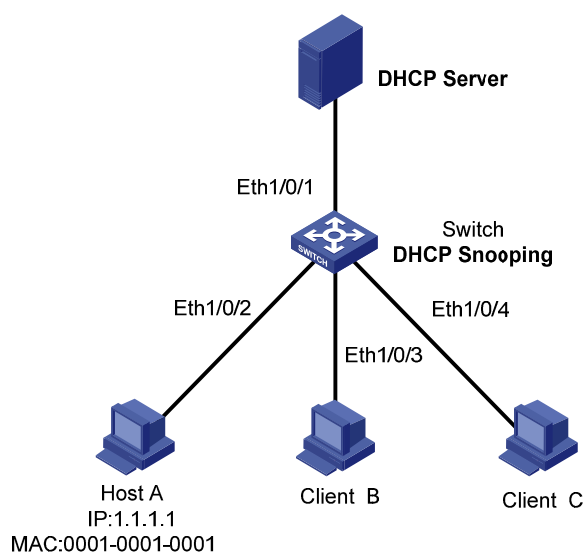
Network requirements

As shown in [Figure 4-7](#), Ethernet 1/0/1 of the S3600 switch is connected to the DHCP server and Ethernet 1/0/2 is connected to Host A. The IP address and MAC address of Host A are 1.1.1.1 and 0001-0001-0001 respectively. Ethernet 1/0/3 and Ethernet 1/0/4 are connected to DHCP Client B and Client C.

- Enable DHCP snooping on the switch, and specify Ethernet 1/0/1 as the DHCP snooping trusted port.
- Enable IP filtering on Ethernet 1/0/2, Ethernet 1/0/3, and Ethernet 1/0/4 to prevent attacks to the server from clients using fake source IP addresses.
- Create static binding entries on the switch, so that Host A using a fixed IP address can access external networks.

Network diagram

Figure 4-7 Network diagram for IP filtering configuration



Configuration procedure

Enable DHCP snooping on the switch.

```
<Switch> system-view
[Switch] dhcp-snooping
```

Specify Ethernet 1/0/1 as the trusted port.

```
[Switch] interface ethernet 1/0/1
[Switch-Ethernet1/0/1] dhcp-snooping trust
[Switch-Ethernet1/0/1] quit
```

Enable IP filtering on Ethernet 1/0/2, Ethernet 1/0/3, and Ethernet 1/0/4 to filter packets based on the source IP addresses/MAC addresses.

```
[Switch] interface ethernet 1/0/2
[Switch-Ethernet1/0/2] ip check source ip-address mac-address
[Switch-Ethernet1/0/2] quit
[Switch] interface ethernet 1/0/3
[Switch-Ethernet1/0/3] ip check source ip-address mac-address
[Switch-Ethernet1/0/3] quit
[Switch] interface ethernet 1/0/4
[Switch-Ethernet1/0/4] ip check source ip-address mac-address
[Switch-Ethernet1/0/4] quit
```

Create static binding entries on Ethernet 1/0/2 of the switch.

```
[Switch] interface ethernet 1/0/2
[Switch-Ethernet1/0/2] ip source static binding ip-address 1.1.1.1 mac-address
0001-0001-0001
```

QoS Profile and IP Filtering Association Configuration Example

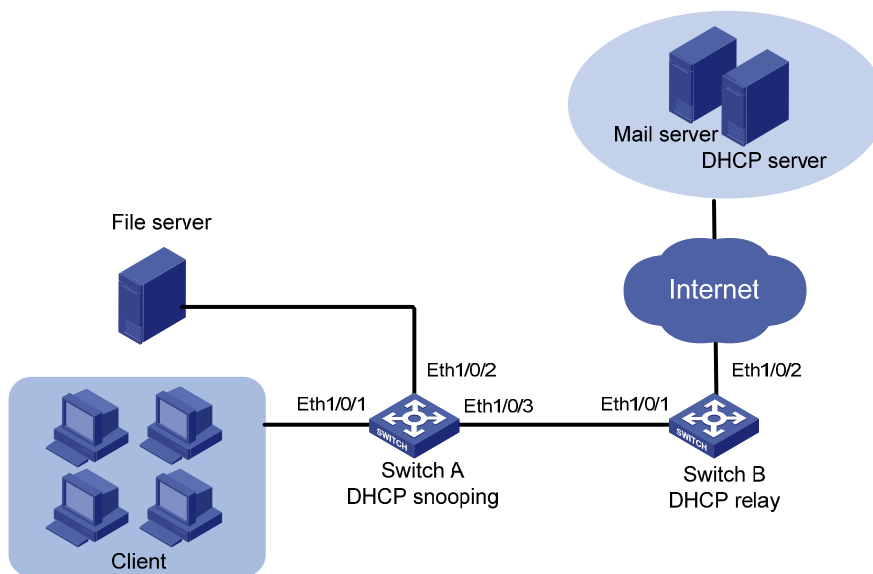
Network requirements

As shown in the following figure, the clients access the internal file server through Switch A, and access the DHCP server and mail server through a DHCP relay agent. It is required that:

- The clients obtain IP addresses on the network segment 192.168.0.0/24 from the DHCP server.
- Enable DHCP snooping on Switch A, and configure Ethernet 1/0/3 as a trusted port. Enable IP filtering on Ethernet 1/0/1 to prevent IP packet attacks from clients.
- Configure a QoS profile on Switch A, limiting the rate at which the clients send packets to the internal network (such as the file server with IP address 192.168.0.1/24) to 4 Mbps, and that to external networks to 2 Mbps. Exceeding packets will be discarded.

Network diagram

Figure 4-8 Network diagram for QoS profile and IP filtering association



Configuration procedure

Define ACL 3000 on Switch A, permitting packets destined for network segment 192.168.0.0/24 to pass.

```
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule 1 permit ip destination 192.168.0.0 0.0.0.255
[SwitchA-acl-adv-3000] quit
```

Define ACL 3001 on Switch A, permitting packets with any destination IP address to pass.

```
[SwitchA] acl number 3001
[SwitchA-acl-adv-3001] rule 1 permit ip destination any
[SwitchA-acl-adv-3001] quit
```

Define a QoS profile named **example**. Configure the internal packet rate as 4096 Kbps, and external packet rate as 2048 Kbps. Exceeding packets are discarded.

```
[SwitchA] qos-profile example
[SwitchA-qos-profile-example] traffic-limit inbound ip-group 3000 4096 exceed drop
[SwitchA-qos-profile-example] traffic-limit inbound ip-group 3001 2048 exceed drop
```

```
[SwitchA-qos-profile-example] quit
```

Enable DHCP snooping on Switch A, and configure Ethernet 1/0/3 as a trusted port.

```
[SwitchA] dhcp-snooping
```

```
[SwitchA] interface ethernet 1/0/3
```

```
[SwitchA-Ethernet1/0/3] dhcp-snooping trust
```

```
[SwitchA-Ethernet1/0/3] quit
```

Associate IP filtering with QoS profile on Ethernet 1/0/1 of Switch A.

```
[SwitchA] interface ethernet 1/0/1
```

```
[SwitchA-Ethernet1/0/1] ip check source ip-address qos-profile example
```

```
[SwitchA-Ethernet1/0/1] quit
```

5 DHCP Packet Rate Limit Configuration

When configuring the DHCP packet rate limit function, go to these sections for information you are interested in:

- [Introduction to DHCP Packet Rate Limit](#)
- [Configuring DHCP Packet Rate Limit](#)
- [Rate Limit Configuration Example](#)

Introduction to DHCP Packet Rate Limit

To prevent ARP attacks and attacks from unauthorized DHCP servers, ARP packets and DHCP packets will be processed by the switch CPU for validity checking. But, if attackers generate a large number of ARP packets or DHCP packets, the switch CPU will be under extremely heavy load. As a result, the switch cannot work normally and even goes down.

S3600 series Ethernet switches support ARP and DHCP packet rate limit on a port and shut down the port under attack to prevent hazardous impact on the device CPU. For details about ARP packet rate limit, refer to *ARP Operation* in this manual. The following describes only the DHCP packet rate limit function.

After DHCP packet rate limit is enabled on an Ethernet port, the switch counts the number of DHCP packets received on this port per second. If the number of DHCP packets received per second exceeds the specified value, packets are passing the port at an over-high rate, which implies an attack to the port. In this case, the switch shuts down this port so that it cannot receive any packet, thus protect the switch from attacks.

In addition, the switch supports port state auto-recovery. After a port is shut down due to over-high packet rate, it resumes automatically after a configurable period of time.



Note

When both port state auto-recovery interval for over-high ARP packet rate and port state auto-recovery interval for over-high DHCP packet rate are configured on a port, the shorter one will be the auto-recovery time.

Configuring DHCP Packet Rate Limit

Configuring DHCP Packet Rate Limit

Follow these steps to configure rate limit of DHCP packets:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
Enter port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the DHCP packet rate limit function	dhcp rate-limit enable	Required By default, DHCP packet rate limit is disabled.
Configure the maximum DHCP packet rate allowed on the port	dhcp rate-limit rate	Optional By default, the maximum rate is 15 pps.
Enable the port state auto-recovery function	dhcp protective-down recover enable	Optional By default, the port state auto-recovery function is disabled.
Set the port state auto-recovery interval	dhcp protective-down recover interval <i>interval</i>	Optional The port state auto-recovery interval is 300 seconds.



Note

- Enable the port state auto-recovery function before setting the auto-recovery interval.
- You are not recommended to configure DHCP packet rate limit on the ports of an aggregation group.

Rate Limit Configuration Example

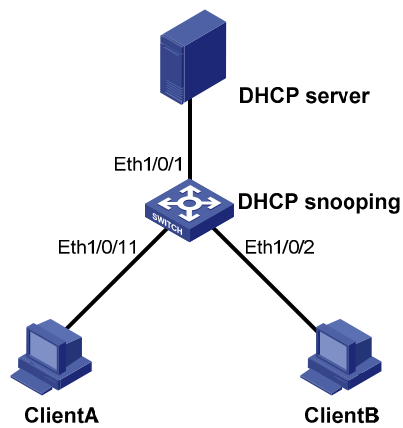
Network requirements

As shown in [Figure 5-1](#), Ethernet 1/0/1 of the S3600 switch is connected to the DHCP server. Ethernet 1/0/2 is connected to client B and Ethernet 1/0/11 is connected to client A.

- Enable DHCP snooping on the switch, and specify Ethernet 1/0/1 as the DHCP snooping trusted port.
- Configure DHCP packet rate limit on Ethernet 1/0/11 and set the maximum DHCP packet rate allowed on the port to 100 pps.
- Set the port state auto-recovery interval to 30 seconds on the switch.

Networking diagram

Figure 5-1 Network diagram for DHCP packet rate limit configuration



Configuration procedure

Enable DHCP snooping on the switch.

```
<Switch> system-view
[Switch] dhcp-snooping
```

Specify Ethernet 1/0/1 as the trusted port.

```
[Switch] interface ethernet 1/0/1
[Switch-Ethernet1/0/1] dhcp-snooping trust
[Switch-Ethernet1/0/1] quit
```

Enable auto recovery.

```
[Sysname] dhcp protective-down recover enable
```

Set the port state auto-recovery interval to 30 seconds.

```
[Sysname] dhcp protective-down recover interval 30
```

Enter port view.

```
[Sysname] interface ethernet 1/0/11
```

Enable DHCP packet rate limit on Ethernet 1/0/11.

```
[Sysname-Ethernet1/0/11] dhcp rate-limit enable
```

Set the maximum DHCP packet rate allowed on Ethernet 1/0/11 to 100 pps.

```
[Sysname-Ethernet1/0/11] dhcp rate-limit 100
```

6 DHCP/BOOTP Client Configuration

When configuring the DHCP/BOOTP client, go to these sections for information you are interested in:

- [Introduction to DHCP Client](#)
- [Introduction to BOOTP Client](#)
- [Configuring a DHCP/BOOTP Client](#)
- [Displaying DHCP/BOOTP Client Configuration](#)

Introduction to DHCP Client

After you specify a VLAN interface as a DHCP client, the device can use DHCP to obtain parameters such as IP address dynamically from the DHCP server, which facilitates user configuration and management.

Refer to [Obtaining IP Addresses Dynamically](#) for the process of how a DHCP client dynamically obtains an IP address through DHCP.

For S3600 series Ethernet switches (operating as DHCP clients), the vendor and device information contained in Option 60 of DHCP requests is not configurable; instead, it is populated by the application program of the switches in the format of *vendor-name. vendor-name device-model*.

Introduction to BOOTP Client

After you specify an interface as a Bootstrap Protocol (BOOTP) client, the interface can use BOOTP to get information (such as IP address) from the BOOTP server, which simplifies your configuration.

Before using BOOTP, an administrator needs to configure a BOOTP parameter file for each BOOTP client on the BOOTP server. The parameter file contains information such as MAC address and IP address of a BOOTP client. When a BOOTP client sends a request to the BOOTP server, the BOOTP server will search for the BOOTP parameter file and return it to the client.

A BOOTP client dynamically obtains an IP address from a BOOTP server in the following way:

- 1) The BOOTP client broadcasts a BOOTP request, which contains its own MAC address.
- 2) The BOOTP server receives the request and searches for the corresponding IP address according to the MAC address of the BOOTP client and sends the information in a BOOTP response to the BOOTP client.
- 3) The BOOTP client obtains the IP address from the received response.



Note

Because a DHCP server can interact with a BOOTP client, you can use the DHCP server to assign an IP address to the BOOTP client, without needing to configure any BOOTP server.

Configuring a DHCP/BOOTP Client

Follow these steps to configure a DHCP/BOOTP client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface vlan-interface <i>vlan-id</i>	—
Configure the VLAN interface to obtain IP address through DHCP or BOOTP	ip address { bootp-alloc dhcp-alloc }	Required By default, no IP address is configured for the VLAN interface.



Note

- Currently, an S3600 Ethernet switch functioning as the DHCP client can use an IP address for 24 days at most. That is, the DHCP client can obtain an address lease for no more than 24 days even though the DHCP server offers a longer lease period.
- If a switch belongs to an IRF fabric, you need to enable the UDP Helper function on the switch before configuring its VLAN interfaces to obtain IP addresses through DHCP.



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 specific implementation is:

- Using the **ip address dhcp-alloc** command enables the DHCP client, and UDP port 68.
- Using the **undo ip address dhcp-alloc** command disables the DHCP client, and UDP port 68.

DHCP Client Configuration Example

Network requirements

Using DHCP, VLAN-interface 1 of Switch B is connected to the LAN to obtain an IP address from the DHCP server.

Network diagram

See [Figure 2-1](#).

Configuration procedure

The following describes only the configuration on Switch B serving as a DHCP client.

Configure VLAN-interface 1 to dynamically obtain an IP address by using DHCP.

```

<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ip address dhcp-alloc

```

BOOTP Client Configuration Example

Network requirement

Switch B's port belonging to VLAN1 is connected to the LAN. VLAN-interface 1 obtains an IP address from the DHCP server by using BOOTP.

Network diagram

See [Figure 2-1](#).

Configuration procedure

The following describes only the configuration on Switch B serving as a client.

Configure VLAN-interface 1 to dynamically obtain an IP address from the DHCP server.

```

<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address bootp-alloc

```

Displaying DHCP/BOOTP Client Configuration

To do...	Use the command...	Remarks
Display related information on a DHCP client	display dhcp client [verbose]	Optional Available in any view
Display related information on a BOOTP client	display bootp client [interface Vlan-interface <i>vlan-id</i>]	

Table of Contents

1 ACL Configuration	1-1
ACL Overview	1-1
ACL Matching Order	1-2
Ways to Apply an ACL on a Switch	1-3
Types of ACLs Supported by S3600 Series Ethernet Switches	1-3
ACL Configuration Task List	1-4
Configuring Time Range	1-4
Configuring Basic ACL	1-6
Configuring Advanced ACL	1-7
Configuring Layer 2 ACL	1-8
Configuring User-defined ACL	1-10
Configuring IPv6 ACL	1-11
Applying ACL Rules on Ports	1-14
Applying ACL Rules to Ports in a VLAN	1-15
Displaying and Maintaining ACL Configuration	1-15
Examples for Upper-layer Software Referencing ACLs	1-16
Example for Controlling Telnet Login Users by Source IP	1-16
Example for Controlling Web Login Users by Source IP	1-17
Examples for Applying ACLs to Hardware	1-17
Basic ACL Configuration Example	1-17
Advanced ACL Configuration Example	1-18
Layer 2 ACL Configuration Example	1-19
User-defined ACL Configuration Example	1-20
IPv6 ACL Configuration Example	1-21
Example for Applying an ACL to a VLAN	1-22

1 ACL Configuration

When configuring ACL, go to these sections for information you are interested in:

- [ACL Overview](#)
- [ACL Configuration Task List](#)
- [Displaying and Maintaining ACL Configuration](#)
- [Examples for Upper-layer Software Referencing ACLs](#)
- [Examples for Applying ACLs to Hardware](#)



Note

- The feature of IPv6 ACL is newly added, which is described in [Configuring IPv6 ACL](#).
 - Only S3600-SI series Ethernet switches support IPv6 ACL.
-

ACL Overview

As the network scale and network traffic are increasingly growing, security control and bandwidth assignment play a more and more important role in network management. Filtering data packets can prevent a network from being accessed by unauthorized users efficiently while controlling network traffic and saving network resources. Access Control Lists (ACLs) are often used to filter packets with configured matching rules.

Upon receiving a packet, the switch compares the packet with the rules of the ACL applied on the current port to permit or discard the packet.

The rules of an ACL can be referenced by other functions that need traffic classification, such as QoS.

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.

According to their application purposes, ACLs fall into the following categories.

- Basic ACL. Rules are created based on 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, 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, type of Layer 2 protocol, and so on.

- User-defined ACL. An ACL of this type matches packets by comparing the strings retrieved from the packets with specified strings. It defines the byte it begins to perform “and” operation with the mask on the basis of packet headers.
- IPv6 ACL: An ACL of this type matches IPv6 packets by matching information such as the source IP address, destination IP address, source MAC address, destination MAC address, traffic class, next header information, destination TCP or UDP port number, and VLAN tag.

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 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 rules in an ACL are matched in the order determined by the system, namely the “depth-first” rule (Layer 2 ACLs, user-defined ACLs and IPv6 ACLs do not support this feature).

For depth-first rule, there are two cases:

Depth-first match order for rules of a basic ACL

- 1) Range of source IP address: The smaller the source IP address range (that is, the more the number of zeros in the wildcard mask), the higher the match priority.
- 2) Fragment keyword: A rule with the fragment keyword is prior to others.
- 3) If the above two conditions are identical, the earlier configured rule applies.

Depth-first match order for rules of an advanced ACL

- 1) Protocol range: A rule which has specified the types of the protocols carried by IP is prior to others.
- 2) Range of source IP address: The smaller the source IP address range (that is, the more the number of zeros in the wildcard mask), the higher the match priority.
- 3) Range of destination IP address. The smaller the destination IP address range (that is, the more the number of zeros in the wildcard mask), the higher the match priority.
- 4) Range of Layer 4 port number, that is, TCP/UDP port number. The smaller the range, the higher the match priority.
- 5) Number of parameters: the more the parameters, the higher the match priority.

If rule A and rule B are still the same after comparison in the above order, the weighting principles will be used in deciding their priority order. Each parameter is given a fixed weighting value. This weighting value and the value of the parameter itself will jointly decide the final matching order. Involved parameters with weighting values from high to low are **icmp-type**, **established**, **dscp**, **tos**, **precedence**, **fragment**. Comparison rules are listed below.

- The smaller the weighting value left, which is a fixed weighting value minus the weighting value of every parameter of the rule, the higher the match priority.

- If the types of parameter are the same for multiple rules, then the sum of parameters' weighting values of a rule determines its priority. The smaller the sum, the higher the match priority.

Ways to Apply an ACL on a Switch

Being applied to the hardware directly

In the switch, an ACL can be directly applied to 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. For S3600 series Ethernet switches, the later the rule applies, the higher the match priority.

ACLs are directly applied to hardware when they are used for:

- Implementing QoS
- Filtering the packets to be forwarded

Being referenced by upper-level software

ACLs 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 (Layer 2 ACLs, user-defined ACLs and IPv6 ACLs do not support this feature).

When applying an ACL in this way, you can specify the order in which the rules in the ACL are matched. The match order cannot be modified once it is determined, unless you delete all the rules in the ACL and define the match order.

An ACL can be referenced by upper-layer software:

- Referenced by routing policies
- Used to control Telnet, SNMP and Web login users



Note

- When an ACL is directly applied to hardware for packet filtering, the switch will permit packets if the packets do not match the ACL.
 - When an ACL is referenced by upper-layer software to control Telnet, SNMP and Web login users, the switch will deny packets if the packets do not match the ACL.
-

Types of ACLs Supported by S3600 Series Ethernet Switches

The following types of ACLs are supported by S3600 series Ethernet switches:

- Basic ACL

- Advanced ACL
- Layer 2 ACL
- User-defined ACL
- IPv6 ACL

In addition, ACLs defined on S3600 series Ethernet switches can be applied to hardware directly or referenced by upper-layer software for packet filtering.

ACL Configuration Task List

Complete the following tasks to configure ACL:

Task	Remarks
Configuring Time Range	Optional
Configuring Basic ACL	Required
Configuring Advanced ACL	Required
Configuring Layer 2 ACL	Required
Configuring User-defined ACL	Required
Configuring IPv6 ACL	Required
Applying ACL Rules on Ports	Required
Applying ACL Rules to Ports in a VLAN	Required

Configuring Time Range

Time ranges can be used to filter packets. You can specify a time range for each rule in an ACL. A time range-based ACL takes effect only in specified time ranges. Only after a time range is configured and the system time is within the time range, can an ACL rule take effect.

Two types of time ranges are available:

- Periodic time range, which recurs periodically on the day or days of the week.
- Absolute time range, which takes effect only in a period of time and does not recur.



Note

An absolute time range on an H3C S3600 Series Ethernet Switches can be within the range 1970/1/1 00:00 to 2100/12/31 24:00.

Configuration procedure

Follow these steps to configure a time range:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a time range	time-range <i>time-name</i> { <i>start-time to end-time days-of-the-week</i> [from <i>start-time start-date</i>] [to <i>end-time end-date</i>] from <i>start-time start-date</i> [to <i>end-time end-date</i>] to <i>end-time end-date</i> }	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 is 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 is 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 is 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 from 1970/1/1 00:00 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.

Configuration example

Define a periodic time range that spans from 8:00 to 18:00 on Monday through Friday.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 working-day
[Sysname] display time-range test
Current time is 13:27:32 Apr/16/2005 Saturday
```

```
Time-range : test ( Inactive )
08:00 to 18:00 working-day
```

Define an absolute time range spans from 15:00 1/28/2006 to 15:00 1/28/2008.

```
<Sysname> system-view
[Sysname] time-range test from 15:00 1/28/2006 to 15:00 1/28/2008
[Sysname] display time-range test
Current time is 13:30:32 Apr/16/2005 Saturday
```

```
Time-range : test ( Inactive )
```

Configuring Basic ACL

A basic ACL filters packets based on their source IP addresses.

A basic ACL can be numbered from 2000 to 2999.

Configuration prerequisites

- 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 [Configuring Time Range](#).
- The source IP addresses based on which the ACL filters packets are determined.

Configuration procedure

Follow these steps to define a basic ACL rule:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create an ACL and enter basic ACL view	acl number <i>acl-number</i> [match-order { auto config }]	Required config by default
Define an ACL rule	rule [<i>rule-id</i>] { deny permit } [<i>rule-string</i>]	Required For information about <i>rule-string</i> , refer to <i>ACL Command</i> .
Configure a description string to the ACL	description <i>text</i>	Optional Not configured by default

Note that:

- With the **config** match order specified for the basic ACL, you can modify any existent rule. The unmodified part of the rule remains. With the **auto** match order specified for the basic ACL, you cannot modify any existent rule; otherwise the system will tell you that the rule cannot be modified.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will tell you that the rule cannot be created and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rule; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.
- With the **auto** match order specified, the newly created rules will be inserted in the existent ones by depth-first principle, but the numbers of the existent rules are unaltered.

Configuration example

```
# Configure ACL 2000 to deny packets whose source IP addresses are 192.168.0.1.
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 192.168.0.1 0

# Display the configuration information of ACL 2000.
[Sysname-acl-basic-2000] display acl 2000
Basic ACL 2000, 1 rule
Acl's step is 1
rule 0 deny source 192.168.0.1 0
```

Configuring Advanced ACL

An advanced ACL can filter packets by their source and destination IP addresses, the protocols carried by IP, and protocol-specific features such as TCP/UDP source and destination ports, ICMP message type and message code.

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 cluster management.

Advanced ACLs support analysis and processing of three packet priority levels: type of service (ToS) priority, IP priority and differentiated services codepoint (DSCP).

Using advanced ACLs, you can define classification rules that are more accurate, more abundant, and more flexible than those defined for basic ACLs.

Configuration prerequisites

- To configure a time range-based advanced ACL rule, you need to create the corresponding time ranges first. For information about time range configuration, refer to [Configuring Time Range](#).
- 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.

Configuration procedure

Follow these steps to define an advanced ACL rule:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create an advanced ACL and enter advanced ACL view	acl number <i>acl-number</i> [match-order { auto config }]	Required config by default
Define an ACL rule	rule [<i>rule-id</i>] { permit deny } <i>protocol</i> [<i>rule-string</i>]	Required For information about <i>protocol</i> and <i>rule-string</i> , refer to <i>ACL Commands</i> .

To do...	Use the command...	Remarks
Assign a description string to the ACL rule	rule <i>rule-id</i> comment <i>text</i>	Optional No description by default
Assign a description string to the ACL	description <i>text</i>	Optional No description by default

Note that:

- With the **config** match order specified for the advanced ACL, you can modify any existent rule. The unmodified part of the rule remains. With the **auto** match order specified for the ACL, you cannot modify any existent rule; otherwise the system will tell you that the rule cannot be modified.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will tell you that the rule cannot be created and you need to specify a number for the 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 the ACL is created with the **auto** keyword specified, the newly created rules will be inserted in the existent ones by depth-first principle, but the numbers of the existent rules are unaltered.

Configuration example

Configure ACL 3000 to permit the TCP packets sourced from the network 129.9.0.0/16 and destined for the network 202.38.160.0/24 and with the destination port number being 80.

```
<Sysname> system-view
```

```
[Sysname] acl number 3000
```

```
[Sysname-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
```

Display the configuration information of ACL 3000.

```
[Sysname-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
```

Configuring Layer 2 ACL

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.

Configuration prerequisites

- 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 [Configuring Time Range](#).
- The settings to be specified in the rule, such as source and destination MAC addresses, VLAN priorities, and Layer 2 protocol types, are determined.

Configuration procedure

Follow these steps to define a Layer 2 ACL rule:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a Layer 2 ACL and enter layer 2 ACL view	acl number <i>acl-number</i>	Required
Define an ACL rule	rule [<i>rule-id</i>] { permit deny } <i>rule-string</i>	Required For information about <i>rule-string</i> , refer to <i>ACL Commands</i> .
Assign a description string to the ACL rule	rule <i>rule-id</i> comment <i>text</i>	Optional No description by default
Assign a description string to the ACL	description <i>text</i>	Optional No description by default

Note that:

- You can modify any existent rule of the Layer2 ACL and the unmodified part of the ACL remains.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will tell you that the rule cannot be created and you need to specify a number for the 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.

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.

```
<Sysname> system-view
[Sysname] acl number 4000
```

```
[Sysname-acl-ethernetframe-4000] rule deny cos 3 source 000d-88f5-97ed
ffff-ffff-ffff dest 0011-4301-991e ffff-ffff-ffff

# Display the configuration information of ACL 4000.

[Sysname-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
```

Configuring User-defined ACL

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.

Configuration prerequisites

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 [Configuring Time Range](#).

Configuration procedure

Follow these steps to define a user-defined ACL rule:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a user-defined ACL and enter user-defined ACL view	acl number <i>acl-number</i>	Required
Define an ACL rule	rule [<i>rule-id</i>] { permit deny } [<i>rule-string rule-mask offset</i>] &<1-8> [time-range <i>time-name</i>]	Required For information about <i>rule-string</i> , refer to <i>ACL Commands</i> .
Define a comment for the ACL rule	rule <i>rule-id</i> comment <i>text</i>	Optional No description by default
Define a description for the ACL	description <i>text</i>	Optional No description by default



Note

When configuring a rule that matches specific fields of packets, take the following two items into account:

- If VLAN-VPN is not enabled, each packet in the switch carries one VLAN tag, which is 4 bytes long.
 - If VLAN-VPN is enabled on a port, each packet in the switch carries two VLAN tags, which is 8 bytes long.
-

Note that:

- You can modify any existent rule of a user-defined ACL. If you modify only the time range and/or action, the unmodified parts of the rule remain the same. If you modify the *rule-string rule-mask offset* combinations, however, the new combinations will replace all of the original ones.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will tell you that the rule cannot be created and you need to specify a number for the 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.

Configuration example

Configure ACL 5000 to deny all TCP packets, provided that VLAN-VPN is not enabled on any port. In the ACL rule, 06 is the TCP protocol number, ff is the mask of the rule, and 27 is the protocol field offset of an internally processed IP packet.

```
<Sysname> system-view
[Sysname] acl number 5000
[Sysname-acl-user-5000] rule deny 06 ff 27

# Display the configuration information of ACL 5000.

[Sysname-acl-user-5000] display acl 5000
User defined ACL 5000, 1 rule
Acl's step is 1
rule 0 deny 06 ff 27
```

Configuring IPv6 ACL

You can match IPv6 packets by IPv6 ACLs to process IPv6 data flows as required. The number of an IPv6 ACL is in the range from 5000 to 5999.

S3600-SI Series Ethernet switches support matching the following fields:

- **cos**: Matches the CoS field in IPv6 packets.

- **dest-ip**: Matches the destination IP address field in IPv6 packets.
- **dest-mac**: Matches the destination MAC address field in IPv6 packets.
- **double-tag**: Matches IPv6 packets with two tags.
- **dscp**: Matches the traffic class field in IPv6 packets.
- **ip-protocol**: Matches the next header field in IPv6 packets.
- **ipv6-type**: Matches IPv6 packets with the Layer 2 protocol being IPv6.
- **src-ip**: Matches the source address field in IPv6 packets.
- **dest-ip**: Matches the destination address field in IPv6 packets.
- **src-port**: Matches the TCP/UDP source port field in IPv6 packets.
- **dest-port**: Matches the TCP/UDP destination port field in IPv6 packets.
- **icmpv6-type**: Matches the ICMPv6 type field in IPv6 packets.
- **icmpv6-code**: Matches the ICMPv6 code field in IPv6 packets.
- **vlan**: Matches the VLAN tag field in IPv6 packets.



Note

IPv6 ACLs do not match IPv6 packets with extension headers.



Note

When configuring IPv6 ACL rules, note that:

- To specify the **src-port** or **dest-port** keyword for a rule, you need to specify the **ip-protocol rule-string rule-mask** combination as TCP or UDP, that is, 0x06 or 0x11. To specify the **icmpv6-type** or **icmpv6-code** keyword for a rule, you need to specify the **ip-protocol rule-string rule-mask** combination as ICMPv6, that is, 0x3a.
 - The total length of the fields in a rule cannot be more than 32 bytes; otherwise, the rule configuration will fail. For example, if you define the **src-ip** and **dest-ip** fields in rule 1, which are 16 bytes each and 32 bytes in total, you can define no more fields for the rule.
-

Configuration prerequisites

- To configure time range-based IPv6 ACL rules, you need to create the corresponding time ranges first. For information about time range configuration, refer to section [Configuring Time Range](#).
- The settings to be specified in the rule are determined.

Configuration procedure

Follow these steps to define an IPv6 ACL rule:

Operation	Command	Description
Enter system view	system-view	—
Create an IPv6 ACL and enter IPv6 ACL view	acl number <i>acl-number</i>	Required
Define an ACL rule	rule [<i>rule-id</i>] { deny permit } [cos <i>rule-string rule-mask</i>] [dest-ip <i>ipv6-address prefix-length</i>] [dest-mac <i>rule-string rule-mask</i>] [double-tag] [dscp <i>rule-string rule-mask</i>] [ip-protocol <i>rule-string rule-mask</i>] [ipv6-type] [src-ip <i>ipv6-address prefix-length</i>] [src-mac <i>rule-string rule-mask</i>] [vlan <i>rule-string rule-mask</i>] [[src-port <i>rule-string rule-mask</i> dest-port <i>rule-string rule-mask</i>] *] [icmpv6-type <i>rule-string rule-mask</i> icmpv6-code <i>rule-string rule-mask</i>] *] [time-range <i>time-name</i>]	Required To specify the src-port or dest-port keyword in the command, you need to specify the ip-protocol <i>rule-string rule-mask</i> combination as TCP or UDP, that is, 0x06 or 0x11. To specify the icmpv6-type or icmpv6-code keyword, you need to specify the ip-protocol <i>rule-string rule-mask</i> combination as ICMPv6, that is, 0x3a.
Assign a description string to the ACL rule	rule <i>rule-id</i> comment <i>text</i>	Optional No description by default
Assign a description string to the ACL	description <i>text</i>	Optional No description by default

Note that:

- You can modify any existent rule of an IPv6 ACL. If you modify only the action to be taken or the time range, the unmodified part of the rule remains the same. If you modify the contents of a user-defined string, the new string overwrites the original one.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rule of the ACL; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.



Note

IPv6 ACLs do not match IPv6 packets with extension headers.

Configuration example

```
# Configure an rule for IPv6 ACL 5000, denying packets from 3001::1/64 to 3002::1/64.
<Sysname> system-view
[Sysname] acl number 5000
[Sysname-acl-user-5000] rule deny src-ip 3001::1 64 dest-ip 3002::1 64

# Display the configuration information of ACL 5000.
[Sysname-acl-user-5000] display acl 5000
User defined ACL 5000, 1 rule
Acl's step is 1
rule 0 deny src-ip 3001::1 64 dest-ip 3002::1 64
```

Applying ACL Rules on Ports

By applying ACL rules on ports, you can filter packets on the corresponding ports.

Configuration prerequisites

You need to define an ACL before applying it on a port. For information about defining an ACL, refer to [Configuring Basic ACL](#), [Configuring Advanced ACL](#), [Configuring Layer 2 ACL](#), [Configuring User-defined ACL](#) and [Configuring IPv6 ACL](#).

Configuration procedure

Follow these steps to apply an ACL on a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Apply ACL rules on the port	packet-filter { inbound outbound } <i>acl-rule</i>	Required For information about <i>acl-rule</i> , refer to <i>ACL Commands</i> .

Configuration example

```
# Apply ACL 2000 on Ethernet 1/0/1 to filter inbound packets.
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] packet-filter inbound ip-group 2000
```

Applying ACL Rules to Ports in a VLAN

By applying ACL rules to ports in a VLAN, you can add filtering of packets on all the ports in the VLAN.



Note

The ACL rules are only applied to ports that are in the VLAN at the time the **packet-filter vlan** command is executed. In other words:

- A port joining the VLAN later will not use the ACL rules for packet filtering.
- A port leaving the VLAN later will keep using the ACL rules for packet filtering.

Configuration prerequisites

Before applying ACL rules to ports in a VLAN, you need to define the related ACLs. For information about defining an ACL, refer to [Configuring Basic ACL](#), [Configuring Advanced ACL](#), [Configuring Layer 2 ACL](#), [Configuring User-defined ACL](#) and [Configuring IPv6 ACL](#).

Configuration procedure

Follow these steps to apply ACL rules to ports in a VLAN:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Apply ACL rules to ports in a VLAN	packet-filter vlan <i>vlan-id</i> { inbound outbound } <i>acl-rule</i>	Required For information about <i>acl-rule</i> , refer to <i>ACL Commands</i> .

Configuration example

Apply ACL 2000 to all ports of VLAN 1 in the inbound direction to filter packets.

```
<Sysname> system-view
```

```
[Sysname] packet-filter vlan 1 inbound ip-group 2000
```

Displaying and Maintaining ACL Configuration

To do...	Use the command...	Remarks
Display a configured ACL or all the ACLs	display acl { all <i>acl-number</i> }	Available in any view

To do...	Use the command...	Remarks
Display a time range or all the time ranges	display time-range { all <i>time-name</i> }	
Display information about packet filtering	display packet-filter { interface <i>interface-type interface-number</i> unitid <i>unit-id</i> }	
Display information about ACL resources	display drv qacl_resource	

Examples for Upper-layer Software Referencing ACLs

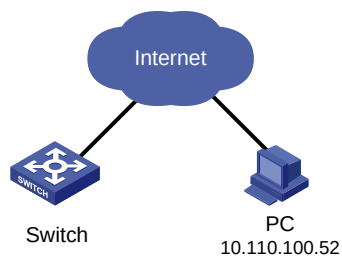
Example for Controlling Telnet Login Users by Source IP

Network requirements

Apply an ACL to permit users with the source IP address of 10.110.100.52 to telnet to the switch.

Network diagram

Figure 1-1 Network diagram for controlling Telnet login users by source IP



Configuration procedure

```

# Define ACL 2000.
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-basic-2000] quit

# Reference ACL 2000 on VTY user interface to control Telnet login users.
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] acl 2000 inbound
  
```

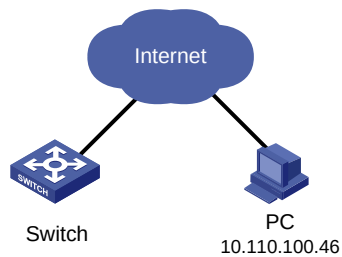
Example for Controlling Web Login Users by Source IP

Network requirements

Apply an ACL to permit Web users with the source IP address of 10.110.100.46 to log in to the switch through HTTP.

Network diagram

Figure 1-2 Network diagram for controlling Web login users by source IP



Configuration procedure

```
# Define ACL 2001.
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule 1 permit source 10.110.100.46 0
[Sysname-acl-basic-2001] quit

# Reference ACL 2001 to control users logging in to the Web server.
[Sysname] ip http acl 2001
```

Examples for Applying ACLs to Hardware

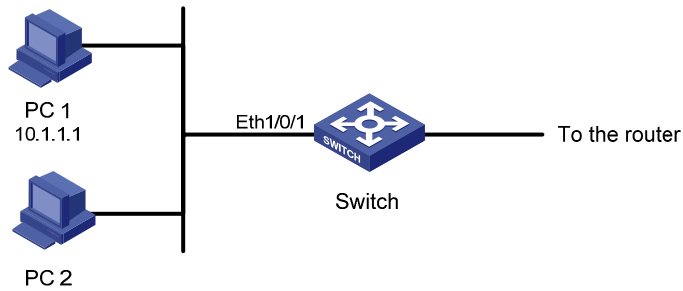
Basic ACL Configuration Example

Network requirements

PC 1 and PC 2 connect to the switch through Ethernet 1/0/1. PC1's IP address is 10.1.1.1. Apply an ACL on Ethernet 1/0/1 to deny packets with the source IP address of 10.1.1.1 from 8:00 to 18:00 everyday.

Network diagram

Figure 1-3 Network diagram for basic ACL configuration



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<Sysname> system-view
```

```
[Sysname] time-range test 8:00 to 18:00 daily
```

Define ACL 2000 to filter packets with the source IP address of 10.1.1.1.

```
[Sysname] acl number 2000
```

```
[Sysname-acl-basic-2000] rule 1 deny source 10.1.1.1 0 time-range test
```

```
[Sysname-acl-basic-2000] quit
```

Apply ACL 2000 on Ethernet 1/0/1.

```
[Sysname] interface Ethernet1/0/1
```

```
[Sysname-Ethernet1/0/1] packet-filter inbound ip-group 2000
```

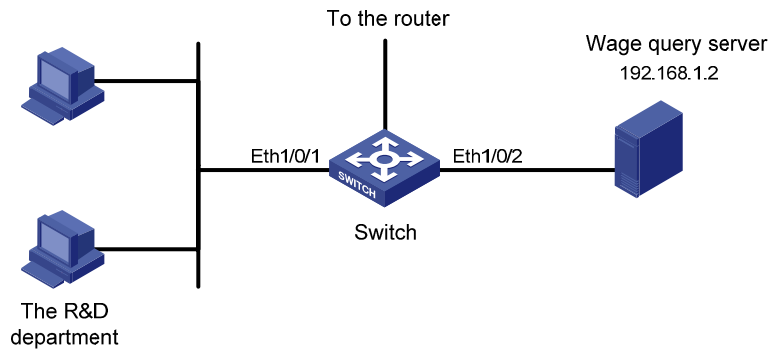
Advanced ACL Configuration Example

Network requirements

Different departments of an enterprise are interconnected through a switch. The IP address of the wage query server is 192.168.1.2. The R&D department is connected to Ethernet 1/0/1 of the switch. Apply an ACL to deny requests from the R&D department and destined for the wage server during the working hours (8:00 to 18:00).

Network diagram

Figure 1-4 Network diagram for advanced ACL configuration



Configuration procedure

```
# Define a periodic time range that is active from 8:00 to 18:00 everyday.
```

```
<Sysname> system-view
```

```
[Sysname] time-range test 8:00 to 18:00 working-day
```

```
# Define ACL 3000 to filter packets destined for wage query server.
```

```
[Sysname] acl number 3000
```

```
[Sysname-acl-adv-3000] rule 1 deny ip destination 192.168.1.2 0 time-range test
```

```
[Sysname-acl-adv-3000] quit
```

```
# Apply ACL 3000 on Ethernet 1/0/1.
```

```
[Sysname] interface Ethernet1/0/1
```

```
[Sysname-Ethernet1/0/1] packet-filter inbound ip-group 3000
```

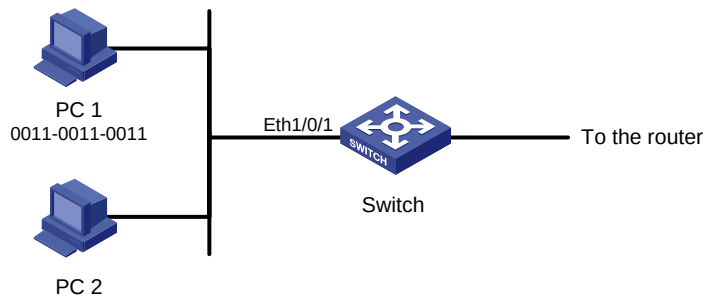
Layer 2 ACL Configuration Example

Network requirements

PC 1 and PC 2 connect to the switch through Ethernet 1/0/1. PC 1's MAC address is 0011-0011-0011. Apply an ACL to filter packets with the source MAC address of 0011-0011-0011 and the destination MAC address of 0011-0011-0012 from 8:00 to 18:00 everyday.

Network diagram

Figure 1-5 Network diagram for Layer 2 ACL



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<Sysname> system-view
```

```
[Sysname] time-range test 8:00 to 18:00 daily
```

Define ACL 4000 to filter packets with the source MAC address of 0011-0011-0011 and the destination MAC address of 0011-0011-0012.

```
[Sysname] acl number 4000
```

```
[Sysname-acl-ethernetframe-4000] rule 1 deny source 0011-0011-0011 ffff-ffff-ffff  
dest 0011-0011-0012 ffff-ffff-ffff time-range test
```

```
[Sysname-acl-ethernetframe-4000] quit
```

Apply ACL 4000 on Ethernet 1/0/1.

```
[Sysname] interface Ethernet1/0/1
```

```
[Sysname-Ethernet1/0/1] packet-filter inbound link-group 4000
```

User-defined ACL Configuration Example

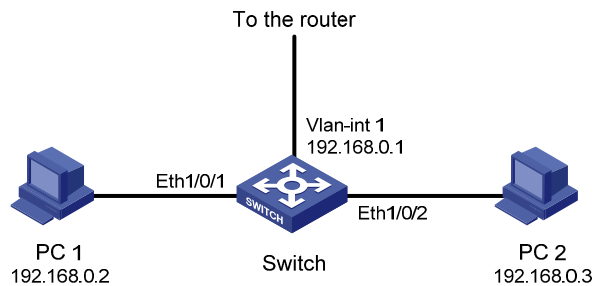
Network requirements

As shown in [Figure 1-6](#), PC 1 and PC 2 are connected to the switch through Ethernet 1/0/1 and Ethernet 1/0/2 respectively. They belong to VLAN 1 and access the Internet through the same gateway, which has an IP address of 192.168.0.1 (the IP address of VLAN-interface 1).

Configure a user-defined ACL to deny all ARP packets from PC 1 that use the gateway IP address as the source address from 8:00 to 18:00 everyday.

Network diagram

Figure 1-6 Network diagram for user-defined ACL



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<Sysname> system-view
```

```
[Sysname] time-range test 8:00 to 18:00 daily
```

Define ACL 5000 to deny any ARP packet whose source IP address is 192.168.0.1 from 8:00 to 18:00 everyday (provided that VLAN-VPN is not enabled on any port). In the ACL rule, 0806 is the ARP protocol number, ffff is the mask of the rule, 16 is the protocol type field offset of the internally processed Ethernet frame, c0a80001 is the hexadecimal form of 192.168.0.1, and 32 is the source IP address field offset of the internally processed ARP packet.

```
[Sysname] acl number 5000
```

```
[Sysname-acl-user-5000] rule 1 deny 0806 ffff 16 c0a80001 ffffffff 32 time-range test
```

Apply ACL 5000 on Ethernet 1/0/1.

```
[Sysname] interface Ethernet1/0/1
```

```
[Sysname-Ethernet1/0/1] packet-filter inbound user-group 5000
```

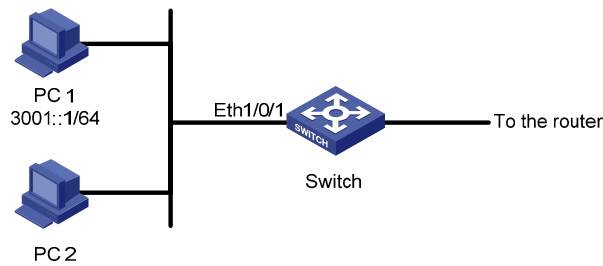
IPv6 ACL Configuration Example

Network requirements

PC 1 and PC 2 connect to the switch through Ethernet 1/0/1. The IP address of PC 1 is 3001::1/64. Configure an ACL to filter packets that PC 1 sends to 3002::1/64 from 8:00 to 18:00 everyday.

Network diagram

Figure 1-7 Network diagram for IPv6 ACL configuration



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<Sysname> system-view
```

```
[Sysname] time-range test 8:00 to 18:00 daily
```

Create an IPv6 ACL and configure a rule for the ACL, denying packets from 3001::1/64 to 3002::1/64.

```
[Sysname] acl number 5000
```

```
[Sysname-acl-user-5000] rule deny src-ip 3001::1 64 dest-ip 3002::1 64 time-range test
```

```
[Sysname-acl-user-5000] quit
```

Apply the ACL to port Ethernet 1/0/1.

```
[Sysname] interface Ethernet1/0/1
```

```
[Sysname-Ethernet1/0/1] packet-filter inbound user-group 5000
```

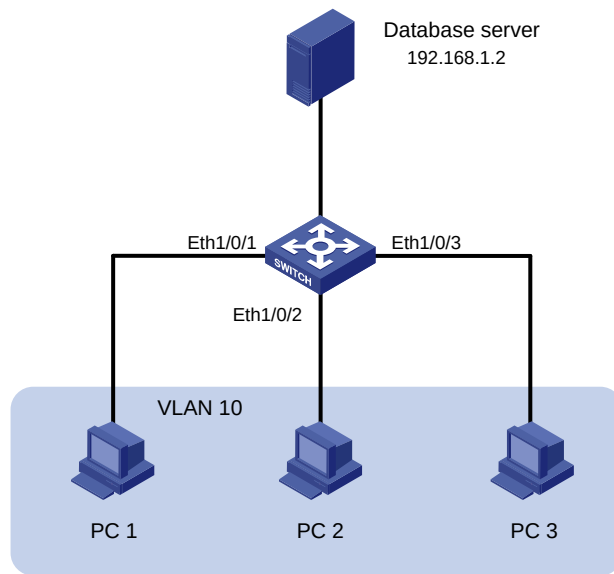
Example for Applying an ACL to a VLAN

Network requirements

PC 1, PC 2 and PC 3 belong to VLAN 10 and connect to the switch through Ethernet 1/0/1, Ethernet 1/0/2 and Ethernet 1/0/3 respectively. The IP address of the database server is 192.168.1.2. Apply an ACL to deny packets from PCs in VLAN 10 to the database server from 8:00 to 18:00 in working days.

Network diagram

Figure 1-8 Network diagram for applying an ACL to a VLAN



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 in working days.

```
<Sysname> system-view
```

```
[Sysname] time-range test 8:00 to 18:00 working-day
```

Define an ACL to deny packets destined for the database server.

```
[Sysname] acl number 3000
```

```
[Sysname-acl-adv-3000] rule 1 deny ip destination 192.168.1.2 0 time-range test
```

```
[Sysname-acl-adv-3000] quit
```

Apply ACL 3000 to VLAN 10.

```
[Sysname] packet-filter vlan 10 inbound ip-group 3000
```

Table of Contents

1 QoS Configuration	1-1
Overview	1-1
Introduction to QoS	1-1
Traditional Packet Forwarding Service	1-1
New Applications and New Requirements	1-1
Major Traffic Control Techniques	1-2
QoS Supported By S3600 Series Ethernet Switches	1-3
Introduction to QoS Functions	1-4
Traffic Classification	1-4
Priority Trust Mode	1-4
Protocol Priority	1-8
Priority Marking	1-8
Traffic Policing	1-8
Line Rate	1-9
Traffic Redirecting	1-9
VLAN Mapping	1-10
Queue Scheduling	1-10
Congestion Avoidance	1-12
Flow-based Traffic Accounting	1-13
Burst	1-13
Traffic mirroring	1-13
QoS Configuration	1-13
Configuring Priority Trust Mode	1-14
Configuring the Mapping between 802.1p Priority and Local Precedence	1-15
Setting the Priority of Protocol Packets	1-16
Marking Packet Priority	1-16
Configuring Traffic Policing	1-18
Configuring Line Rate	1-19
Configuring Traffic Redirecting	1-19
Configuring VLAN Mapping	1-20
Configuring Queue Scheduling	1-21
Configuring WRED	1-23
Configuring Traffic Accounting	1-23
Enabling the Burst Function	1-24
Configuring Traffic Mirroring	1-24
Displaying and Maintaining QoS	1-26
QoS Configuration Examples	1-26
Configuration Example of Traffic policing and Line Rate	1-26
Configuration Example of Priority Marking and Queue Scheduling	1-27
VLAN Mapping Configuration Example	1-29
Configuring Traffic Mirroring and Redirecting Traffic to a Port	1-31
2 QoS Profile Configuration	2-1
Overview	2-1

Introduction to QoS Profile	2-1
QoS Profile Application Mode	2-1
QoS Profile Configuration Task List.....	2-2
Configuring a QoS Profile.....	2-2
Applying a QoS Profile	2-3
Displaying and Maintaining QoS Profile Configuration	2-4
Configuration Example.....	2-4
QoS Profile Configuration Example.....	2-4

1 QoS Configuration

When configuring QoS, go to these sections for information you are interested in:

- [Overview](#)
- [QoS Supported By S3600 Series Ethernet Switches](#)
- [QoS Configuration](#)
- [Displaying and Maintaining QoS](#)
- [QoS Configuration Examples](#)

Overview

Introduction to QoS

Quality of Service (QoS) is a concept concerning service demand and supply. It reflects the ability to meet customer needs. Generally, QoS does not focus on grading services precisely, but on improving services under certain conditions.

In an internet, QoS refers to the ability of the network to forward packets. The evaluation on QoS of a network can be based on different aspects because the network may provide various services. Generally, QoS refers to the ability to provide improved service by solving the core issues such as delay, jitter, and packet loss ratio in the packet forwarding process.

Traditional Packet Forwarding Service

In traditional IP networks, packets are treated equally. That is, the FIFO (first in first out) policy is adopted for packet processing. Network resources required for packet forwarding is determined by the order in which packets arrive. All the packets share the resources of the network. Network resources available to the packets completely depend on the time they arrive. This service policy is known as Best-effort, which delivers the packets to their destination with the best effort, with no assurance and guarantee for delivery delay, jitter, packet loss ratio, reliability, and so on.

The traditional Best-Effort service policy is only suitable for applications insensitive to bandwidth and delay, such as WWW, E-mail and FTP.

New Applications and New Requirements

With the expansion of computer network, more and more networks become part of the Internet. The Internet gains rapid development in terms of scale, coverage and user quantities. More and more users use the Internet as a platform for their services and for data transmission.

Besides the traditional applications such as WWW, E-mail, and FTP, new services are developed on the Internet, such as tele-education, telemedicine, video telephone, videoconference and Video-on-Demand (VoD). Enterprise users expect to connect their regional branches together using VPN techniques for coping with daily business, for instance, accessing databases or manage remote equipments through Telnet.

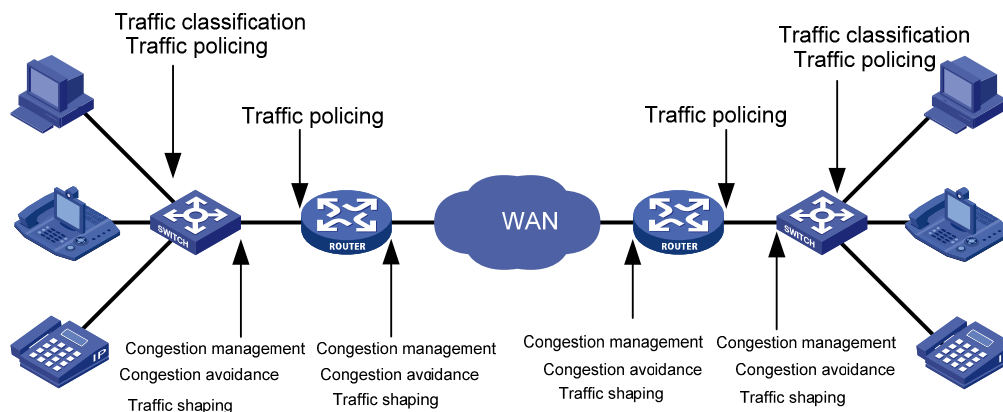
All these new applications have one thing in common, that is, they have special requirements for bandwidth, delay, and jitter. For instance, bandwidth, delay, and jitter are critical for videoconference

and VoD. As for other applications, such as transaction processing and Telnet, although bandwidth is not as critical, a too long delay may cause unexpected results. That is, they need to get serviced in time even if congestion occurs.

Newly emerging applications demand higher service performance from IP networks. In addition to simply delivering packets to their destinations, better network services are demanded, such as allocating dedicated bandwidth, reducing packet loss ratio, avoiding congestion, regulating network traffic, and setting priority of the packets. To meet those requirements, the network should be provided with better service capability.

Major Traffic Control Techniques

Figure 1-1 End-to-end QoS model



As shown in the figure above, traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance are the foundations for a network to provide differentiated services. They are described as follow:

- Traffic classification identifies traffic based on certain matching rules. It is a prerequisite for differentiated services and is usually applied in the inbound direction of a port.
- Traffic policing confines traffic to a specific specification and is usually applied in the inbound direction of a port. You can configure restriction or penalty measures against the exceeding traffic to protect carrier benefits and network resources.
- Traffic shaping adapts output traffic rate usually to the input capability of the receiving device to avoid packet drop and port congestion. Traffic shaping is usually applied in the outbound direction of a port.
- Congestion management handles resource competition during network congestion. Generally, it adds packets to queues first, and then forwards the packets by using a scheduling algorithm. Congestion management is usually applied in the outbound direction of a port.
- Congestion avoidance monitors the use of network resources and drops packets actively when congestion reaches certain degree. It relieves network load by adjusting traffics. Congestion avoidance is usually applied in the outbound direction of a port.

Traffic classification is the basis of all the above-mentioned traffic management technologies. It identifies packets using certain rules and makes differentiated services possible. Traffic policing, traffic shaping, congestion management, and congestion avoidance are methods for implementing network traffic control and network resource management. They are occurrences of differentiated services.

QoS Supported By S3600 Series Ethernet Switches

The S3600 series Ethernet switches support the QoS features listed in [Table 1-1](#):

Table 1-1 QoS features supported by S3600 series Ethernet switches

QoS Feature	Description	Refer to ...
Traffic classification	Classify incoming traffic based on ACLs. The S3600 series support the following types of ACLs: • Basic ACLs • Advanced ACLs • Layer-2 ACLs • User-defined ACLs • IPv6 ACLs (only S3600-SI series support)	• For information about ACLs, refer to the <i>ACL Operation</i> and <i>ACL Command</i> manuals. • For information about traffic classification, refer to Traffic Classification.
QoS action	The S3600 series support performing the following QoS actions for packets matching the specified ACL: • Priority marking • Traffic policing • Traffic redirecting • VLAN Mapping • Traffic accounting • Traffic mirroring	• For information about priority marking, refer to Priority Marking. • For information about traffic policing, refer to Traffic Policing. • For information about traffic redirecting, refer to Traffic Redirecting. • For information about VLAN Mapping, refer to VLAN Mapping. • For information about traffic accounting, refer to Flow-based Traffic Accounting. • For information about traffic mirroring, refer to Traffic mirroring.
	You can configure the following QoS actions as required on the S3600 series: • Priority trust mode • Protocol packet priority • Line rate • Burst	• For information about priority trust mode, refer to Priority Trust Mode. • For information about specifying priority for protocol packets, refer to Protocol Priority. • For information about line rate, refer to Line Rate. • For information about the burst function, refer to Burst.
Congestion avoidance	WRED	For information about congestion avoidance and WRED, refer to Congestion Avoidance .
Congestion management	The S3600 series support SP, WFQ, and WRR queue scheduling algorithms and support the following five queue scheduling modes: • SP • WFQ • WRR • SP+WFQ • SP+WRR	For information about SP, WFQ, and WRR, refer to Queue Scheduling .

Introduction to QoS Functions

Traffic Classification

Traffic here refers to service traffic; that is, all the packets passing the switch.

Traffic classification means identifying packets that conform to certain characteristics according to certain rules. It is the foundation for providing differentiated services.

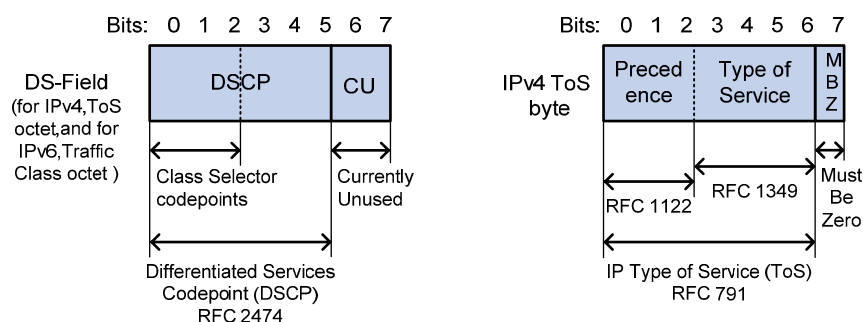
In traffic classification, the priority bit in the type of service (ToS) field in IP packet header can be used to identify packets of different priorities. The network administrator can also define traffic classification policies to identify packets by the combination of source address, destination address, MAC address, IP protocol or the port number of an application. Normally, traffic classification is done by checking the information carried in packet header. Packet payload is rarely adopted for traffic classification. The identifying rule is unlimited in range. It can be a quintuplet consisting of source address, source port number, protocol number, destination address, and destination port number. It can also be simply a network segment.

Priority Trust Mode

Introduction to precedence types

- 1) IP precedence, ToS precedence, and DSCP precedence

Figure 1-2 DS field and ToS byte



The ToS field in an IP header contains eight bits numbered 0 through 7, among which,

- The first three bits indicate IP precedence in the range 0 to 7.
- Bit 3 to bit 6 indicate ToS precedence in the range of 0 to 15.
- In RFC2474, the ToS field in IP packet header is also known as DS field. The first six bits (bit 0 through bit 5) of the DS field indicate differentiated service codepoint (DSCP) in the range of 0 to 63, and the last two bits (bit 6 and bit 7) are reserved.

Table 1-2 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

IP Precedence (decimal)	IP Precedence (binary)	Description
5	101	critical
6	110	internet
7	111	network

In a network providing differentiated services, traffics are grouped into the following four classes, and packets are processed according to their DSCP values.

- 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 subclasses;
- 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 1-3 Description on DSCP precedence values

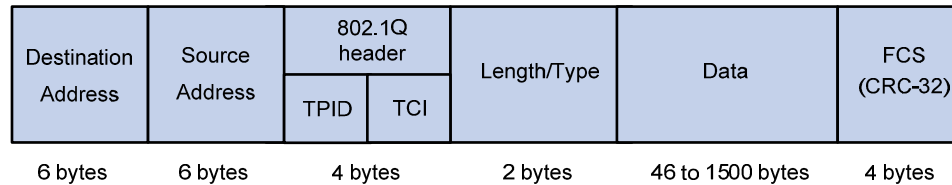
DSCP value (decimal)	DSCP value (binary)	Description
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7

DSCP value (decimal)	DSCP value (binary)	Description
0	000000	be (default)

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.

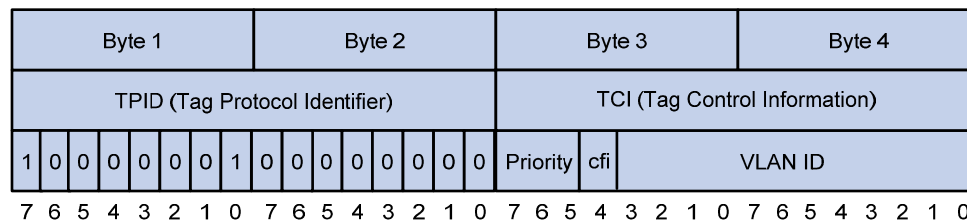
Figure 1-3 An Ethernet frame with an 802.1Q tag header



As shown in the figure above, the 4-byte 802.1Q tag header consists of the tag protocol identifier (TPID, two bytes in length), whose value is 0x8100, and the tag control information (TCI, two bytes in length).

[Figure 1-4](#) describes the detailed contents of an 802.1Q tag header.

Figure 1-4 802.1Q tag headers



In the figure above, the priority field (three bits in length) in TCI is 802.1p priority (also known as CoS precedence), which ranges from 0 to 7.

Table 1-4 Description on 802.1p priority

802.1p priority (decimal)	802.1p priority (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.

3) Local precedence

Local precedence is a locally significant precedence that the device assigns to a packet. A local precedence value corresponds to one of the eight hardware output queues. Packets with the highest local precedence are processed preferentially. As local precedence is used only for internal queuing, a packet does not carry it after leaving the queue.

Priority trust mode

After a packet enters a switch, the switch sets the 802.1p priority and local precedence for the packet according to its own capability and the corresponding rules.

1) For a packet carrying no 802.1q tag

When a packet carrying no 802.1q tag reaches the port of a switch, the switch uses the port priority as the 802.1p precedence value of the received packet, searches for the local precedence corresponding to the port priority of the receiving port in the 802.1p-to-local precedence mapping table, and assigns the local precedence to the packet.

2) For an 802.1q tagged packet

When an 802.1q tagged packet reaches the port of a switch, you can use the **priority trust** on the receiving port to configure the port to trust packet priority or use the **priority** command on the receiving port to configure the port to trust port priority. By default, port priority is trusted and the priority of a port is 0.

- Trusting port priority

In this mode, the switch replaces the 802.1p priority of the received packet with the port priority, searches for the local precedence corresponding to the port priority of the receiving port in the 802.1p-to-local precedence mapping table, and assigns the local precedence to the packet.

- Trusting packet priority

In this mode, the switch searches for the local precedence corresponding to the 802.1p priority of the packet in the 802.1p-to-local precedence mapping table and assigns the local precedence to the packet.

[Table 1-5](#) shows the default 802.1p priority-to-local precedence mapping table. You can modify the default mapping tables at the CLI. For detailed configuration procedure, refer to [Configuring the Mapping between 802.1p Priority and Local Precedence](#).

Table 1-5 802.1p priority-to-local precedence mapping table

802.1p priority	Local precedence
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Protocol Priority

Protocol packets generated by a switch carry their own priority. You can set a new IP precedence or DSCP precedence for the specific type of protocol packets to implement QoS.

Priority Marking

The priority marking function is to reassign priority for the traffic matching an ACL referenced for traffic classification.

- If 802.1p priority marking is configured, the traffic will be mapped to the local precedence corresponding to the re-marked 802.1p priority and assigned to the output queue corresponding to the local precedence.
- If local precedence marking is configured, the traffic will be assigned to the output queue corresponding to the re-marked local precedence.
- If IP precedence or DSCP marking is configured, the traffic will be marked with new IP precedence or DSCP precedence.

Traffic Policing

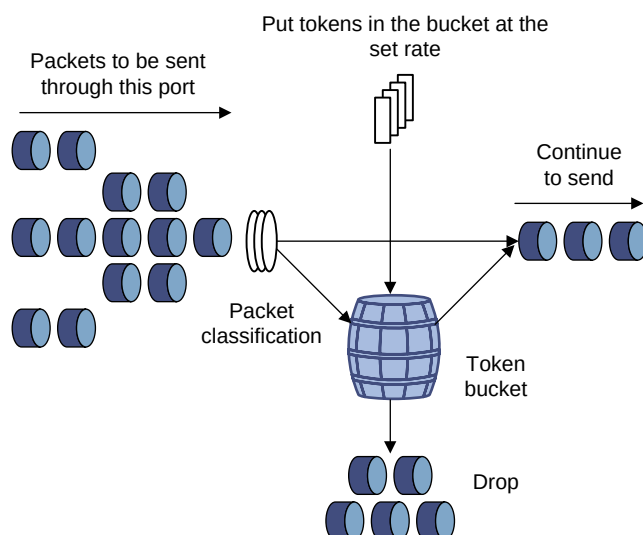
The network will be made more congested by plenty of continuous burst packets if the traffic of each user is not limited. The traffic of each user must be limited in order to make better use of the limited network resources and provide better service for more users. For example, traffic can be limited to get only its committed resources during a time period to avoid network congestion caused by excessive bursts.

Traffic policing is a kind of traffic control policy used to limit the traffic and the resource occupied by supervising the traffic. The regulation policy is implemented according to the evaluation result on the premise of knowing whether the traffic exceeds the specification when traffic policing is performed. Normally, token bucket is used for traffic evaluation.

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 1-5 Evaluate the traffic with the token bucket



Evaluating the traffic with the token bucket

When token bucket is used for traffic evaluation, the number of the tokens in the token bucket determines the amount of the packets that can be forwarded. If the number of tokens in the bucket is enough to forward the packets, the traffic is conforming to the specification; otherwise, the traffic is nonconforming or excess.

Parameters concerning token bucket 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.

Traffic policing

The typical application of traffic policing is to supervise specific traffic into the network and limit it to 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, traffic policing can choose to drop the packets or to reset the priority of the packets.

Traffic policing is widely used in policing the traffic into the network of internet service providers (ISPs). Traffic policing can identify the policed traffic and perform pre-defined policing actions based on different evaluation results. These actions include:

- Drop. Drop the packet whose evaluation result is "nonconforming".
- Modify the DSCP precedence and forward. Modify the DSCP precedence of the packets whose evaluation result is "nonconforming" and then forward them.

Line Rate

Line rate refers to limiting the total rate of inbound or outbound packets on a port.

Line rate can be implemented through token buckets. That is, if you perform line rate configuration for a port, the token bucket determines the way to process the packets to be sent by this port or packets reaching the port. Packets can be sent or received if there are enough tokens in the token bucket; otherwise, they will be dropped.

Compared to traffic policing, line rate applies to all the packets passing a port. It is a simpler solution if you want to limit the rate of all the packets passing a port.

Traffic Redirecting

Traffic redirecting identifies traffic using ACLs and redirects the matched packets to CPU, the specified ports/aggregation group. By traffic redirecting, you can change the way in which a packet is forwarded to achieve specific purposes.

VLAN Mapping

VLAN mapping identifies traffics using ACLs and maps the VLAN tags carrier in matched packets to specific VLAN tags. By employing VLAN mapping on a switch connecting user networks to the carrier network, you can map the VLAN tags of specific user network packets to those of specific VLANs in the carrier network, thus meeting the requirements of the carrier network.

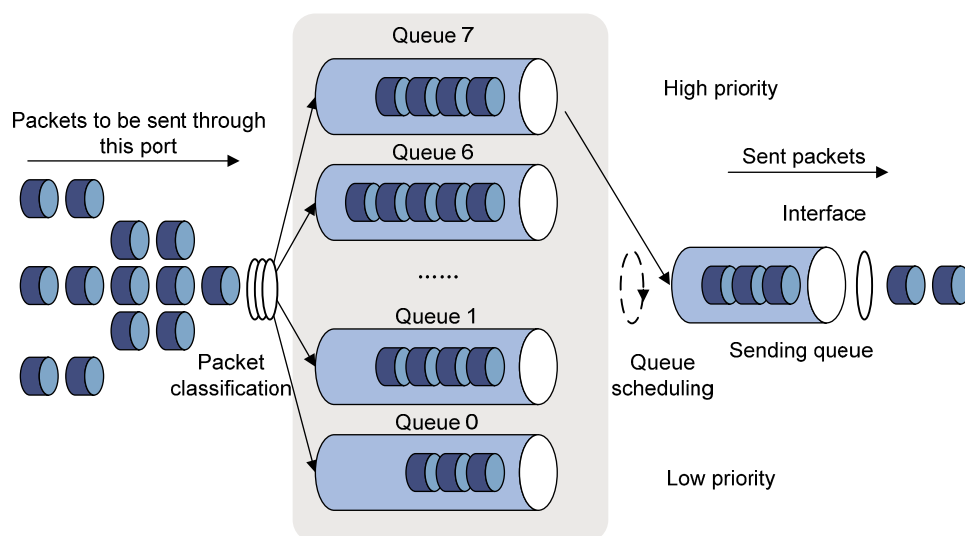
Queue Scheduling

When the network is congested, the problem that many packets compete for resources must be solved, usually through queue scheduling.

The S3600 series switches support three queue scheduling algorithms: Strict Priority (SP) queuing, Weighted Fair Queuing (WFQ), and Weighted Round Robin (WRR) queuing.

1) SP queuing

Figure 1-6 Diagram for SP queuing



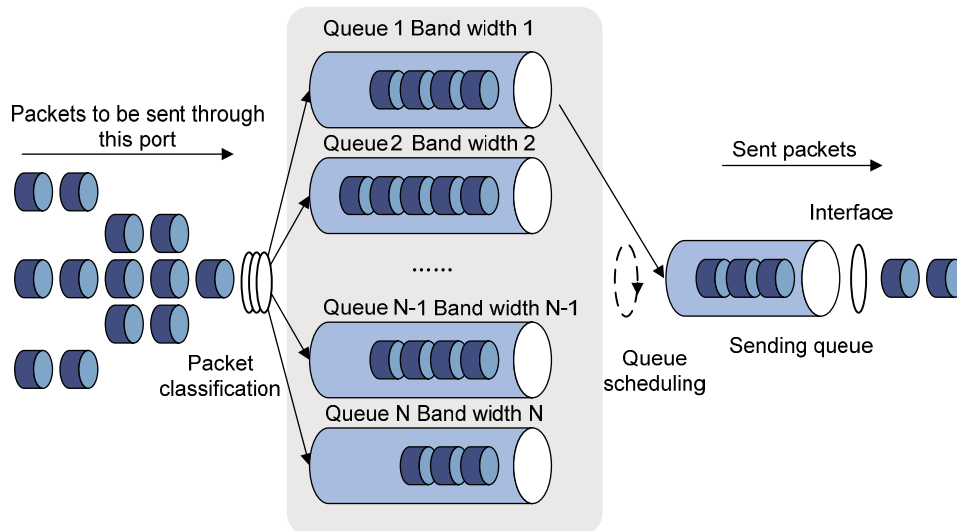
SP queue-scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay. Assume that there are eight output queues on the port and the preferential queue 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 queuing

Figure 1-7 Diagram for WFQ queuing



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:

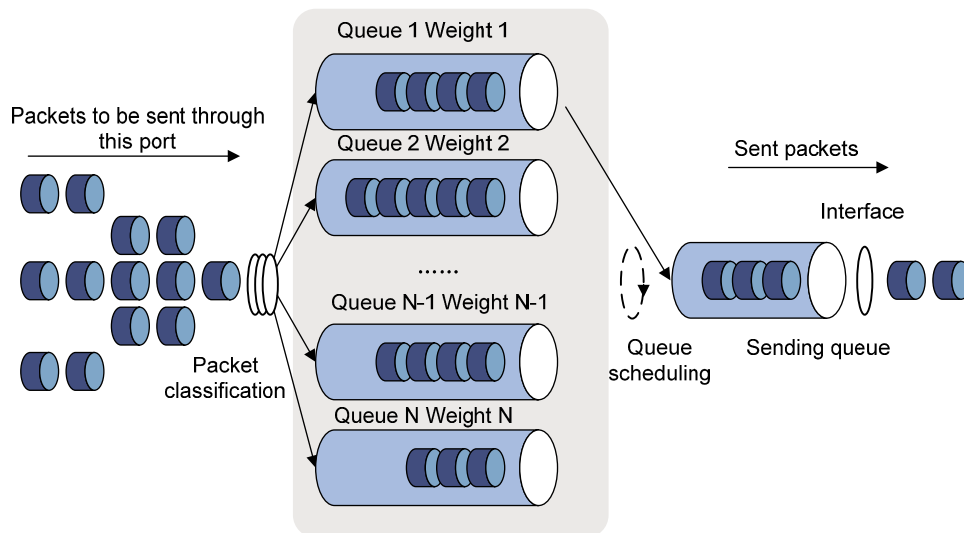
- Different queues are scheduled fairly, so the delay of each flow is balanced globally.
- Both short and long packets are scheduled fairly. When there are multiple long packets and short packets to be sent among different queues, the short packets must be scheduled preferentially, so that the delay 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 values in the ToS field. WFQ also provide as many queues as possible to accommodate each flow evenly. Thus, the delay of each flow is balanced globally. When the packets dequeue, WFQ assigns the bandwidth to each flow 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 is taken out to be sent according to the proportion of bandwidth.

You can use the WFQ algorithm to assign bandwidth to the output queues of a port, 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 decide how much bandwidth is to be assigned to each traffic.

3) WRR queuing

Figure 1-8 Diagram for WRR queuing



WRR queue-scheduling algorithm schedules all the queues in turn and every queue can be assured of a certain service time.

In a typical H3C switch there are eight output queues on each port. WRR configures a weight value for each queue, for example: w_7 , w_6 , w_5 , w_4 , w_3 , w_2 , w_1 , and w_0 respectively for queue 7 through queue 0. A weight value indicates the proportion of resources available for a queue. On a 100-Mbps port, configure the weight value of WRR queue-scheduling algorithm to 5, 5, 3, 3, 1, 1, 1, and 1 (corresponding to w_7 , w_6 , w_5 , w_4 , w_3 , w_2 , w_1 , and w_0 in order). In this way, the queue with the lowest priority can get 5 Mbps ($100 \text{ Mbps} \times 1/(5+5+3+3+1+1+1+1)$) 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.

Congestion Avoidance

Congestion may cause network resource unavailable and thus need to be prevented. As a type of flow control mechanism, congestion avoidance aims to relieve network load through traffic adjusting. With congestion avoidance configuration performed, packets are dropped in advance when the utilization of certain network resources (such as output queues or buffer created in the memory) reaches certain degree.

Traditional packet dropping policy

Tail drop is adopted in traditional packet drop policies. It drops all the newly arrived packets when the current queue length reaches a specific value.

Such a policy will result in global TCP connection synchronization. If a queue drops packets of multiple TCP connections simultaneously, the TCP connections will turn to the state of congestion avoidance and slow startup for the traffics to be regulated. The traffic peak will then occur in a certain future time. Consequently, the network traffic jitters all the time.

WRED

You can use weighted random early detection (WRED) to avoid global TCP session synchronization.

In WRED algorithm, an upper limit and a lower limit are set for each queue, and the packets in a queue are processed as follows.

- When the current queue length is smaller than the lower limit, no packet is dropped;
- When the queue length exceeds the upper limit, all the newly received packets are dropped;
- When the queue length is between the lower limit and the upper limit, the newly received packets are dropped at random. The longer the queue, the more likely the newly received packets may be dropped. However, a maximum drop probability exists.

In WRED, random numbers are generated to determine the packets to be dropped. As the dropping policy is determined by IP precedence, packets with lower precedence are more likely to be dropped.

WRED prevents global TCP session synchronization. It enables other TCP sessions to be free of a TCP session slowed down because of its packets being dropped. In this way, TCP sessions can operate in different rates in any case and the link bandwidth can be fully utilized.

Flow-based Traffic Accounting

The function of flow-based traffic accounting is to use ACL rules in traffic classification and perform traffic accounting on the packets matching the ACL rules. You can get the statistics of the packets you are interested in through this function.

Burst

The Burst function can provide better packet cache function and traffic forwarding performance. It is suitable for networks where

- Large amount of broadcast/multicast packets and large burst traffic exist.
- Packets of high-rate links are forwarded to low-rate links or packets of multiple links with the equal rates are forwarded to a single link that is of the same rate as that of the incoming links.

Although the burst function helps reduce the packet loss ratio and improve packet processing capability in the networks mentioned above, it may affect QoS performance. So, use this function with caution.

Traffic mirroring

Traffic mirroring identifies traffic using ACLs and duplicates the matched packets to the destination mirroring port or CPU depending on your configuration. For information about port mirroring, refer to the Mirroring module of this manual.

QoS Configuration

Complete the following tasks to configure QoS:

Task	Remarks
Configuring Priority Trust Mode	Optional
Configuring the Mapping between 802.1p Priority and Local Precedence	Optional
Setting the Priority of Protocol Packets	Optional
Marking Packet Priority	Optional
Configuring Traffic Policing	Optional
Configuring Line Rate	Optional

Task	Remarks
Configuring Traffic Redirecting	Optional
Configuring VLAN Mapping	Optional
Configuring Queue Scheduling	Optional
Configuring WRED	Optional
Configuring Traffic Accounting	Optional
Enabling the Burst Function	Optional
Configuring Traffic Mirroring	Optional

Configuring Priority Trust Mode

Refer to section [Priority Trust Mode](#) for introduction to priority trust mode.

Configuration prerequisites

- The priority trust mode to be adopted has been determined.
- The port where priority trust mode is to be configured has been determined.
- The port priority value has been determined.

Configuration procedure

Follow these steps to configure to trust port priority:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure to trust port priority and configure the port priority	priority <i>priority-level</i>	Optional By default, the switch trusts port priority and the priority of a port is 0.

Follow these steps to configure to trust packet priority:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure to trust packet priority	priority trust	Required By default, the switch trusts port priority.

Configuration example

- Configure to trust port priority on Ethernet 1/0/1 and set the priority of Ethernet 1/0/1 to 7.

Configuration procedure:

```
<Sysname> system-view
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] priority 7
```

- Configure to trust packet priority on Ethernet 1/0/2.

Configuration procedure:

```
<Sysname> system-view
[Sysname] interface Ethernet1/0/2
[Sysname-Ethernet1/0/2] priority trust
```

Configuring the Mapping between 802.1p Priority and Local Precedence

When the default mapping between 802.1p priority and local precedence cannot satisfy your requirements, you can modify the mapping at the CLI, thus modifying the mapping between 802.1p priority and the output queues and assigning packets with different priorities to the corresponding output queues.

Note that, this is a global setting, not a per port setting. This is only recommended for advanced network environments.

Configuration prerequisites

The mapping between 802.1p priority and local precedence has been determined.

Configuration procedure

Follow these steps to configure the mapping between 802.1p priority and local precedence:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the mapping between 802.1p priority and local precedence	qos cos-local-precedence-map <i>cos0-map-local-prec cos1-map-local-prec</i> <i>cos2-map-local-prec cos3-map-local-prec</i> <i>cos4-map-local-prec cos5-map-local-prec</i> <i>cos6-map-local-prec cos7-map-local-prec</i>	Required

Configuration example

- Configure the following mapping between 802.1p priority and local precedence: 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.

Configuration procedure:

```
<Sysname> system-view
[Sysname] qos cos-local-precedence-map 2 3 4 1 7 0 5 6
[Sysname] display 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
```

Setting the Priority of Protocol Packets

Refer to section [Protocol Priority](#) for information about priority of protocol packets.

Configuration prerequisites

- The protocol type has been determined.
- The priority type (IP or DSCP) and priority value have been determined.

Configuration procedure

Follow these steps to set the priority for specific protocol packets:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the priority for specific protocol packets	protocol-priority protocol-type <i>protocol-type { ip-precedence ip-precedence dscp dscp-value }</i>	Required You can modify the IP precedence or DSCP precedence of the corresponding protocol packets.



Note

- On an S3600-EI switch, you can set the priority for protocol packets of Telnet, OSPF, SNMP, and ICMP.
- On an S3600-SI switch, you can set the priority for protocol packets of Telnet, SNMP, and ICMP.

Configuration example

- Set the IP precedence of ICMP packets to 3.
- Display the configuration.

Configuration procedure:

```
<Sysname> system-view
[Sysname] protocol-priority protocol-type icmp ip-precedence 3
[Sysname] display protocol-priority
Protocol: icmp
IP-Precedence: flash(3)
```

Marking Packet Priority

Refer to section [Priority Marking](#) for information about marking packet priority.

Marking packet priority can be implemented in the following two ways:

- Through traffic policing

When configuring traffic policing, you can define the action of marking the DSCP precedence for packets exceeding the traffic specification. Refer to section [Configuring Traffic Policing](#).

- Through the **traffic-priority** command

You can use the **traffic priority** command to mark the IP precedence, 802.1p priority, DSCP precedence, and local precedence of the packets.

Configuration prerequisites

The following items are defined or determined before the configuration:

- The ACL rules used for traffic classification have been specified. Refer to the ACL module of this manual for related information.
- The type and value of the precedence to be marked for the packets matching the ACL rules have been determined.
- The port or VLAN on which the configuration is to be performed has been determined.

Configuration procedure

Follow these steps to configure priority marking on a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Mark the priorities for packets matching specific ACL rules	traffic-priority { inbound outbound } <i>acl-rule</i> { { dscp <i>dscp-value</i> ip-precedence { <i>pre-value</i> from-cos } } cos { <i>pre-value</i> from-ipprec } local-precedence <i>pre-value</i> }*	Required Refer to the command manual for information about the <i>acl-rule</i> argument.

Follow these steps to configure priority marking on a VLAN:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Mark the priorities for the packets belonging to a VLAN and matching specific ACL rules	traffic-priority vlan <i>vlan-id</i> { inbound outbound } <i>acl-rule</i> { { dscp <i>dscp-value</i> ip-precedence { <i>pre-value</i> from-cos } } cos { <i>pre-value</i> from-ipprec } local-precedence <i>pre-value</i> }*	Required Refer to the command manual for information about the <i>acl-rule</i> argument.

Configuration example

- Ethernet 1/0/1 belongs to VLAN 2 and is connected to the 10.1.1.1/24 network segment.
- Mark the DSCP precedence as 56 for the packets from the 10.1.1.1/24 network segment.

1) Method I

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] traffic-priority inbound ip-group 2000 dscp 56
```

2) Method II

```
<Sysname> system-view
[Sysname] acl number 2000
```

```
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] traffic-priority vlan 2 inbound ip-group 2000 dscp 56
```

Configuring Traffic Policing

Refer to section [Traffic Policing](#) for information about traffic policing.

Configuration prerequisites

- The ACL rules used for traffic classification have been defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The rate limit for traffic policing, and the actions for the packets exceeding the rate limit have been determined.
- The ports that need this configuration have been determined.

Configuration procedure

Follow these steps to configure traffic policing:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure traffic policing	traffic-limit inbound <i>acl-rule</i> [union-effect] [egress-port <i>interface-type interface-number</i>] <i>target-rate</i> [burst-bucket <i>burst-bucket-size</i>] [exceed <i>action</i>]	Required Specify a committed information rate (CIR) for the <i>target-rate</i> argument, and specify a committed bust size (CBS) for the <i>burst-bucket-size</i> argument. By default, traffic policing is disabled.



Note

The granularity of traffic policing is 64 Kbps. If the number you input is in the range of $N \times 64$ to $(N+1) \times 64$ (N is a natural number), it will be rounded off to $(N+1) \times 64$.

Configuration example

- Ethernet 1/0/1 of the switch is connected to the 10.1.1.0/24 network segment
- Perform traffic policing on the packets from the 10.1.1.0/24 network segment, setting the rate to 128 kbps
- Mark the DSCP precedence as 56 for the inbound packets exceeding the rate limit.

Configuration procedure:

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] interface Ethernet1/0/1
```


[Sysname-Ethernet1/0/1] traffic-limit inbound ip-group 2000 128 exceed remark-dscp 56

Configuring Line Rate

Refer to section [Line Rate](#) for information about line rate.

Configuration prerequisites

- The port on which line rate configuration is to be performed has been determined.
- The target rate and the direction of rate limiting (inbound or outbound) have been determined.

Configuration procedure

Follow these steps to configure line rate:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure line rate	line-rate { inbound outbound } <i>target-rate</i> [burst-bucket <i>burst-bucket-size</i>]	Required Specify a committed information rate (CIR) for the <i>target-rate</i> argument, and specify a committed bust size (CBS) for the <i>burst-bucket-size</i> argument. By default, line rate is disabled.

Configuration example

- Configure line rate for outbound packets on Ethernet 1/0/1.
- The rate limit is 1,024 Kbps

Configuration procedure:

```
<Sysname> system-view
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] line-rate outbound 1024
```

Configuring Traffic Redirecting

Refer to section [Traffic Redirecting](#) for information about traffic redirecting.

Configuration prerequisites

- The ACL rules used for traffic classification have been defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The traffic redirecting destination has been determined.
- The ports that need this configuration have been determined.

Configuration procedure

Follow these steps to configure traffic redirecting:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure traffic redirecting	traffic-redirect { inbound outbound } <i>acl-rule</i> { cpu { interface <i>interface-type</i> <i>interface-number</i> link-aggregation-group <i>agg-id</i> } [untagged] }	Required By default, traffic redirecting is not configured.



Note

- Packets redirected to the CPU are not forwarded.
- If the traffic is redirected to a Combo port in down state, the system automatically redirects the traffic to the port corresponding to the Combo port in up state. Refer to the Port Basic Configuration module of this manual for information about Combo ports.
- If the traffic is configured to be redirected to an aggregation group, the traffic is redirected to the master port of the aggregation group. Refer to the Link Aggregation module of this manual for information about aggregation group.
- When the traffic redirecting function is used in conjunction with the selective QinQ function, you can specify the **untagged** keyword as required (that is, remove the outer VLAN tag of a packet after the packet is redirected to the uplink port) in a tree network with a single uplink port (or an aggregation group). Do not specify the **untagged** keyword in a ring network or a network with multiple uplink ports. Refer to the VLAN-VPN module of this manual for information about selective QinQ.

Configuration example

- Ethernet 1/0/1 is connected to the 10.1.1.0/24 network segment.
- Redirect all the packets from the 10.1.1.0/24 network segment to Ethernet 1/0/7.

Configuration procedure:

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] traffic-redirect inbound ip-group 2000 interface Ethernet1/0/7
```

Configuring VLAN Mapping

Refer to section [VLAN Mapping](#) for information about VLAN mapping.

Configuration prerequisites

- The ACL rules used for traffic classification have been defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The ports on which the configuration is to be performed have been determined.
- The VLAN ID to be set for the packets has been determined.

Configuration procedure

Follow these steps to configure VLAN mapping:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure VLAN mapping	traffic-mark-vlanid inbound <i>acl-rule</i> remark-vlan <i>remark-vlanid</i>	Required By default, VLAN mapping is not configured.

Configuring Queue Scheduling

Refer to section [Queue Scheduling](#) for information about queue scheduling.

Configuration prerequisites

The algorithm for queue scheduling to be used and the related parameters have been determined.

Configuration procedure

Follow these steps to configure queue scheduling in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure queue scheduling	queue-scheduler { strict-priority wfq <i>queue0-width queue1-width</i> <i>queue2-width queue3-width</i> <i>queue4-width queue5-width</i> <i>queue6-width queue7-width wrr</i> <i>queue0-weight queue1-weight</i> <i>queue2-weight queue3-weight</i> <i>queue4-weight queue5-weight</i> <i>queue6-weight queue7-weight }</i>	Required By default, the queue scheduling algorithm adopted on all the ports is WRR. The default weights of the eight output queues of a port are 1, 2, 3, 4, 5, 9, 13, and 15 (in the order queue 0 through queue 7).

Follow these steps to configure queue scheduling in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure queue scheduling	queue-scheduler { wfq <i>queue0-width queue1-width</i> <i>queue2-width queue3-width</i> <i>queue4-width queue5-width</i> <i>queue6-width queue7-width wrr</i> <i>queue0-weight queue1-weight</i> <i>queue2-weight queue3-weight</i> <i>queue4-weight queue5-weight</i> <i>queue6-weight queue7-weight }</i>	Required By default, the queue scheduling algorithm adopted on all the ports is WRR. The default weights of the eight output queues of a port are 1, 2, 3, 4, 5, 9, 13, and 15 (in the order queue 0 through queue 7).

A port of an S3600 Ethernet switch supports eight output queues. These queue scheduling algorithms are available: SP, WRR, and WFQ. With WRR (or WFQ) adopted, if you set the weight or the bandwidth of one or multiple queues to 0, the switch will add the queue or these queues to the SP group, where SP is adopted. For other queues, WRR (or WFQ) still applies. In this case, both SP and WRR (or WFQ) are adopted.

In cases where both SP and WRR (or WFQ) queue scheduling algorithms are adopted, the queues in the SP group take precedence over other queues. For example, if queue 0, queue 1, queue 2, and queue 3 are in the SP group, queue 4, queue 5, queue 6, and queue 7 are scheduled using WRR (or WFQ), the switch will schedule the queues in the SP group preferentially by using the SP algorithm. Then queues outside the SP group are scheduled by using WRR (or WFQ) algorithm only when all the queues in the SP group are empty.



Note

- The queue scheduling algorithm specified by using the **queue-scheduler** command in system view takes effect on all the ports. The queue scheduling algorithm configured in port view must be the same as that configured in system view. Otherwise, the system prompts configuration errors.
 - If the weight (or bandwidth value) specified in system view for a queue of WRR queuing or WFQ queuing cannot meet the requirement of a port, you can modify the weight (or bandwidth value) for this port in the corresponding Ethernet port view. The new weight (or bandwidth value) takes effect only on the port.
 - If the weight (or bandwidth value) specified in system view for a queue of SP-WRR queuing or SP-WFQ queuing in the command cannot meet the requirement of a port, you can modify the weight (or bandwidth value) for this port in the corresponding Ethernet port view. The new weight (or bandwidth value) takes effect only on the port.
 - The **display queue-scheduler** command cannot display the queue weight (or bandwidth value) specified in Ethernet port view.
-

Configuration example

- Adopts WRR for queue scheduling, setting the weights of the output queues to 2, 2, 3, 3, 4, 4, 5, and 5 (in the order queue 0 through queue 7).
- Verify the configuration.

Configuration procedure:

```
<Sysname> system-view
[Sysname] queue-scheduler wrr 2 2 3 3 4 4 5 5
[Sysname] 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

Configuring WRED

Refer to section [Congestion Avoidance](#) for information about WRED.

Configuration prerequisites

- The indexes of queues to be dropped at random, the queue length that starts the drop action, and the drop probability have been determined.
- The ports that need this configuration have been determined.

Configuration procedure

Follow these steps to configure WRED:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure WRED	wred <i>queue-index</i> <i>qstart</i> <i>probability</i>	Required By default, WRED is not configured.

Configuration example

Configure WRED for queue 2 of Ethernet 1/0/1 to drop the packets in queue 2 randomly when the number of packets in queue 2 exceeds 64, setting the dropping probability being 20%.

Configuration procedure:

```
<Sysname> system-view
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] wred 2 64 20
```

Configuring Traffic Accounting

Refer to section [Flow-based Traffic Accounting](#) for information about traffic accounting.

Configuration prerequisites

- The ACL rules for traffic classification have been defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The port that needs this configuration has been determined.

Configuration procedure

Follow these steps to configure traffic accounting:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—

To do...	Use the command...	Remarks
Configure traffic accounting	traffic-statistic inbound <i>acl-rule</i>	Required By default, traffic accounting is disabled.
Clear the traffic statistics	reset traffic-statistic inbound <i>acl-rule</i>	Required

Configuration example

- Ethernet 1/0/1 is connected to the 10.1.1.0/24 network segment.
- Perform traffic accounting on the packets sourced from the 10.1.1.0/24 network segment.
- Clear the traffic statistics.

Configuration procedure:

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] traffic-statistic inbound ip-group 2000
[Sysname-Ethernet1/0/1] reset traffic-statistic inbound ip-group 2000
```

Enabling the Burst Function

Refer to section [Burst](#) for information about the burst function.

Configuration prerequisites

You have determined that the burst function is required.

Configuration procedure

Follow these steps to enable the burst function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the burst function	burst-mode enable	Required By default, the burst function is disabled.



Caution

With the IRF function enabled, do not enable the burst function. Otherwise, packets may be forwarded improperly. Refer to the IRF Fabric part for the detailed information about IRF.

Configuring Traffic Mirroring

Refer to section [Traffic mirroring](#) for information about traffic mirroring.

Configuration prerequisites

- The ACL rules for traffic classification have been defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The source mirroring ports and mirroring direction have been determined.
- The destination mirroring port has been determined.

Configuration procedure

Follow these steps to configure traffic mirroring:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enter Ethernet port view		interface <i>interface-type</i> <i>interface-number</i>	—
Configure the current port as a source mirroring port		mirrored-to { inbound outbound } <i>acl-rule</i> { monitor-interface cpu }	Required Omit the following steps if you redirect traffic to the CPU. Proceed to the following steps if you redirect traffic to a port.
Quit to system view		quit	—
Configure the specified port as the destination mirroring port	In system view	mirroring-group <i>group-id</i> monitor-port <i>monitor-port-id</i>	Required Use either approach.
	In Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	
		monitor-port	



Note

For information about the **mirroring-group monitor-port** command and the **monitor-port** command, refer to the part talking about mirroring.

Configuration example

Network requirements:

- Ethernet 1/0/1 is connected to the 10.1.1.0/24 network segment.
- Duplicate the packets from network segment 10.1.1.0/24 to the destination mirroring port Ethernet 1/0/4.

Configuration procedure:

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] interface Ethernet1/0/4
```

```
[Sysname-Ethernet1/0/4] monitor-port
[Sysname-Ethernet1/0/4] quit
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] mirrored-to inbound ip-group 2000 monitor-interface
```

Displaying and Maintaining QoS

To do...	Use the command...	Remarks
Display the mapping between 802.1p priority and local precedence	display qos cos-local-precedence-map	Available in any view
Display the priority marking configuration	display qos-interface { <i>interface-type</i> <i>interface-number</i> <i>unit-id</i> } traffic-priority	
Display the protocol packet priority configuration	display protocol-priority	
Display line rate configuration	display qos-interface { <i>interface-type</i> <i>interface-number</i> <i>unit-id</i> } line-rate	
Display traffic policing configuration	display qos-interface { <i>interface-type</i> <i>interface-number</i> <i>unit-id</i> } traffic-limit	
Display traffic redirecting configuration	display qos-interface { <i>interface-type</i> <i>interface-number</i> <i>unit-id</i> } traffic-redirect	
Display VLAN mapping configuration	display qos-interface { <i>interface-type</i> <i>interface-number</i> <i>unit-id</i> } traffic-remark-vlanid	
Display queue scheduling configuration	display queue-scheduler	
Display traffic accounting configuration	display qos-interface { <i>interface-type</i> <i>interface-number</i> <i>unit-id</i> } traffic-statistic	
Display traffic mirroring configuration	display qos-interface { <i>interface-type</i> <i>interface-number</i> <i>unit-id</i> } mirrored-to	
Display all the QoS configuration	display qos-interface { <i>interface-type</i> <i>interface-number</i> <i>unit-id</i> } all	

QoS Configuration Examples

Configuration Example of Traffic policing and Line Rate

Network requirement

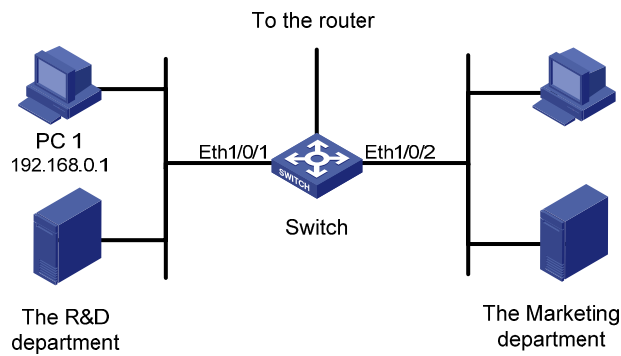
An enterprise network connects all the departments through an Ethernet switch. PC 1, with the IP address 192.168.0.1 belongs to the R&D department and is connected to Ethernet 1/0/1 of the switch. The marketing department is connected to Ethernet 1/0/2 of the switch.

Configure traffic policing and line rate to satisfy the following requirements:

- Set the maximum rate of outbound packets sourced from the marketing department to 64 kbps. Drop the packets exceeding the rate limit.
- Set the maximum rate of outbound IP packets sent by PC 1 in the R&D department to 640 kbps. Drop the packets exceeding the rate limit.

Network diagram

Figure 1-9 Network diagram for traffic policing and rate limiting configuration



Configuration procedure

1) Define an ACL for traffic classification.

Create ACL 2000 and enter basic ACL view.

```
<Sysname> system-view
```

```
[Sysname] acl number 2000
```

Define a rule for the packets with 192.168.0.1 as the source IP address.

```
[Sysname-acl-basic-2000] rule permit source 192.168.0.1 0
```

```
[Sysname-acl-basic-2000] quit
```

2) Configure traffic policing and rate limiting

Set the maximum rate of outbound packets sourced from the marketing department to 64 kbps.

```
[Sysname] interface Ethernet1/0/2
```

```
[Sysname-Ethernet1/0/2] line-rate inbound 64
```

```
[Sysname-Ethernet1/0/2] quit
```

Set the maximum rate of outbound IP packets sent by PC 1 in the R&D department to 640 kbps.

```
[Sysname] interface Ethernet1/0/1
```

```
[Sysname-Ethernet1/0/1] traffic-limit inbound ip-group 2000 640 exceed drop
```

Configuration Example of Priority Marking and Queue Scheduling

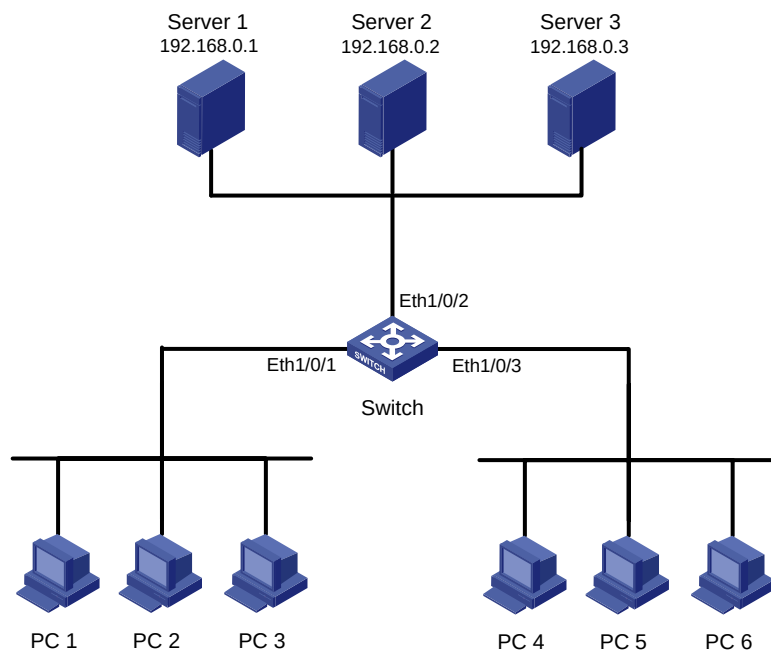
Network requirements

As shown in [Figure 1-10](#), an enterprise network connects all the departments through an Ethernet switch. Clients PC 1 through PC 3 are connected to Ethernet 1/0/1 of the switch; clients PC 4 through PC 6 are connected to Ethernet 1/0/3 of the switch. Server 1 (the database server), Server 2 (the mail server), and Server 3 (the file server) are connected to Ethernet 1/0/2 of the switch.

Configure priority marking and queue scheduling on the switch to mark traffic flows accessing Server 1, Server 2, and Server 3 with different priorities respectively and assign the three traffic flows to different queues for scheduling.

Network diagram

Figure 1-10 Network diagram for priority marking and queue scheduling configuration



Configuration procedure

1) Define an ACL for traffic classification

Create ACL 3000 and enter advanced ACL view.

```
<Sysname> system-view
```

```
[Sysname] acl number 3000
```

Define ACL rules for identifying packets based on destination IP addresses.

```
[Sysname-acl-adv-3000] rule 0 permit ip destination 192.168.0.1 0
```

```
[Sysname-acl-adv-3000] rule 1 permit ip destination 192.168.0.2 0
```

```
[Sysname-acl-adv-3000] rule 2 permit ip destination 192.168.0.3 0
```

```
[Sysname-acl-adv-3000] quit
```

2) Configure priority marking

Mark priority for packets received through Ethernet 1/0/2 and matching ACL 3000.

```
[Sysname] interface Ethernet1/0/2
```

```
[Sysname-Ethernet1/0/2] traffic-priority inbound ip-group 3000 rule 0 local-precedence 4
```

```
[Sysname-Ethernet1/0/2] traffic-priority inbound ip-group 3000 rule 1 local-precedence 3
```

```
[Sysname-Ethernet1/0/2] traffic-priority inbound ip-group 3000 rule 2 local-precedence 2
```

```
[Sysname-Ethernet1/0/2] quit
```

3) Configure queue scheduling

Apply SP queue scheduling algorithm.

```
[Sysname] queue-scheduler strict-priority
```

VLAN Mapping Configuration Example

Network requirements

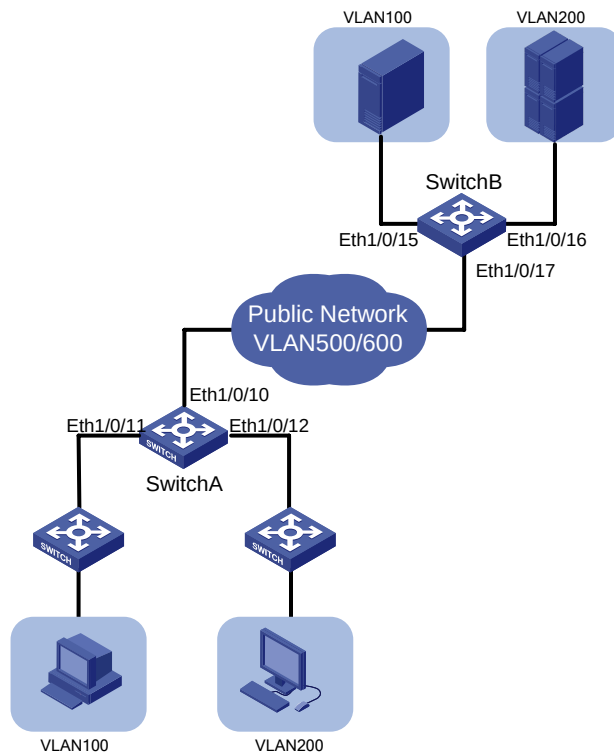
Two customer networks are connected to the public network through Switch A and Switch B. Configure the VLAN mapping function on the switches to enable the hosts on the two customer networks to communicate through public network VLANs.

- Switch A provides network access for terminal devices in VLAN 100 and VLAN 200 through Ethernet 1/0/11 and Ethernet 1/0/12. On the other side of the public network, Switch B provides network access for servers in VLAN 100 and VLAN 200 through Ethernet 1/0/15 and Ethernet 1/0/16.
- Switch A provides access to the public network through Ethernet 1/0/10 and Switch B provides access to the public network through Ethernet 1/0/17.

Configure the switches to have packets of VLAN 100 and packets of VLAN 200 transmitted in VLAN 500 and VLAN 600 across the public network.

Network diagram

Figure 1-11 Network diagram for VLAN mapping configuration



Configuration procedure

Create customer VLANs VLAN 100 and VLAN 200 and service VLANs VLAN 500 and VLAN 600 on Switch A.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] quit
[SwitchA] vlan 200
[SwitchA-vlan200] quit
```

```
[SwitchA] vlan 500
[SwitchA-vlan500] quit
[SwitchA] vlan 600
[SwitchA-vlan600] quit
```

Configure Ethernet 1/0/11 of Switch A as a trunk port and configure its default VLAN as VLAN 100. Assign Ethernet 1/0/11 to VLAN 100 and VLAN 500. Configure Ethernet 1/0/12 in the same way.

```
[SwitchA] interface Ethernet 1/0/11
[SwitchA-Ethernet1/0/11] port link-type trunk
[SwitchA-Ethernet1/0/11] port trunk pvid vlan 100
[SwitchA-Ethernet1/0/11] port trunk permit vlan 100 500
[SwitchA-Ethernet1/0/11] quit
[SwitchA] interface Ethernet 1/0/12
[SwitchA-Ethernet1/0/12] port link-type trunk
[SwitchA-Ethernet1/0/12] port trunk pvid vlan 200
[SwitchA-Ethernet1/0/12] port trunk permit vlan 200 600
[SwitchA-Ethernet1/0/12] quit
```

Configure Ethernet 1/0/10 of Switch A as a trunk port, and assign it to VLAN 100, VLAN 200, VLAN 500, and VLAN 600.

```
[SwitchA] interface Ethernet 1/0/10
[SwitchA-Ethernet1/0/10] port link-type trunk
[SwitchA-Ethernet1/0/10] port trunk permit vlan 100 200 500 600
[SwitchA-Ethernet1/0/10] quit
```

Configure Layer-2 ACLs on Switch A. Configure ACL 4000 to permit packets from VLAN 100, ACL 4001 to permit packets from VLAN 200, ACL 4002 to permit packets from VLAN 500, and ACL 4003 to permit packets from VLAN 600.

```
[SwitchA] acl number 4000
[SwitchA-acl-ethernetframe-4000] rule permit source 100
[SwitchA] quit
[SwitchA] acl number 4001
[SwitchA-acl-ethernetframe-4001] rule permit source 200
[SwitchA] quit
[SwitchA] acl number 4002
[SwitchA-acl-ethernetframe-4002] rule permit source 500
[SwitchA] quit
[SwitchA] acl number 4003
[SwitchA-acl-ethernetframe-4003] rule permit source 600
[SwitchA] quit
```

Configure VLAN mapping on Ethernet 1/0/11 to replace VLAN tag 100 with VLAN tag 500.

```
[SwitchA] interface Ethernet 1/0/11
[SwitchA-Ethernet1/0/11] traffic-remark-vlanid inbound link-group 4000 remark-vlan 500
[SwitchA-Ethernet1/0/11] quit
```

Configure VLAN mapping on Ethernet 1/0/12 to replace VLAN tag 200 with VLAN tag 600.

```
[SwitchA] interface Ethernet 1/0/12
[SwitchA-Ethernet1/0/12] traffic-remark-vlanid inbound link-group 4001 remark-vlan 600
[SwitchA-Ethernet1/0/12] quit
```

Configure VLAN mapping on Ethernet 1/0/10 to replace VLAN tag 500 with VLAN tag 100 and replace VLAN tag 600 with VLAN tag 200.

```
[SwitchA] interface Ethernet 1/0/10
[SwitchA-Ethernet1/0/10] traffic-remark-vlanid inbound link-group 4002 remark-vlan 100
[SwitchA-Ethernet1/0/10] traffic-remark-vlanid inbound link-group 4003 remark-vlan 200
[SwitchA-Ethernet1/0/10] quit
```

Define the same VLAN mapping rules on Switch B. The detailed configuration procedure is similar to that of Switch A and thus is omitted here.

Configuring Traffic Mirroring and Redirecting Traffic to a Port

Network Requirements

A company uses a switch to interconnect all the departments. As shown in [Figure 1-12](#),

- The marketing department is connected to Ethernet 1/0/1 of the switch. The IP address segment for the hosts of the marketing department is 192.168.1.0/25, and the hosts access the Internet through the switch.
- The R&D department is connected to Ethernet 1/0/2 of the switch. The IP address segment for the hosts of the R&D department is 192.168.2.0/25, and the hosts access the Internet through the switch.
- The data monitoring device is connected to Ethernet 1/0/3 of the switch.

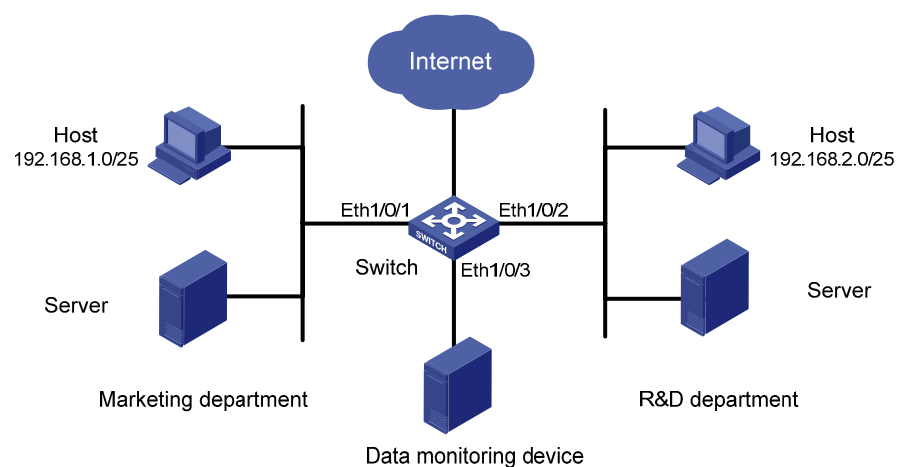
Configure traffic redirecting and traffic mirroring to satisfy the following requirements:

- From 8:00 to 18:00 in working days, mirror the HTTP traffic from the marketing department to the Internet to the data monitoring device.
- From 8:00 to 18:00 in working days, redirect the HTTP traffic from the R&D department to the Internet to the data monitoring device.

On the data monitoring device, the network administrator can analyze the HTTP traffic from each department to the Internet.

Network diagram

Figure 1-12 Network diagram for traffic redirecting and traffic mirroring configuration



Configuration procedure

- 1) Define a time range for working days

Create a time range **trname** covering the period from 8:00 to 18:00 during working days.

```
<Switch> system-view
```

```
[Switch] time-range trname 8:00 to 18:00 working-day
```

2) Configure a policy for the traffic of the marketing department

Create basic ACL 2000 to permit the traffic of the hosts in the marketing department during the specified time range.

```
[Switch] acl number 2000
```

```
[Switch-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.127 time-range trname
```

```
[Switch-acl-basic-2000] quit
```

Configure to mirror traffic matching ACL 2000 to Ethernet 1/0/3.

```
[Switch] interface ethernet 1/0/1
```

```
[Switch-Ethernet1/0/1] mirrored-to inbound ip-group 2000 monitor-interface
```

```
[Switch-Ethernet1/0/1] quit
```

```
[Switch] interface ethernet 1/0/3
```

```
[Switch-Ethernet1/0/3] monitor-port
```

```
[Switch-Ethernet1/0/3] quit
```

3) Configure a policy for the traffic of the R&D department

Create basic ACL 2001 to permit the traffic of the hosts in the R&D department during the specified time range.

```
[Switch] acl number 2001
```

```
[Switch-acl-basic-2001] rule permit source 192.168.2.0 0.0.0.127 time-range trname
```

```
[Switch-acl-basic-2001] quit
```

Configure to redirect traffic matching ACL 2001 to Ethernet 1/0/3.

```
[Switch] interface ethernet 1/0/2
```

```
[Switch-Ethernet1/0/2] traffic-redirect inbound ip-group 2001 interface Ethernet 1/0/3
```

2 QoS Profile Configuration

When configuring QoS profile, go to these sections for information you are interested in:

- [Overview](#)
- [QoS Profile Configuration Task List](#)
- [Displaying and Maintaining QoS Profile Configuration](#)
- [Configuration Example](#)

Overview

Introduction to QoS Profile

QoS profile is a set of QoS configurations. It provides an easy way for performing and managing QoS configuration. A QoS profile can contain one or multiple QoS actions. In networks where hosts change their positions frequently, you can define QoS policies for the specific hosts and add the QoS policies to a QoS profile. When a host is connected to another port of a switch, you can simply apply the corresponding QoS profile to the port statically or dynamically to maintain the same QoS configuration performed for the host.

Currently, a QoS profile can contain configurations concerning packet filtering, traffic policing, and priority marking.

QoS Profile Application Mode

Dynamic application mode

A QoS profile can be applied dynamically to a user or a group of users passing 802.1x authentication. To apply QoS profiles dynamically, a user name-to-QoS profile mapping table is required on the AAA server. For a switch operating in this mode, after a user passes the 802.1x authentication, the switch looks up the user name-to-QoS profile mapping table for the QoS profile using the user name and then applies the QoS profile found to the port the user is connected to.

Corresponding to the 802.1x authentication modes, dynamic QoS profile application can be user-based and port-based.

- User-based QoS profile application

The switch generates a new QoS profile by adding user source MAC address information to the identifying rule defined in the existing QoS profile and then applies the new QoS profile to the port the user is connected to.

- Port-based QoS profile application

The switch directly applies the QoS profile to the port the user is connected to.



Note

A user-based QoS profile application fails if the traffic classification rule defined in the QoS profile contains source address information (including source MAC address information, source IP address information, and VLAN information).

Manual application mode

You can use the **apply** command to manually apply a QoS profile to a port.

QoS Profile Configuration Task List

Complete the following tasks to configure QoS profile:

Operation	Description
Configuring a QoS Profile	Required
Applying a QoS Profile	Optional

Configuring a QoS Profile

Configuration prerequisites

- The ACL rules used for traffic classification are defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The type and number of actions in the QoS profile are specified.

Configuration procedure

Follow these steps to configure a QoS profile:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a QoS profile and enter QoS profile view	qos-profile <i>profile-name</i>	Required If the specified QoS profile already exists, you enter the QoS profile view directly.
Configure traffic policing	traffic-limit inbound <i>acl-rule</i> [union-effect] [egress-port <i>interface-type interface-number</i>] <i>target-rate</i> [burst-bucket <i>burst-bucket-size</i>] [exceed <i>action</i>]	Optional
Configure packet filtering	packet-filter { inbound outbound } <i>acl-rule</i>	Optional Refer to the ACL module of this manual for information about packet filtering.

To do...	Use the command...	Remarks
Configure priority marking	traffic-priority { inbound outbound } acl-rule { { dscp <i>dscp-value</i> ip-precedence { <i>pre-value</i> from-cos } } cos { <i>pre-value</i> from-ipprec } local-precedence <i>pre-value</i> }*	Optional

Applying a QoS Profile

You can configure to apply a QoS profile dynamically or simply apply a QoS profile manually.

Configuration prerequisites

- To configure to apply a QoS profile dynamically, make sure 802.1x is enabled both globally and on the port, and the authentication mode is determined. For information about 802.1x, refer to the 802.1x and System Guard module of this manual.
- To apply a QoS profile manually, make sure the port to which the QoS profile is to be applied is determined.
- The QoS profile to be applied is determined.

Configuration procedure

Follow these steps to configure to apply a QoS profile dynamically:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Specify the mode to apply a QoS profile	Configure the mode to apply a QoS profile as port-based	Optional By default, the mode to apply a QoS profile is user-based. • If the 802.1x authentication mode is MAC address-based, the mode to apply a QoS profile must be configured user-based. • If the 802.1x authentication mode is port-based, the mode to apply a QoS profile must be configured as port-based.
	Configure the mode to apply a QoS profile as user-based	

Follow these steps to apply a QoS profile manually:

To do...			Use the command...	Remarks
Enter system view			system-view	—
Apply a QoS profile to specific ports	In system view		apply qos-profile <i>profile-name</i> interface <i>interface-list</i>	Select either of the operations. By default, a port has no QoS profile applied to it.
	In Ethernet port view	Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	
		Apply a QoS profile to the current port	apply qos-profile <i>profile-name</i>	

Displaying and Maintaining QoS Profile Configuration

To do...	Use the command...	Remarks
Display QoS profile configuration	display qos-profile { all name <i>profile-name</i> interface <i>interface-type</i> <i>interface-number</i> user <i>user-name</i> }	Available in any view

Configuration Example

QoS Profile Configuration Example

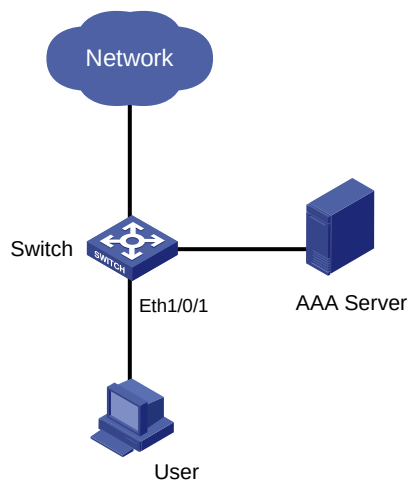
Network requirements

All departments of a company are interconnected through a switch. The 802.1x protocol is used to authenticate users and control their access to network resources. A user name is **someone**, and the authentication password is **hello**. It is connected to Ethernet 1/0/1 of the switch and belongs to the test.net domain.

It is required to configure a QoS profile to limit the rate of all the outbound IP packets of the user to 128 kbps and configuring to drop the packets exceeding the target packet rate.

Network diagram

Figure 2-1 Network diagram for QoS profile configuration



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. Refer to the user manual of the AAA server for detailed configuration.

2) Configuration on the switch

Configure IP addresses for the RADIUS server.

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] primary authentication 10.11.1.1
```

```
[Sysname-radius-radius1] primary accounting 10.11.1.2
```

```
[Sysname-radius-radius1] secondary authentication 10.11.1.2
```

```
[Sysname-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.

```
[Sysname-radius-radius1] key authentication money
```

```
[Sysname-radius-radius1] key accounting money
```

Configure the switch to delete the user domain name from the user name and then send the user name to the RADIUS sever.

```
[Sysname-radius-radius1] user-name-format without-domain
```

```
[Sysname-radius-radius1] quit
```

Create the user domain test.net and specify radius1 as your RADIUS server group.

```
[Sysname] domain test.net
```

```
[Sysname-isp-test.net] radius-scheme radius1
```

```
[Sysname-isp-test.net] quit
```

Create ACL 3000 to permit IP packets destined for any IP address.

```
[Sysname] acl number 3000
```

```
[Sysname-acl-adv-3000] rule 1 permit ip destination any
```

```
[Sysname-acl-adv-3000] quit
```

Define a QoS profile named "example" to limit the rate of matched packets to 128 kbps and configuring to drop the packets exceeding the target packet rate.

```
[Sysname] qos-profile example
```

```
[Sysname-qos-profile-example] traffic-limit inbound ip-group 3000 128 exceed drop
```

Enable 802.1x.

```
[Sysname] dot1x
```

```
[Sysname] dot1x interface Ethernet 1/0/1
```

After the configuration, the QoS profile named **example** will be applied to the user with user name **someone** automatically after the user passes the authentication.

Table of Contents

1 Web Cache Redirection Configuration	1-1
Web Cache Redirection Overview	1-1
Web Cache Redirection Configuration	1-2
Configuration Prerequisites	1-2
Configuration Procedure	1-2
Displaying Web Cache Redirection Configuration	1-3
Web Cache Redirection Configuration Example	1-3
Configuration Example	1-3

1 Web Cache Redirection Configuration

When configuring Web cache redirection, go to these sections for information you are interested in:

- [Web Cache Redirection Overview](#)
- [Web Cache Redirection Configuration](#)
- [Displaying Web Cache Redirection Configuration](#)
- [Web Cache Redirection Configuration Example](#)



Note

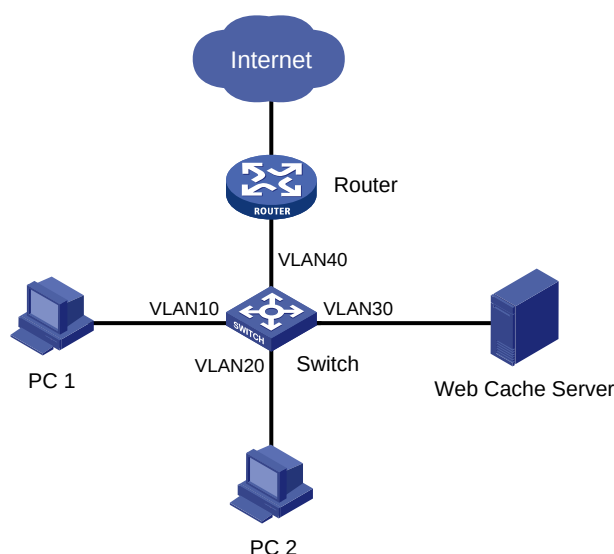
Web cache redirection is available on S3600-EI series switches only.

Web Cache Redirection Overview

Usually, users access Web pages through Hypertext Transfer Protocol (HTTP). Typically, users connect to the Internet through LANs. For LANs containing large amount of users of the Internet, HTTP traffics may congest the links between the LANs and the Internet and may even affect the operation of other services. Web cache server can relieve the HTTP load on the links connecting LANs and the Internet and improve the speed of users' obtaining information from the Internet.

The Web cache redirection function provided by S3600-EI series Ethernet switches can redirect the HTTP traffic to Web cache servers, as illustrated in [Figure 1-1](#).

Figure 1-1 A Web cache redirection implementation



As shown in [Figure 1-1](#), PC 1 and PC 2 are hosts in a LAN connected to the switch, which belong to VLAN 10 and VLAN 20 respectively. The gateway address of PC 1 is set to the IP address of

VLAN-interface 10; the gateway address of PC 2 is set to the IP address of VLAN-interface 20. Web Cache Server is used to store the information from the Internet that is frequently accessed by the users in the LAN. It belongs to VLAN 30. The switch connects to the router through VLAN 40. Normally, HTTP traffic of PC 1 and PC 2 are forwarded through VLAN 40 to the router, which then sends the traffic to the Internet. By enabling Web cache redirection function on the switch, HTTP traffic of PC 1 and PC 2 is redirected to Web Cache Server through VLAN 30.

When a user in the LAN accesses the Internet,

- If the information requested is already stored in Web Cache Server, the Web Cache Server sends the information to the user directly, thus eliminating the access to the Internet.
- If Web Cache Server does not contain the information requested, it retrieves the information from the Internet and then forwards the information to the user.

If both the Web cache redirection function and the STP function are configured on the switch, to avoid Web cache redirection failure, you are recommended to configure the port connecting with the Web Cache Server as a Trunk or Hybrid port that permits the packets of the VLAN used for HTTP traffic transmission, VLAN 40 in [Figure 1-1](#) for example.

Web Cache Redirection Configuration

Configuration Prerequisites

- The route between the switch and the Web cache server is reachable, and the Web cache function is enabled on the Web cache server.
- The IP address and MAC address of the Web cache server and the VLANs whose HTTP traffic is to be redirected to the Web cache are configured.
- The port through which the switch is connected to the Web cache server and TCP port number used by HTTP are determined.

Configuration Procedure

You can configure Web cache redirection in system view or Ethernet port (connecting with the Web cache server) view.

Follow these steps to configure Web cache redirection in system view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure Web cache server parameters	webcache address <i>ip-address</i> mac <i>mac-address</i> vlan <i>vlan-id</i> port <i>interface-type</i> <i>interface-number</i> [tcpport <i>tcpport-number</i>]	Required Not configured by default.
Specify a VLAN whose HTTP traffic is to be redirected to the Web cache server	webcache redirect-vlan <i>vlan-id</i>	Required By default, no HTTP packet is redirected to the Web cache server.

Follow these steps to configure Web cache redirection in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure Web cache server parameters	webcache address <i>ip-address</i> mac <i>mac-address</i> vlan <i>vlan-id</i> [tcpport <i>tcpport-number</i>]	Required Not configured by default.
Quit to system view	quit	—
Specify a VLAN whose HTTP traffic is to be redirected to the Web cache server	webcache redirect-vlan <i>vlan-id</i>	Required By default, no HTTP packet is redirected to the Web cache server.



Note

- Make sure the route between the switch and Web cache server is reachable for the Web cache redirection function to take effect.
- A switch can have only one Web cache server configured. That is, a newly configured Web cache server replaces the existing one.
- Make sure both the interface of the VLAN that the Web cache server belongs to and that of the VLAN whose HTTP traffic is to be redirected are up for the Web cache redirection to take effect.
- A switch does not support to redirect the HTTP traffic of the VLAN where the Web cache server resides to the Web cache server.

Displaying Web Cache Redirection Configuration

To do...	Use the command...	Remarks
Display Web cache redirection configuration and the status of the Web cache	display webcache	Available in any view.

Web Cache Redirection Configuration Example

Configuration Example

Networking requirements

The network of a company is organized as follows.

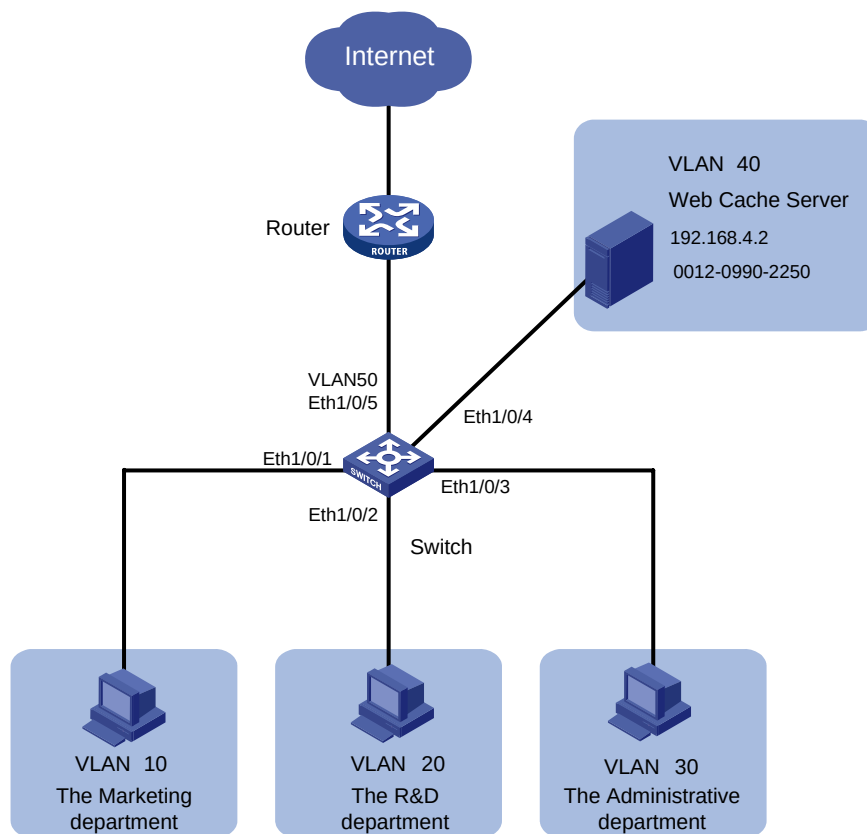
- The market department belongs to VLAN 10 and is connected to port Ethernet 1/0/1 of the switch. The IP address of VLAN 10 interface is 192.168.1.1/24.
- The R&D department belongs to VLAN 20 and is connected to port Ethernet 1/0/2 of the switch. The IP address of VLAN 20 interface is 192.168.2.1/24.

- The administrative department belongs to VLAN 30 and is connected to port Ethernet 1/0/3 of the switch. The IP address of VLAN 30 interface is 192.168.3.1/24.
- The WEB Cache Server, with the IP address 192.168.4.2 and the MAC address 0012-0990-2250, belongs to VLAN 40 and is connected to port Ethernet 1/0/4 of the switch. The IP address of VLAN 40 interface is 192.168.4.1/24.
- The switch is connected to the router through port Ethernet 1/0/5 and accesses the Internet through the router. Ethernet 1/0/5 belongs to VLAN 50. The IP address of VLAN 50 interface is 192.168.5.1/24.

The WEB Cache redirection function is enabled on the switch, and all the packets of the market department, R&D department, and administrative department are redirected to the WEB Cache Server, so as to relieve the load from the connection links of the WAN, and improve the speed of Internet access.

Networking diagram

Figure 1-2 Networking diagram for Web cache redirection configuration



Configuration procedure

Create VLAN 10 for the market department, and assign an IP address 192.168.1.1 to the VLAN-interface 10.

```

<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] port Ethernet 1/0/1
[Sysname-vlan10] quit
[Sysname] interface Vlan-interface 10
[Sysname-Vlan-interface10] ip address 192.168.1.1 24
  
```

```

[Sysname-Vlan-interface10] quit

# Create VLAN 20 for the R&D department, and assign an IP address 192.168.2.1 to the
VLAN-interface 20.

[Sysname] vlan 20
[Sysname-vlan20] port Ethernet 1/0/2
[Sysname-vlan20] quit
[Sysname] interface Vlan-interface 20
[Sysname-Vlan-interface20] ip address 192.168.2.1 24
[Sysname-Vlan-interface20] quit

# Create VLAN 30 for the administrative department, and assign an IP address 192.168.3.1 to the
VLAN-interface 30.

[Sysname] vlan 30
[Sysname-vlan30] port Ethernet 1/0/3
[Sysname-vlan30] quit
[Sysname] interface Vlan-interface 30
[Sysname-Vlan-interface30] ip address 192.168.3.1 24
[Sysname-Vlan-interface30] quit

# Create VLAN 40 for the WEB Cache Server, and assign an IP address 192.168.4.1 to the
VLAN-interface 40.

[Sysname] vlan 40
[Sysname-vlan40] quit
[Sysname] interface Vlan-interface 40
[Sysname-Vlan-interface40] ip address 192.168.4.1 24
[Sysname-Vlan-interface40] quit

# Create VLAN 50 for the switch to connect to the router, and assign an IP address 192.168.5.1 to
VLAN-interface 50.

[Sysname] vlan 50
[Sysname-vlan50] port Ethernet 1/0/5
[Sysname-vlan50] quit
[Sysname] interface Vlan-interface 50
[Sysname-Vlan-interface50] ip address 192.168.5.1 24
[Sysname-Vlan-interface50] quit

# Configure port Ethernet 1/0/4 (through which the switch connects to the Web Cache Server) as a
Trunk port, and configure the port to allow the packets of VLAN 40 and VLAN 50 to pass through.

[Sysname] interface Ethernet 1/0/4
[Sysname-Ethernet1/0/4] port link-type trunk
[Sysname-Ethernet1/0/4] port trunk permit vlan 40 50
[Sysname-Ethernet1/0/4] quit

# Enable the WEB Cache redirection function, and redirect all the HTTP packets received on VLAN 10,
VLAN 20 and VLAN 30 to the WEB Cache Server.

[Sysname] webcache address 192.168.4.2 mac 0012-0990-2250 vlan 40 port Ethernet 1/0/4
[Sysname] webcache redirect-vlan 10
[Sysname] webcache redirect-vlan 20
[Sysname] webcache redirect-vlan 30

```

Table of Contents

1 Mirroring Configuration	1-1
Mirroring Overview	1-1
Local Port Mirroring	1-1
Remote Port Mirroring	1-2
Traffic Mirroring	1-3
Port Mirroring – STP Collaboration Overview	1-3
Mirroring Configuration.....	1-4
Configuring Local Port Mirroring.....	1-4
Configuring Remote Port Mirroring.....	1-6
Displaying and Maintaining Port Mirroring	1-9
Mirroring Configuration Examples.....	1-10
Local Port Mirroring Configuration Example.....	1-10
Remote Port Mirroring Configuration Example	1-11

1 Mirroring Configuration

When configuring mirroring, go to these sections for information you are interested in:

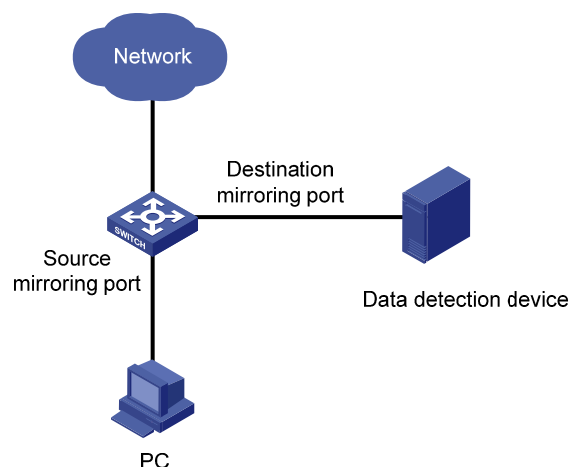
- [Mirroring Overview](#)
- [Mirroring Configuration](#)
- [Displaying and Maintaining Port Mirroring](#)
- [Mirroring Configuration Examples](#)

Mirroring Overview

Mirroring is to duplicate packets from a port to another port connected with a data monitoring device for network monitoring and diagnosis.

The port where packets are duplicated is called the source mirroring port or monitored port and the port to which duplicated packets are sent is called the destination mirroring port or the monitor port, as shown in the following figure.

Figure 1-1 Mirroring



The S3600 series Ethernet switches support three types of port mirroring:

- [Local Port Mirroring](#)
- [Remote Port Mirroring](#)
- [Traffic Mirroring](#)

They are described in the following sections.

Local Port Mirroring

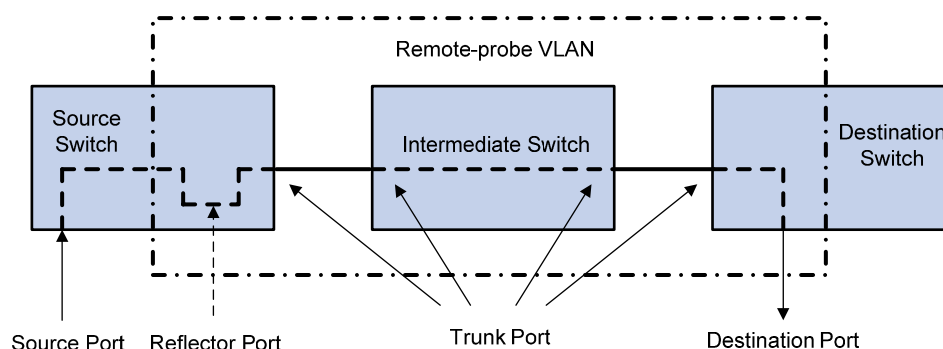
In local port mirroring, packets passing through one or more source ports of a device are copied to the destination port on the same device for packet analysis and monitoring. In this case, the source ports and the destination port must be located on the same device.

Remote Port Mirroring

Remote port mirroring does not require the source and destination ports to be on the same device. The source and destination ports can be located on multiple devices across the network. This allows an administrator to monitor traffic on remote devices conveniently.

To implement remote port mirroring, a special VLAN, called remote-probe VLAN, is used. All mirrored packets are sent from the reflector port of the source switch to the monitor port on the destination switch through the remote-probe VLAN. [Figure 1-2](#) illustrates the implementation of remote port mirroring.

Figure 1-2 Remote port mirroring application



The switches involved in remote port mirroring function as follows:

- Source switch

The source switch is the device where the monitored port is located. It copies traffic passing through the monitored port to the reflector port. The reflector port then transmits the traffic to an intermediate switch (if any) or destination switch through the remote-probe VLAN.

- Intermediate switch

Intermediate switches are 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 through the remote-probe VLAN. No intermediate switch is present if the source and destination switches directly connect to each other.

- Destination switch

The destination switch is where the monitor port is located. The destination switch forwards the 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 packets to the reflector port through local port mirroring. There can be more than one source port.
	Reflector port	Receives packets from the source port and broadcasts the packets in the remote-probe VLAN.
	Trunk port	Sends mirrored packets to the intermediate switch or the destination switch.

Switch	Ports involved	Function
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.
Destination switch	Trunk port	Receives remote mirrored packets.
	Destination port	Receives packets forwarded from the trunk port and transmits the packets to the data detection device.



Caution

- Do not configure a default VLAN, a management VLAN, or a dynamic VLAN as the remote-probe VLAN.
- Configure all ports connecting the devices in the remote-probe VLAN as trunk ports, and ensure the Layer 2 connectivity from the source switch to the destination switch over the remote-probe VLAN.
- Do not configure a Layer 3 interface for the remote-probe VLAN, run other protocol packets, or carry other service packets on the remote-probe VLAN and do not use the remote-probe VLAN as the voice VLAN and protocol VLAN; otherwise, remote port mirroring may be affected.

Traffic Mirroring

Traffic mirroring uses ACL to monitor traffic that matches certain criteria on a specific port. Unlike port mirroring where all inbound/outbound traffic passing through a port is monitored, traffic mirroring provides a finer monitoring granularity. For detailed configuration about traffic mirroring, refer to *QoS-QoS Profile Operation*.

Port Mirroring – STP Collaboration Overview

In a LAN, STP or MSTP is usually used to eliminate loops. Configurations or network topology changes may cause some ports to transit to Discarding state. A port in Discarding state cannot send or receive packets except BPDUs. If such a port is configured as a mirroring port, mirroring configuration does not take effect on the port. However, the mirroring configuration still occupies system resources and may even cause MAC address table oscillation.

Port mirroring – STP collaboration was introduced to address this problem. This feature monitors the status of each port in real time. The device determines whether to enable port mirroring on a port according to the status of the port:

- The device automatically disables port mirroring on a port in Discarding state;
- The device enables port mirroring on the port when the port restores to Forwarding state.

In this way, port mirroring collaborates with STP, and port mirroring is utilized more efficiently.



Note

For introduction to STP port state, refer to *MSTP Configuration*.

Mirroring Configuration

Complete the following tasks to configure mirroring:

Task	Remarks
Configuring Local Port Mirroring	Optional
Configuring Remote Port Mirroring	Optional



Note

On an S3600-EI series Ethernet switch, only one destination port for local port mirroring and only one reflector port can be configured, and the two types of ports cannot both exist.

Configuring Local Port Mirroring

Configuration prerequisites

- The source port is determined and the direction in which the packets are to be mirrored is determined.
- The destination port is determined.

Configuration procedure

Follow these steps to configure port mirroring on S3600-EI series Ethernet switches:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Create a port mirroring group		mirroring-group <i>group-id</i> local	Required
Enable port mirroring – STP collaboration		mirroring stp-collaboration	Required This configuration applies to all ports of the current device. By default, port mirroring – STP collaboration is not enabled.
Configure the source port for the port mirroring group	In system view	mirroring-group <i>group-id</i> mirroring-port <i>mirroring-port-list</i> { both inbound outbound }	Use either approach You can configure multiple source ports at a time in system view, or you can configure the source port in specific port view.
	In port view	interface <i>interface-type</i> <i>interface-number</i>	

To do...		Use the command...	Remarks
		mirroring-group <i>group-id</i> mirroring-port { both inbound outbound }	The configurations in the two views have the same effect.
		quit	
Configure the destination port for the port mirroring group	In system view	mirroring-group <i>group-id</i> monitor-port <i>monitor-port-id</i>	Use either approach The configurations in the two views have the same effect.
	In port view	interface <i>interface-type</i> <i>interface-number</i>	
		mirroring-group <i>group-id</i> monitor-port	

Follow these steps to configure local port mirroring on S3600-SI series Ethernet switches:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enable port mirroring – STP collaboration		mirroring stp-collaboration	Required This configuration applies to all ports of the current device. By default, port mirroring – STP collaboration is not enabled.
Configuring the source port for port mirroring	Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
	Configure the current port as the source port	mirroring-port { both inbound outbound }	Required
	Return to system view	quit	—
Configure the destination port for port mirroring	Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
	Configure the current port as the destination port	monitor-port	Required

When configuring local port mirroring, note that:

- You need to configure the source and destination ports for the local port mirroring to take effect.
- The source port and the destination port cannot be a fabric port or a member port of an existing mirroring group; besides, the destination port cannot be a member port of an aggregation group or a port enabled with LACP or STP.



Note

- With port mirroring – STP collaboration enabled, if you configure a port in Discarding state as a mirroring port, the port mirroring configuration does not take effect until the port transits to Forwarding state.
- Suppose port mirroring – STP collaboration is enabled on a device in an MSTP network. To make the port mirroring configuration take effect on a port, make sure that the port is in Forwarding state in all instances.
- To enable port mirroring on an IRF stack, you are recommended to enable port mirroring – STP collaboration.

Configuring Remote Port Mirroring



Note

- S3600-SI series Ethernet switches do not support remote port mirroring.
- An S3600-EI series Ethernet switch can serve as a source switch, an intermediate switch, or a destination switch in a remote port mirroring networking environment.

Configuration on a switch acting as a source switch

- 1) Configuration prerequisites
 - The source port, the reflector port, and the remote-probe VLAN are determined.
 - Layer 2 connectivity is ensured between the source and destination switches over the remote-probe VLAN.
 - The direction of the packets to be monitored is determined.
- 2) Configuration procedure

Follow these steps to perform configurations on the source switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a VLAN and enter the VLAN view	vlan <i>vlan-id</i>	<i>vlan-id</i> is the ID of the remote-probe VLAN.
Configure the current VLAN as the remote-probe VLAN	remote-probe vlan enable	Required
Return to system view	quit	—
Enable port mirroring – STP collaboration	mirroring stp-collaboration	Required This configuration applies to all ports of the current device. By default, port mirroring – STP collaboration is not enabled.

To do...	Use the command...	Remarks
Enter the view of the Ethernet port that connects to the intermediate switch or destination switch	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the current port as trunk port	port link-type trunk	Required By default, the port type is Access.
Configure the trunk port to permit packets from the remote-probe VLAN	port trunk permit vlan <i>remote-probe-vlan-id</i>	Required
Return to system view	quit	—
Create a remote source mirroring group	mirroring-group <i>group-id</i> remote-source	Required
Configure source port(s) for the remote source mirroring group	mirroring-group <i>group-id</i> mirroring-port <i>mirroring-port-list</i> { both inbound outbound }	Required
Configure the reflector port for the remote source mirroring group	mirroring-group <i>group-id</i> reflector-port <i>reflector-port</i>	Required
Configure the remote-probe VLAN for the remote source mirroring group	mirroring-group <i>group-id</i> remote-probe vlan <i>remote-probe-vlan-id</i>	Required

When configuring the source switch, note that:

- All ports of a remote source mirroring group are on the same device. Each remote source mirroring group can be configured with only one reflector port.
- The reflector port cannot be a member port of an existing mirroring group, a fabric port, a member port of an aggregation group, or a port enabled with LACP or STP. It must be an access port and cannot be configured with functions like VLAN-VPN, port loopback detection, packet filtering, QoS, port security, and so on.
- You cannot modify the duplex mode, port rate, and MDI attribute of a reflector port.
- Only an existing static VLAN can be configured as the remote-probe VLAN. To remove a remote-probe VLAN, you need to restore it to a normal VLAN first. A remote port mirroring group gets invalid if the corresponding remote port mirroring VLAN is removed.
- 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.



Note

- With port mirroring – STP collaboration enabled, if you configure a port in Discarding state as a mirroring port, the port mirroring configuration does not take effect until the port transits to Forwarding state.
- Suppose port mirroring – STP collaboration is enabled on a device in an MSTP network. To make the port mirroring configuration take effect on a port, make sure that the port is in Forwarding state in all instances.
- To enable port mirroring on an IRF stack, you are recommended to enable port mirroring – STP collaboration.

Configuration on a switch acting as an intermediate switch

1) Configuration prerequisites

- The trunk ports and the remote-probe VLAN are determined.
- Layer 2 connectivity is ensured between the source and destination switches over the remote-probe VLAN.

2) Configuration procedure

Follow these steps to perform configurations on the intermediate switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a VLAN and enter VLAN view	vlan <i>vlan-id</i>	<i>vlan-id</i> is the ID of the remote-probe VLAN.
Configure the current VLAN as the remote-probe VLAN	remote-probe vlan enable	Required
Return to system view	quit	—
Enter the view of the Ethernet port connecting to the source switch, destination switch or other intermediate switch	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the current port as trunk port	port link-type trunk	Required By default, the port type is Access.
Configure the trunk port to permit packets from the remote-probe VLAN	port trunk permit vlan <i>remote-probe-vlan-id</i>	Required

Note that an S3600 series Ethernet switch acting as the intermediate switch in remote port mirroring networking does not support bidirectional packet mirroring (the **both** keyword).

Configuration on a switch acting as a destination switch

1) Configuration prerequisites

- The destination port and the remote-probe VLAN are determined.
- Layer 2 connectivity is ensured between the source and destination switches over the remote-probe VLAN.

2) Configuration procedure

Follow these steps to configure remote port mirroring on the destination switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a VLAN and enter VLAN view	vlan <i>vlan-id</i>	<i>vlan-id</i> is the ID of the remote-probe VLAN.
Configure the current VLAN as a remote-probe VLAN	remote-probe vlan enable	Required
Return to system view	quit	—
Enter the view of the Ethernet port connecting to the source switch or an intermediate switch	interface <i>interface-type</i> <i>interface-number</i>	—
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 <i>remote-probe-vlan-id</i>	Required
Return to system view	quit	—
Create a remote destination mirroring group	mirroring-group <i>group-id</i> remote-destination	Required
Configure the destination port for the remote destination mirroring group	mirroring-group <i>group-id</i> monitor-port <i>monitor-port</i>	Required
Configure the remote-probe VLAN for the remote destination mirroring group	mirroring-group <i>group-id</i> remote-probe vlan <i>remote-probe-vlan-id</i>	Required

When configuring a destination switch, note that:

- An S3600 series Ethernet switch acting as the destination switch in remote port mirroring networking does not support bidirectional packet mirroring (the **both** keyword).
- The destination port of remote port mirroring cannot be a member port of an existing mirroring group, a fabric port, a member port of an aggregation group, or a port enabled with LACP or STP.
- Only an existing static VLAN can be configured as the remote-probe VLAN. To remove a remote-probe VLAN, you need to restore it to a normal VLAN first. A remote port mirroring group gets invalid if the corresponding remote port mirroring VLAN is removed.

Displaying and Maintaining Port Mirroring

To do...	Use the command...	Remarks
Display port mirroring configuration on an S3600-EI series Ethernet switch	display mirroring-group { <i>group-id</i> all local remote-destination remote-source }	Available in any view

To do...	Use the command...	Remarks
Display port mirroring configuration on an S3600-SI series Ethernet switch	display mirror	

Mirroring Configuration Examples

Local Port Mirroring Configuration Example

Network requirements

The departments of a company connect to each other through S3600-EI Ethernet switches:

- Research and Development (R&D) department is connected to Switch C through Ethernet 1/0/1.
- Marketing department is connected to Switch C through Ethernet 1/0/2.
- Data detection device is connected to Switch C through Ethernet 1/0/3

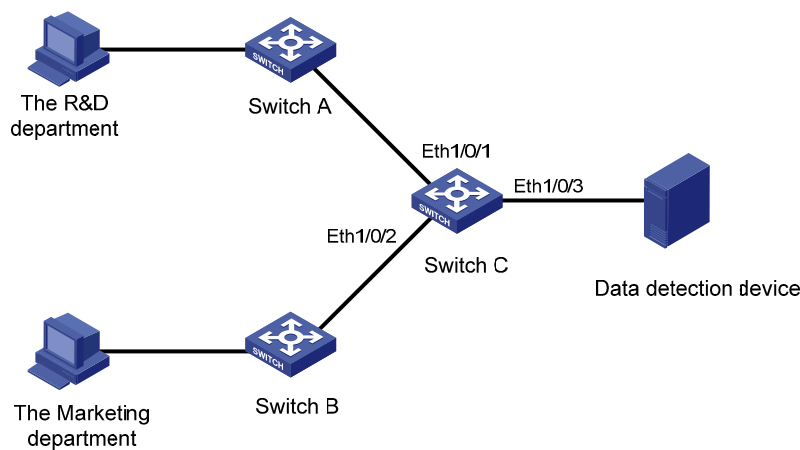
The administrator wants to monitor the packets received on and sent from the R&D department and the marketing department through the data detection device.

Use the local port mirroring function to meet the requirement. Perform the following configurations on Switch C.

- Configure Ethernet 1/0/1 and Ethernet 1/0/2 as mirroring source ports.
- Configure Ethernet 1/0/3 as the mirroring destination port.

Network diagram

Figure 1-3 Network diagram for local port mirroring



Configuration procedure

Configure Switch C:

Create a local mirroring group.

```
<Sysname> system-view
```

```
[Sysname] mirroring-group 1 local
```

Configure the source ports and destination port for the local mirroring group.

```
[Sysname] mirroring-group 1 mirroring-port Ethernet 1/0/1 Ethernet 1/0/2 both
```

```
[Sysname] mirroring-group 1 monitor-port Ethernet 1/0/3
```

Display configuration information about local mirroring group 1.

```
[Sysname] display mirroring-group 1
```

```
mirroring-group 1:
```

```
type: local
```

```
status: active
```

```
mirroring port:
```

```
    Ethernet1/0/1  both
```

```
    Ethernet1/0/2  both
```

```
monitor port: Ethernet1/0/3
```

After the configurations, you can monitor all packets received on and sent from the R&D department and the marketing department on the data detection device.

Remote Port Mirroring Configuration Example

Network requirements

The departments of a company connect to each other through S3600-EI Ethernet switches:

- Switch A, Switch B, and Switch C are S3600-EI series switches.
- Department 1 is connected to Ethernet 1/0/1 of Switch A.
- Department 2 is connected to Ethernet 1/0/2 of Switch A.
- Ethernet 1/0/3 of Switch A connects to Ethernet 1/0/1 of Switch B.
- Ethernet 1/0/2 of Switch B connects to Ethernet 1/0/1 of Switch C.
- The data detection device is connected to Ethernet 1/0/2 of Switch C.

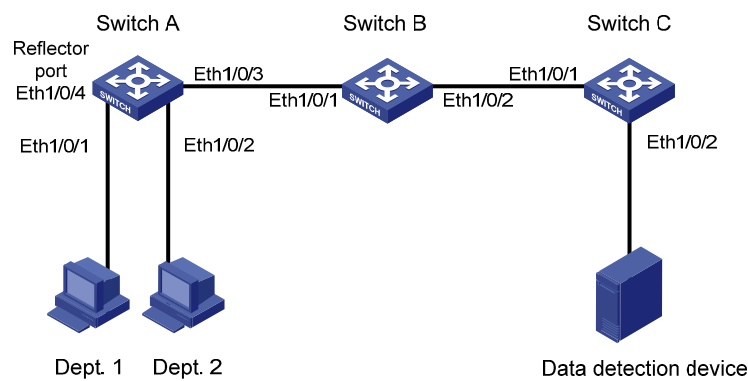
The administrator wants to monitor the packets sent from Department 1 and 2 through the data detection device.

Use the remote port mirroring function to meet the requirement. Perform the following configurations:

- Use Switch A as the source switch, Switch B as the intermediate switch, and Switch C as the destination switch.
- On Switch A, create a remote source mirroring group, configure VLAN 10 as the remote-probe VLAN, ports Ethernet 1/0/1 and Ethernet 1/0/2 as the source ports, and port Ethernet 1/0/4 as the reflector port.
- On Switch B, configure VLAN 10 as the remote-probe VLAN.
- Configure Ethernet 1/0/3 of Switch A, Ethernet 1/0/1 and Ethernet 1/0/2 of Switch B, and Ethernet 1/0/1 of Switch C as trunk ports, allowing packets of VLAN 10 to pass.
- On Switch C, create a remote destination mirroring group, configure VLAN 10 as the remote-probe VLAN, and configure Ethernet 1/0/2 connected with the data detection device as the destination port.

Network diagram

Figure 1-4 Network diagram for remote port mirroring



Configuration procedure

1) Configure the source switch (Switch A)

Create remote source mirroring group 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
```

Configure VLAN 10 as the remote-probe VLAN.

```
[Sysname] vlan 10
[Sysname-vlan10] remote-probe vlan enable
[Sysname-vlan10] quit
```

Configure the source ports, reflector port, and remote-probe VLAN for the remote source mirroring group.

```
[Sysname] mirroring-group 1 mirroring-port Ethernet 1/0/1 Ethernet 1/0/2 inbound
[Sysname] mirroring-group 1 reflector-port Ethernet 1/0/4
[Sysname] mirroring-group 1 remote-probe vlan 10
```

Configure Ethernet 1/0/3 as trunk port, allowing packets of VLAN 10 to pass.

```
[Sysname] interface Ethernet 1/0/3
[Sysname-Ethernet1/0/3] port link-type trunk
[Sysname-Ethernet1/0/3] port trunk permit vlan 10
[Sysname-Ethernet1/0/3] quit
```

Display configuration information about remote source mirroring group 1.

```
[Sysname] display mirroring-group 1
mirroring-group 1:
  type: remote-source
  status: active
  mirroring port:
    Ethernet1/0/1  inbound
    Ethernet1/0/2  inbound
  reflector port: Ethernet1/0/4
  remote-probe vlan: 10
```

2) Configure the intermediate switch (Switch B)

Configure VLAN 10 as the remote-probe VLAN.

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] remote-probe vlan enable
[Sysname-vlan10] quit
```

Configure Ethernet 1/0/1 as the trunk port, allowing packets of VLAN 10 to pass.

```
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] port link-type trunk
[Sysname-Ethernet1/0/1] port trunk permit vlan 10
[Sysname-Ethernet1/0/1] quit
```

Configure Ethernet 1/0/2 as the trunk port, allowing packets of VLAN 10 to pass.

```
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] port link-type trunk
[Sysname-Ethernet1/0/2] port trunk permit vlan 10
```

3) Configure the destination switch (Switch C)

Create remote destination mirroring group 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-destination
```

Configure VLAN 10 as the remote-probe VLAN.

```
[Sysname] vlan 10
[Sysname-vlan10] remote-probe vlan enable
[Sysname-vlan10] quit
```

Configure the destination port and remote-probe VLAN for the remote destination mirroring group.

```
[Sysname] mirroring-group 1 monitor-port Ethernet 1/0/2
[Sysname] mirroring-group 1 remote-probe vlan 10
```

Configure Ethernet 1/0/1 as the trunk port, allowing packets of VLAN 10 to pass.

```
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] port link-type trunk
[Sysname-Ethernet1/0/1] port trunk permit vlan 10
[Sysname-Ethernet1/0/1] quit
```

Display configuration information about remote destination mirroring group 1.

```
[Sysname] display mirroring-group 1
mirroring-group 1:
    type: remote-destination
    status: active
    monitor port: Ethernet1/0/2
    remote-probe vlan: 10
```

After the configurations, you can monitor all packets sent from Department 1 and 2 on the data detection device.

Table of Contents

1 IRF Fabric Configuration	1-1
Introduction to IRF.....	1-1
Advantages.....	1-1
Application and Advantages	1-1
Establishment of an IRF Fabric	1-2
How IRF Works	1-6
IRF Fabric Configuration	1-7
IRF Fabric Configuration Task List.....	1-7
Specifying the Fabric Port of a Switch.....	1-8
Specifying the VLAN Used to Form an IRF Fabric.....	1-9
Setting a Unit ID for a Switch	1-10
Assigning a Unit Name to a Switch	1-11
Assigning an IRF Fabric Name to a Switch.....	1-11
Setting the IRF Fabric Authentication Mode.....	1-12
Configuring IRF Automatic Fabric for a Switch	1-12
Displaying and Maintaining IRF Fabric	1-13
IRF Fabric Configuration Example.....	1-13
Network Requirements	1-13
Network Diagram.....	1-14
Configuration Procedure.....	1-14

1 IRF Fabric Configuration

When configuring IRF fabric, go to these sections for information you are interested in:

- [Introduction to IRF](#)
- [IRF Fabric Configuration](#)
- [Displaying and Maintaining IRF Fabric](#)
- [IRF Fabric Configuration Example](#)

Introduction to IRF

Intelligent Resilient Framework (IRF), a feature particular to H3C S3600 series switches, is a new technology for building the core of a network. This feature allows you to build an IRF fabric by interconnecting several S3600 series switches to provide more ports for network devices and improve the reliability of your network.

Advantages

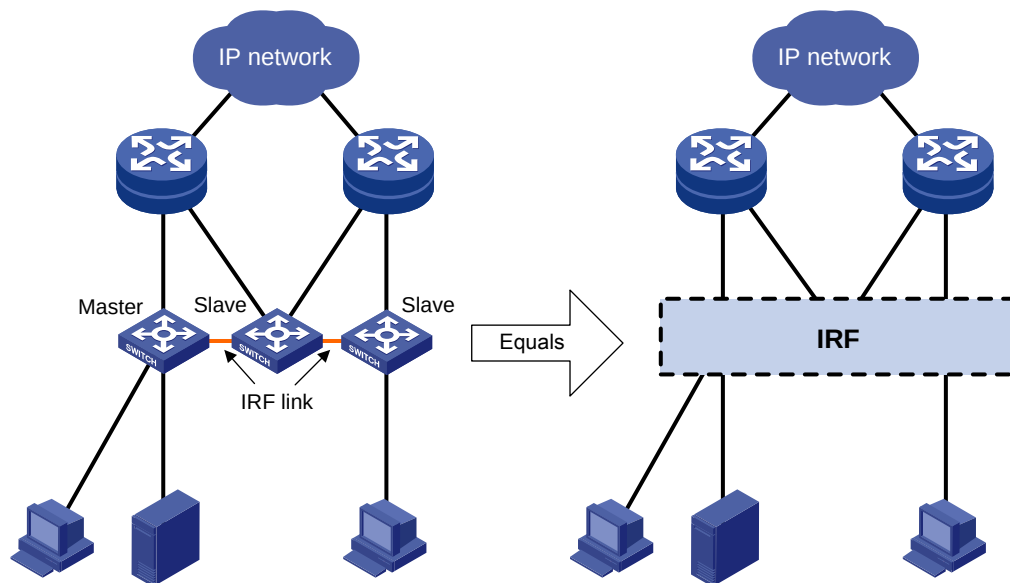
IRF features the following advantages:

- Streamlined management. After an IRF is established, you can log in to the IRF system by connecting to any port of any member to manage all IRF members.
- High reliability. An IRF system comprises multiple member devices: the master runs, manages and maintains the IRF, whereas the slaves process services as well as functioning as the backups. As soon as the master fails, the IRF system elects a new master immediately to prevent service interruption and implement 1:N backup. Besides, the physical links between the IRF system and the upper or lower layer devices can be aggregated, and thus the reliability of the IRF system is increased through the link backup.
- Powerful network expansion capability. By adding member devices, the number of IRF ports and network bandwidth of the IRF system can be easily expanded. Each member device has its own CPU and they can process and forward protocol packets independently; therefore, the processing capability of the IRF system also can be easily expanded.

Application and Advantages

Typically, you can use an IRF in the distribution layer; and you can also apply it in the access layer. An IRF is a single logical device to the users and devices of the upper layer and lower layer, as shown in [Figure 1-1](#).

Figure 1-1 IRF networking

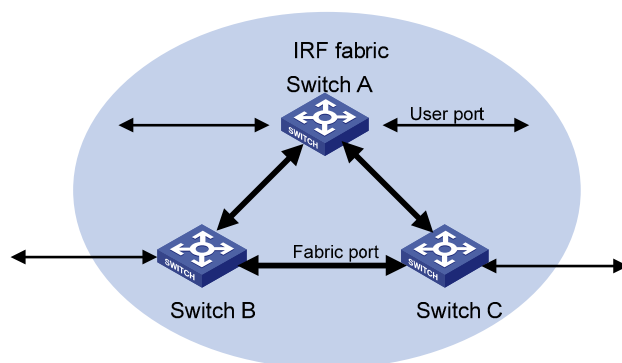


Establishment of an IRF Fabric

Topology and connections of an IRF fabric

An IRF fabric typically has a ring topology structure. As shown in [Figure 1-2](#), each switch has two ports connected with two other switches in the fabric. These two ports are called fabric ports in general, a left port and a right port respectively; the other ports, which are available for connections with users or devices outside the fabric, are called user ports.

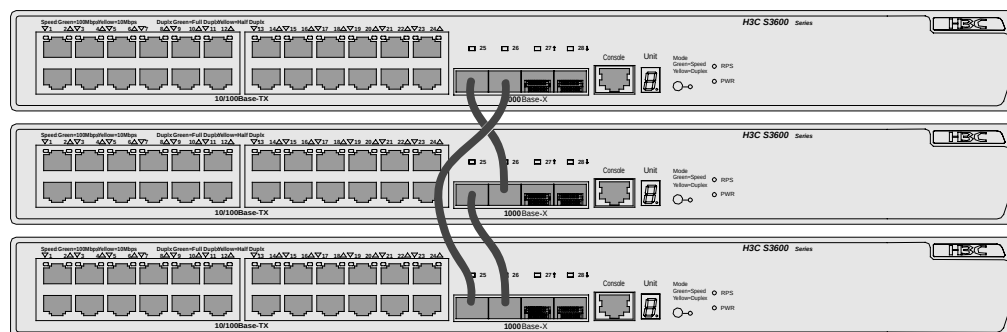
Figure 1-2 A schematic diagram of an IRF fabric



A correctly built IRF fabric features the following:

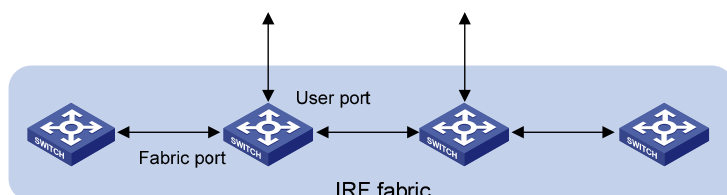
- Multiple S3600 series switches are interconnected through their fabric ports.
- Given a switch, its left port is connected to the right port of another switch, and its right port is connected to the left port of a third one.

Figure 1-3 Port connection mode for S3600 series ring topology IRF fabric Port connection mode for S3600 series ring topology IRF fabric is shown in [Figure 1-3](#).



IRF fabric also supports bus topology, which has the same requirements as the ring topology. The difference is that in a bus topology structure, the units at both ends of the bus have only one fabric port connected, as shown in [Figure 1-4](#).

Figure 1-4 IRF fabric bus topology



A ring topology is more reliable than a daisy chain topology. The failure of one link in a ring connection does not affect the function and performance of the XRN, whereas the failure of one link in a daisy chain connection causes the split of the XRN.

Fabric ports

On an S3600 series Ethernet switch, only four GigabitEthernet ports can be configured as fabric ports. If not used for fabric connection, these four ports can be used as general data ports. The four ports fall into two groups according to their port numbers:

- GigabitEthernet 1/1/1 and GigabitEthernet 1/1/2 form the first group.
- GigabitEthernet 1/1/3 and GigabitEthernet 1/1/4 form the second group.

Only one group of ports can be configured as fabric ports at a time. Given a group, either GigabitEthernet 1/1/1 or GigabitEthernet 1/1/3 can be configured as the left fabric port, and either GigabitEthernet 1/1/2 or GigabitEthernet 1/1/4 can be configured as the right fabric port.

Once you configure a port as a fabric port, the group that comprises this fabric port becomes the fabric port group, and you cannot configure a port in the other group as a fabric port. For example, once you configure GigabitEthernet 1/1/1 as a fabric port, this port automatically becomes the left port and the first group becomes the fabric port group.



Note

The system does not require a consistency in the fabric port groups between different switches. That is, the left fabric port in the first group of a switch can be connected to the right fabric port in the second group of the peer switch.

FTM

As the basis of the IRF function, the Fabric Topology Management (FTM) program manages and maintains the entire topology of a fabric.

With fabric ports configured, the FTM program releases information of the device 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 discovery packet (DISC).

After receiving the packet, the peer device will analyze the packet. A device can form a fabric with the peer or 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 (up to eight devices can form a fabric).
- The fabric name 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 on the device or in the fabric, that is, the same authentication mode and password are configured on the device and the existing devices in the fabric.



Note

In case IRF automatic fabric is enabled on both a switch in the fabric and a switch to be added to the fabric (referred to as candidate switch hereinafter), even if the software version of the candidate switch is inconsistent with that used on the device in the fabric, you can still add a device to the fabric by automatic downloading and loading of the software.

IRF fabric detection

Forming a fabric requires a high consistency of connection modes between the devices and device information. Without all the requirements for forming a fabric being met, a fabric cannot be formed.

The FTM program detects the necessary conditions for forming a fabric one by one and displays the detection results. You can use the **display ftm information** command to view the detection information for the fabric, checking the running status of the fabric or analyzing the problems. [Table 1-1](#) lists the status and solution of the problems.

Table 1-1 Status and solution

Status	Analysis		Solution
normal	—		These three kinds of information do not mean a device or a fabric operates improperly. No measure is needed for any of them.
temporary			
redundance port			
connection error	Indicates three kinds of port matching errors may occur.	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 the 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.
reached max units	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.		Remove the new device or existing devices in the fabric.
different system name	The fabric name of the device directly connected to the switch and the existing fabric name of the fabric are not the same.		Modify the fabric name of the new device to be that of the fabric.
different product version	The software version of the directly connected device and that of the current device are not the same.		Update the software version to make sure the software version of the new device is the same as that of the fabric.
auth failure	The IRF fabric authentication modes configured for the local device and that of the fabric are not the same, or the password configured does not match.		Configure the IRF fabric authentication modes and the passwords for the local device and the fabric as the same.

IRF automatic fabric

If the software version and fabric name of the candidate switch are inconsistent with those of the device in the IRF fabric, the local device cannot be added to the fabric. In this case, you have to manually download and load the software, and then restart the device, or manually change the fabric name to add the device to the fabric. H3C S3600 series switches provide the IRF automatic fabric function, which enables a candidate switch to automatically download the software and change the fabric name in case that the software version and fabric name of the candidate device and that of the device in the fabric are different, thus reducing the manual maintenance workload.

With IRF automatic fabric enabled, if inconsistency in software version or fabric name occurs when a switch is added to a fabric, the system automatically performs the following operations:

- If the software version of the local device is inconsistent with that of the device in the fabric, the system automatically initiates a download request to the device with the smallest unit ID in the

fabric and downloads the software used by the device in the current fabric to the local device. Then the device will automatically restart and be added to the fabric.

- If the fabric name of the local device is inconsistent with that of the device in the fabric, the system automatically ignores the inconsistency check of the fabric name and adds the device to the fabric. Then the system automatically synchronizes the configurations to the device with the smallest unit ID and changes the fabric name.

With the above operations completed, the device can be added to the fabric and work normally.



Caution

- You need to enable the IRF automatic fabric function on all the devices including the candidate switch in the fabric to enable the candidate switch to download software and discovery neighbors and thus be added to the fabric normally.
 - If the candidate switch is going to download software from a unit in an IRF fabric, you are recommended to set the ID of the unit to 1 to make the candidate switch download the software of correct version.
-

How IRF Works

When a fabric is established, the devices determine their respective roles in the fabric by comparing their CPU MAC addresses. The device with the lowest CPU MAC address is elected as the master and the other devices are slaves.

After the election, the fabric can operate normally. The following three functions of IRF can provide simple configuration mode, enhanced network performance and perfect redundancy backup mechanism for users.



Note

- The S3600-SI series Ethernet switches support basic IRF fabric feature, that is, Distributed Device Management (DDM) function and Distributed Link Aggregation (DLA).
 - The S3600-EI series Ethernet switches support enhanced IRF fabric feature, including DDM, Distributed Redundancy Routing (DRR) and Distributed Link Aggregation (DLA).
-

DDM

DDM is a new device management mode provided by IRF. In normal cases, a fabric can be considered as a single device. You can manage the entire fabric by logging onto any device in the fabric with different logging modes. The devices in the fabric synchronize their configurations by exchanging packets, thus ensuring stability of the fabric.

FTM program uses Unit ID, or device ID to distinguish between the devices in a fabric when you manage them. On initialization of the IRF function, each device considers its Unit ID as 1 and after a

fabric connection is established, the FTM program automatically re-numbers the devices or you can manually configure the Unit ID of them.

The master in a fabric collects the newest configurations of the user and the slaves periodically synchronize the configurations from the master. In this way, the entire fabric can operate with the same configurations.

DRR

DRR is used to implement redundancy routing backup. The devices in a fabric run their independent routing protocols and maintain their own routing tables. Unlike a common layer 3 switch, a fabric member does not generate a layer 3 forwarding table to forward packets; instead, it uploads the routing table to the master, which generates a forwarding table used by the entire fabric by integrating the routing tables of all the devices. Then each slave synchronizes this forwarding table from the master and takes it as the basis for layer 3 forwarding.

In this way, the forwarding table entries of each device in the fabric can be consistent. Even if the master fails, other devices can use the forwarding table synchronized from the master to perform layer 3 forwarding, thus ensuring the accuracy of forwarding path. After re-electing the master, the fabric will restart routing update.

DLA

As a new link aggregation mode, DLA can improve fault tolerance and redundancy backup of user networks.

Link aggregation enables you to configure ports on the same device as an aggregation port group, avoiding network interruptions resulted from single port failure. Based on link aggregation, DLA provides a more reliable solution, with which you can select ports on different devices to form an aggregation port group. In this way, single port failure can be avoided and network reliability can be greatly improved, because the fabric can communicate with the destination network through ports on other devices in case a single device fails.

IRF Fabric Configuration

IRF Fabric Configuration Task List

Complete the following tasks to configure IRF fabric:

Task	Remarks
Specifying the Fabric Port of a Switch	Required
Specifying the VLAN Used to Form an IRF Fabric	Optional
Setting a Unit ID for a Switch	Optional
Assigning a Unit Name to a Switch	Optional
Assigning an IRF Fabric Name to a Switch	Optional
Setting the IRF Fabric Authentication Mode	Optional
Configuring IRF Automatic Fabric for a Switch	Optional

Specifying the Fabric Port of a Switch

You can specify the fabric port of a switch in either system view or Ethernet interface view.

Configurations in system view

Follow these steps to specify a fabric port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify the fabric port of a switch	fabric-port <i>interface-type</i> <i>interface-number</i> enable	Required Not specified by default

Configurations in Ethernet interface view

Follow these steps to specify a fabric port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Specify the current port as the fabric port of a switch	port link-type irf-fabric	Required No port is specified as the fabric port by default.



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 configure some functions that affect the IRF for other ports or globally. Otherwise, you cannot enable the fabric port. For detailed restrictions refer to the error information output by devices.
- After an IRF fabric is created, you are not recommended to enable the Burst function on any fabric device. For the introduction to the Burst function, refer to the *QoS-QoS Profile* part in this manual.
- 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 configure 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 to be split and error messages, do not perform such operations.
- To split a fabric, you can simply remove the cables used to form the fabric or disable the 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.
- If you need to configure an IRF fabric as a DHCP server, DHCP relay or DHCP client, configure the UDP Helper function in the fabric at the same time to ensure that the client can successfully obtain an IP address. For the configuration of the UDP Helper function, refer to the UDP Helper part in this manual.
- After you use the **port link-type irf-fabric** command to specify a port as the fabric port, you cannot use the **port link-type** command to change the port to a port of other types. You must use the **undo fabric-port** command first to disable the fabric port function of the port to change the port type.

Specifying the VLAN Used to Form an IRF Fabric

When the devices in an IRF fabric are transmitting IRF data, to avoid it being sent to other non fabric ports, the data should be transmitted in a specified VLAN. You can specify the VLAN used to transmit IRF data.

Follow these steps to specify the VLAN used to form an IRF fabric:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify the VLAN used to form an IRF fabric	ftm fabric-vlan <i>vlan-id</i>	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.

Setting a Unit ID for a Switch

FTM will automatically number the switches to constitute an IRF fabric by default, 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.

Follow these steps to set a unit ID for a switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set a unit ID for the switch	change self-unit to { <i>unit-id</i> 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 configure 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.

Follow these steps to set a unit ID to a new value:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set a unit ID to a new value	change unit-id <i>unit-id1</i> to { <i>unit-id2</i> 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 prompts you to confirm if you really want to change the unit ID. If you choose to change it, 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 program to perform automatic numbering. The value of priority can be 5 or 10. Priority 5 means the switch adopts manual numbering, and priority 10 means the switch adopts automatic numbering. Manual numbering has a higher priority than 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.

Follow these steps to save the unit ID of each unit in the IRF fabric:

To do...	Use the command...	Remarks
Save the unit ID of each unit in the IRF fabric	fabric save-unit-id	Optional

Assigning a Unit Name to a Switch

Follow these steps to assign a unit name to a switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Assign a unit name to a switch	set unit <i>unit-id</i> name <i>unit-name</i>	Required

Assigning an IRF Fabric Name to a Switch

Only the switches with the same IRF fabric name can form an IRF fabric.

Follow these steps to assign a fabric name to a switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Assign a fabric name to the switch	sysname <i>sysname</i>	Optional By default, the IRF fabric name is H3C.

Setting the IRF Fabric Authentication Mode

Only the switches with the same IRF fabric authentication mode can form an IRF fabric.

Follow these steps to set the IRF fabric authentication mode for a switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the IRF fabric authentication mode for the switch	irf-fabric authentication-mode { simple <i>password</i> md5 <i>key</i> }	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.

Configuring IRF Automatic Fabric for a Switch

Configuration prerequisites

- Make sure that the Flash of the newly added device has enough space to download software used on the device in the fabric.
- Configure the fabric port for the newly added device.

Configuration procedure

Follow these steps to configure IRF automatic fabric for a switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure IRF automatic fabric for a switch	fabric member-auto-update software enable	Required Disabled by default



Caution

- You need to enable the IRF automatic fabric function on all the devices including the newly added device in the fabric to enable the newly added device to download software and discovery neighbors and thus be added to the fabric normally.
 - After you configure the IRF automatic fabric function on Slave, execute the **save** command to save the configurations as soon as possible. Otherwise, the device may synchronize the configurations from Master and restart repeatedly because the configurations on the device are lost after the device automatically downloads the software and restarts.
-

Displaying and Maintaining IRF Fabric

To do...	Use the command...	Remarks
Display the information about an IRF fabric	display irf-fabric [port status]	Available in any view
Display the topology information of an IRF fabric	display ftm { information topology-database }	
Clear the FTM statistics	reset ftm statistics	Available in user view

IRF Fabric Configuration Example

Network Requirements

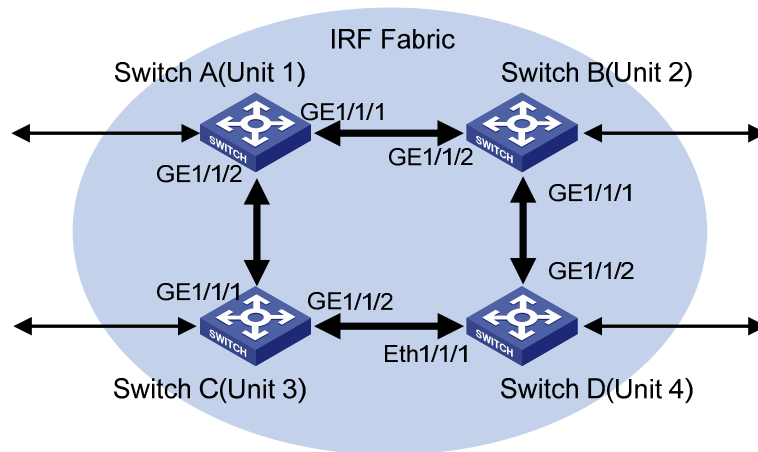
Configure unit ID, unit name, IRF fabric name, and authentication mode for four switches to enable them to form an IRF fabric as shown in [Figure 1-5](#).

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

Network Diagram

Figure 1-5 Network diagram for forming an IRF fabric



Configuration Procedure

1) Configure Switch A.

Configure fabric ports.

```
<Sysname> system-view
```

```
[Sysname] fabric-port GigabitEthernet1/1/1 enable
```

```
[Sysname] fabric-port GigabitEthernet1/1/2 enable
```

Configure the unit name as **Unit 1**.

```
[Sysname] set unit 1 name Unit1
```

Configure the fabric name as **hello**.

```
[Sysname] sysname hello
```

Configure the fabric authentication mode as **simple** and the password as **welcome**.

```
[hello] irf-fabric authentication-mode simple welcome
```

2) Configure Switch B.

Configure fabric ports.

```
<Sysname> system-view
```

```
[Sysname] fabric-port GigabitEthernet1/1/1 enable
```

```
[Sysname] fabric-port GigabitEthernet1/1/2 enable
```

Set the unit ID to 2.

```
[Sysname] change unit-id 1 to 2
```

Configure the unit name as **Unit 2**.

```
[Sysname] set unit 1 name unit2
```

Configure the fabric name as **hello**.

```
[Sysname] sysname hello
```

Configure the fabric authentication mode as **simple** 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

1 Cluster	1-1
Cluster Overview	1-1
Introduction to HGMP	1-1
Roles in a Cluster	1-2
How a Cluster Works	1-3
Cluster Configuration Task List	1-9
Configuring the Management Device	1-9
Configuring Member Devices	1-13
Managing a Cluster through the Management Device	1-15
Configuring the Enhanced Cluster Features	1-16
Configuring the Cluster Synchronization Function	1-18
Displaying and Maintaining Cluster Configuration	1-22
Cluster Configuration Examples	1-23
Basic Cluster Configuration Example	1-23
Network Management Interface Configuration Example	1-26
Enhanced Cluster Feature Configuration Example	1-27

1 Cluster

When configuring cluster, go to these sections for information you are interested in:

-

-  **Note**

- [The cluster synchronization function is added. For the configuration, refer to 36HConfiguring the Cluster Synchronization Function.](#)
- [Cluster Overview](#)
- [Cluster Configuration Task List](#)
- [Displaying and Maintaining Cluster Configuration](#)
- [Cluster Configuration Examples](#)

 **Note**

The cluster synchronization function is added. For the configuration, refer to [Configuring the Cluster Synchronization Function](#).

Cluster Overview

Introduction to HGMP

A cluster contains a group of switches. Through cluster management, you can manage multiple geographically dispersed in a centralized way.

Cluster management is implemented through Huawei Group Management Protocol (HGMP). HGMP version 2 (HGMPv2) is used at present.

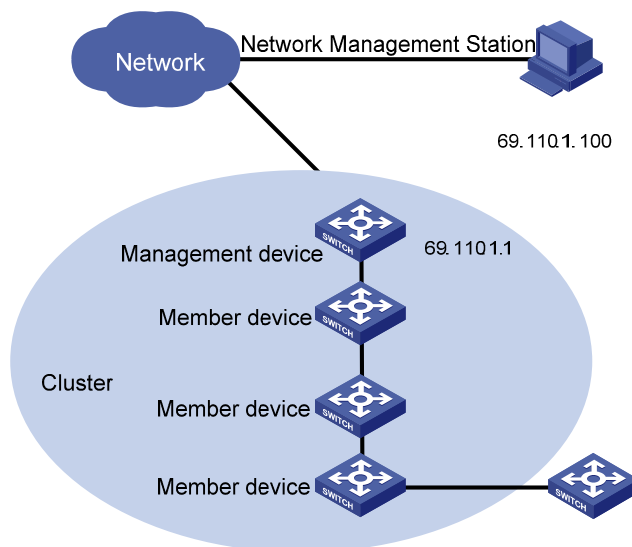
A switch in a cluster plays one of the following three roles:

- Management device
- Member device
- Candidate device

A cluster comprises of a management device and multiple member devices. To manage the devices in a cluster, you need only to configure an external IP address for the management switch. Cluster management enables you to configure and manage remote devices in batches, reducing the workload of the network configuration. Normally, there is no need to configure external IP addresses for member devices.

[Figure 1-1](#) illustrates a cluster implementation.

Figure 1-1 A cluster implementation



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.

Roles in a Cluster

The switches in a cluster play different roles according to their functions and status. You can specify the role a switch plays. A switch in a cluster can also switch to other roles under specific conditions.

As mentioned above, the three cluster roles are management device, member device, and candidate device.

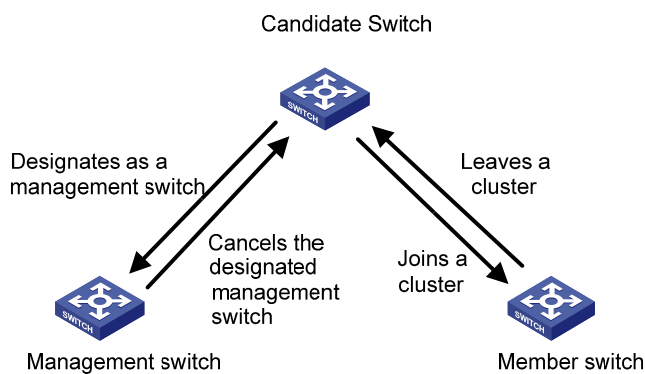
Table 1-1 Description on cluster roles

Role	Configuration	Function
Management device	Configured with a external IP address	• Provides an interface for managing all the switches in a cluster • Manages member devices through command redirection, that is, it forwards the commands intended for specific member devices. • Discovers neighbors, collects the information about network topology, manages and maintains the cluster. Management device also supports FTP server and SNMP host proxy. • Processes the commands issued by users through the public network

Role	Configuration	Function
Member device	Normally, a member device is not assigned an external IP address	- Members of a cluster - Discovers the information about its neighbors, processes the commands forwarded by the management device, and reports log. The member devices of a cluster are under the management of the management device.
Candidate device	Normally, a candidate device is not assigned an external IP address	Candidate device refers to the devices that do not belong to any clusters but are cluster-capable.

[Figure 1-2](#) illustrates the state machine of cluster role.

Figure 1-2 State machine of cluster role



- A candidate device becomes a management device when you create a cluster on it. Note that a cluster must have one (and only one) management device. On becoming a management device, the device collects network topology information and tries to discover and determine candidate devices, which can then be added to the cluster through configurations.
- A candidate device becomes a member device after being added to a cluster.
- A member device becomes a candidate device after it is removed from the cluster.
- A management device becomes a candidate device only after the cluster is removed.



Note

After you create a cluster on an S3600 switch, the switch collects the network topology information periodically and adds the candidate switches it finds to the cluster. The interval for a management device to collect network topology information is determined by the NTDP timer. If you do not want the candidate switches to be added to a cluster automatically, you can set the topology collection interval to 0 by using the **ntdp timer** command. In this case, the switch does not collect network topology information periodically.

How a Cluster Works

HGMPv2 consists of the following three protocols:

- Neighbor Discovery Protocol (NDP)
- Neighbor Topology Discovery Protocol (NTDP)
- Cluster

A cluster configures and manages the devices in it through the above three protocols.

Cluster management involves topology information collection and the establishment/maintenance of a cluster. Topology information collection and cluster establishment/maintenance are independent from each other. The former, as described below, starts before a cluster is established.

- All devices use NDP to collect the information about their neighbors, including software version, host name, MAC address, and port name.
- The management device uses NTDP to collect the information about the devices within specific hops and the topology information about the devices. It also determines the candidate devices according to the information collected.
- The management device adds the candidate devices to the cluster or removes member devices from the cluster according to the candidate device information collected through NTDP.

Introduction to NDP

NDP is a protocol used to discover adjacent devices and provide information about them. NDP operates on 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, the Boot ROM version and so on.

- An NDP-enabled device maintains an NDP neighbor table. Each entry in the NDP table can automatically age 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.

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 detects a 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 timely.

The management device collects the topology information periodically. You can also launch an operation of topology information collection by executing related commands. The process of topology information collection is as follows.

- The management device sends NTDP topology collection requests periodically through its NTDP-enabled ports.
- Upon receiving an NTDP topology collection request, the device returns a NTDP topology collection response to the management device and forwards the request to its neighbor devices through its NTDP-enabled ports. The topology collection response packet contains the information about the local device and the NDP information about all the neighbor devices.
- The neighbor devices perform the same operation until the NTDP topology collection request is propagated to all the devices within the specified hops.

When an NTDP topology collection request is propagated in the network, it is received and forwarded by large numbers of network devices, which may cause network congestion and the management device busy processing of the NTDP topology collection responses. To avoid such cases, the following methods can be used to control the NTDP topology collection request advertisement speed.

- Configuring the devices not to forward the NTDP topology collection request immediately after they receive an NTDP topology collection request. That is, configure the devices to wait for a period before they forward the NTDP topology collection request.
- Configuring each NTDP-enabled port on a device to forward an NTDP topology collection request after a specific period since the previous port on the device forwards the NTDP topology collection request.



Note

- To implement NTDP, you need to enable NTDP both globally and on specific ports on the management device, and configure NTDP parameters.
 - On member/candidate devices, you only need to enable NTDP globally and on specific ports.
 - Member and candidate devices adopt the NTDP settings of the management device.
-

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 need to enable the cluster function first.



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.

Cluster maintenance

1) Adding a candidate device to a cluster

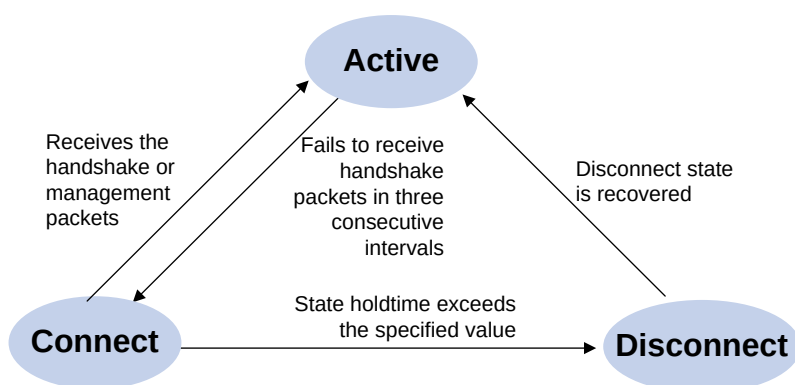
To create a cluster, you need to determine the device to operate as the management device first. The management device discovers and determines candidate devices through NDP and NTDP, and adds them to the cluster. You can also add candidate devices to a cluster manually.

After a candidate device is added to a cluster, the management device assigns a member number and a private IP address (used for cluster management) to it.

2) Communications within a cluster

In a cluster, the management device maintains the connections to the member devices through handshake packets. [Figure 1-3](#) illustrates the state machine of the connection between the management device and a member device.

Figure 1-3 State machine of the connection between the management device and a member device



- After a cluster is created and a candidate device is added to the cluster as a member device, both the management device and the member device store the state information of the member device and mark the member device as Active.
- The management device and the member devices exchange handshake packets periodically. Note that the handshake packets exchanged keep the states of the member devices to be Active and are not responded.
- If the management device does not receive a handshake packet from a member device after a period three times of the interval to send handshake packets, it changes the state of the member device from Active to Connect. Likewise, if a member device fails to receive a handshake packet from the management device after a period three times of the interval to send handshake packets, the state of the member device will also be changed from Active to Connect.
- If the management device receives a handshake packet or management packet from a member device that is in Connect state within the information holdtime, it changes the state of the member

device to Active; otherwise, it changes the state of the member device (in Connect state) to Disconnect, in which case the management device considers the member device disconnected. Likewise, if this member device, which is in Connect state, receives a handshake packet or management packet from the management device within the information holdtime, it changes its state to Active; otherwise, it changes its state to Disconnect.

- If the connection between the management device and a member device in Disconnect state is recovered, the member device will be added to the cluster again. After that, the state of the member device will turn to Active both locally and on the management device.

Besides, handshake packets are also used by member devices to inform the management device of topology changes.

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.

Management VLAN

Management VLAN limits the range of cluster management. Through management VLAN configuration, the following functions can be implemented:

- Enabling the management packets (including NDP packets, NTDP packets, and handshake packets) to be transmitted in the management VLAN only, through which the management packets are isolated from other packets and network security is improved.
- Enabling the management device and the member devices to communicate with each other in the management VLAN.

Cluster management requires the packets of the management VLAN be permitted on ports connecting the management device and the member/candidate devices. Therefore:

- If the packets of management VLAN are not permitted on a candidate device port connecting to the management device, the candidate device cannot be added to the cluster. In this case, you can enable the packets of the management VLAN to be permitted on the port through the management VLAN auto-negotiation function.
- Packets of the management VLAN can be exchanged between the management device and a member device/candidate device without carrying VLAN tags only when the default VLAN ID of both the two ports connecting the management device and the member/candidate device is the management VLAN. If the VLAN IDs of the both sides are not that of the management VLAN, packets of the management VLAN need to be tagged.



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.
-

Tracing a device in a cluster

In practice, you need to implement the following in a cluster sometimes:

- Know whether there is a loop in the cluster
- Locate which port on which switch initiates a network attack
- Determine the port and switch that a MAC address corresponds to
- Locate which switch in the cluster has a fault
- Check whether a link in the cluster and the devices on the link comply with the original plan

In these situations, you can use the **tracemac** command to trace a device in the cluster by specifying a destination MAC address or IP address.

The procedures are as follows:

- 1) Determine whether the destination MAC address or destination IP address is used to trace a device in the cluster
 - If you use the **tracemac** command to trace the device by its MAC address, the switch will query its MAC address table according to the MAC address and VLAN ID in the command to find out the port connected with the downstream switch.
 - If you use the **tracemac** command to trace the device by its IP address, the switch will query the corresponding ARP entry of the IP address to find out the corresponding MAC address and VLAN ID, and thus find out the port connected with the downstream switch.
- 2) After finding out the port connected with the downstream switch, the switch will send a multicast packet with the VLAN ID and specified hops to the port. Upon receiving the packet, the downstream switch compares its own MAC address with the destination MAC address carried in the multicast packet:
 - If the two MAC addresses are the same, the downstream switch sends a response to the switch sending the **tracemac** command, indicating the success of the **tracemac** command.
 - If the two MAC addresses are different, the downstream switch will query the port connected with its downstream switch based on the MAC address and VLAN ID, and then forward the packet to its downstream switch. If within the specified hops, a switch with the specified destination MAC address is found, this switch sends a response to the switch sending the **tracemac** command, indicating the success of the **tracemac** command. If no switch with the specified destination MAC address (or IP address) is found, the multicast packet will not be forwarded to the downstream any more.



Note

- If the queried IP address has a corresponding ARP entry, but the MAC address entry corresponding to the IP address does not exist, the trace of the device fails.
 - To trace a specific device using the **tracemac** command, make sure that all the devices passed support the **tracemac** function.
 - To trace a specific device in a management VLAN using the **tracemac** command, make sure that all the devices passed are within the same management VLAN as the device to be traced.
-

Cluster Configuration Task List

Before configuring a cluster, you need to determine the roles and functions the switches play. You also need to configure the related functions, preparing for the communication between devices within the cluster.

Complete the following tasks to configure cluster:

Task	Remarks
Configuring the Management Device	Required
Configuring Member Devices	Required
Managing a Cluster through the Management Device	Optional
Configuring the Enhanced Cluster Features	Optional
Configuring the Cluster Synchronization Function	Optional

Configuring the Management Device

Management device configuration task list

Complete the following tasks to configure management device:

Task	Remarks
Enabling NDP globally and on specific ports	Required
Configuring NDP-related parameters	Optional
Enabling NTDP globally and on a specific port	Required
Configuring NTDP-related parameters	Optional
Enabling the cluster function	Required
Configuring cluster parameters	Required
Configuring inside-outside interaction for a cluster	Optional
Configuring the network management interface for a cluster	Optional



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.

Enabling NDP globally and on specific ports

Follow these steps to enable NDP globally and on specific ports:

To do...			Use the command...	Remarks
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 <i>port-list</i>	Use either approach. By default, NDP is enabled on a port.
	In Ethernet port view	Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	
		Enable NDP on the port	ndp enable	

Configuring NDP-related parameters

Follow these steps to configure NDP-related parameters:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the holdtime of NDP information	ndp timer aging <i>aging-in-seconds</i>	Optional By default, the holdtime of NDP information is 180 seconds.
Configure the interval to send NDP packets	ndp timer hello <i>seconds</i>	Optional By default, the interval to send NDP packets is 60 seconds.

Enabling NTDP globally and on a specific port

Follow these steps to enable NTDP globally and on a specific port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable NTDP globally	ntdp enable	Required Enabled by default
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable NTDP on the Ethernet port	ntdp enable	Required Enabled by default

Configuring NTDP-related parameters

Follow these steps to configure NTDP-related parameters:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the range to collect topology information	ntdp hop <i>hop-value</i>	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 <i>time</i>	Optional By default, the device forward delay is 200 ms.
Configure the port forward delay of topology collection requests	ntdp timer port-delay <i>time</i>	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	—
Launch topology information collection manually	ntdp explore	Optional

Enabling the cluster function

Follow these steps to enable the cluster function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the cluster function globally	cluster enable	Required By default, the cluster function is enabled.

Configuring cluster parameters

The establishment of a cluster and the related configuration can be accomplished in manual mode or automatic mode, as described below.

1) Establishing a cluster and configuring cluster parameters in manual mode

Follow these steps to establish a cluster and configure cluster parameters in manual mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify the management VLAN	management-vlan <i>vlan-id</i>	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 <i>administrator-ip-address</i> { <i>ip-mask</i> <i>ip-mask-length</i> }	Required

To do...	Use the command...	Remarks
Build a cluster	build <i>name</i>	Required <i>name</i> : Cluster name.
Configure a multicast MAC address for the cluster	cluster-mac <i>H-H-H</i>	Required 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 <i>time-interval</i>	Optional By default, the interval to send multicast packets is one minutes.
Set the holdtime of member switches	holdtime <i>seconds</i>	Optional By default, the holdtime is 60 seconds.
Set the interval to send handshake packets	timer <i>interval</i>	Optional By default, the interval to send handshake packets is 10 seconds.

2) Establish a cluster in automatic mode

Follow these steps to establish a cluster in automatic mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter cluster view	cluster	—
Configure the IP address range for the cluster	ip-pool <i>administrator-ip-address</i> { <i>ip-mask</i> <i>ip-mask-length</i> }	Required
Start automatic cluster establishment	auto-build [recover]	Required Follow prompts to establish a cluster.



Note

- After a cluster is established automatically, ACL 3998 and ACL 3999 will be generated automatically.
- After a cluster is established automatically, ACL 3998 and ACL 3999 can neither be modified nor removed.

Configuring inside-outside interaction for a cluster

Follow these steps to configure inside-outside interaction for a cluster:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter cluster view	cluster	Required

To do...	Use the command...	Remarks
Configure a shared FTP server for the cluster	ftp-server <i>ip-address</i>	Optional By default, the management device acts as the shared FTP server.
Configure a shared TFTP server for the cluster	tftp-server <i>ip-address</i>	Optional By default, no shared TFTP server is configured.
Configure a shared logging host for the cluster	logging-host <i>ip-address</i>	Optional By default, no shared logging host is configured.
Configure a shared SNMP host for the cluster	snmp-host <i>ip-address</i>	Optional By default, no shared SNMP host is configured.

Configuring the network management interface for a cluster

- 1) Configuration prerequisites
 - The cluster switches are properly connected;
 - The shared servers are properly connected to the management switch.
- 2) Configuration procedure

Follow these steps to configure the network management interface for a cluster:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter cluster view	cluster	Required
Configure the network management (NM) interface for the cluster	nm-interface Vlan-interface <i>vlan-id</i>	Required By default, the management VLAN interface is used as the NM interface.

Configuring Member Devices

Member device configuration task list

Complete the following tasks to configure the member device:

Task	Remarks
Enabling NDP globally and on specific ports	Required
Enabling NTDP globally and on a specific port	Required
Enabling the cluster function	Required
Accessing the shared FTP/TFTP server from a member device	Optional



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.

Enabling NDP globally and on specific ports

Follow these steps to enable NDP globally and on specific ports:

To do...			Use the command...	Remarks
Enter system view			system-view	—
Enable NDP globally			ndp enable	Required
Enable NDP on specified ports	In system view		ndp enable interface <i>port-list</i>	Required Use either approach.
	In Ethernet port view	Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	
		Enable NDP on the port	ndp enable	

Enabling NTDP globally and on a specific port

Follow these steps to enable NTDP globally and a specific port:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enable NTDP globally		ntdp enable	Required

To do...	Use the command...	Remarks
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable NTDP on the port	ntdp enable	Required

Enabling the cluster function

Follow these steps to enable the cluster function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the cluster function globally	cluster enable	Optional By default, the cluster function is enabled.

Accessing the shared FTP/TFTP server from a member device

Follow these steps to access the shared FTP/TFTP server from a member device:

To do...	Use the command...	Remarks
Access the shared FTP server of the cluster	ftp cluster	Optional Available in user view
Download a file from the shared TFTP server of the cluster	tftp cluster get <i>source-file</i> [<i>destination-file</i>]	Optional Available in user view
Upload a file to the shared TFTP server of the cluster	tftp cluster put <i>source-file</i> [<i>destination-file</i>]	Optional Available in user view

Managing a Cluster through the Management Device

You can manage the member devices through the management device, for example, adding/removing a cluster member, rebooting a member device, logging into a member device, and so on.

Follow these steps to manage a cluster through management device:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter cluster view	cluster	—
Add a candidate device to the cluster	add-member [<i>member-number</i>] mac-address <i>H-H-H</i> [password <i>password</i>]	Optional
Remove a member device from the cluster	delete-member <i>member-number</i>	Optional
Reboot a specified member device	reboot member { <i>member-number</i> mac-address <i>H-H-H</i> } [eraseflash]	Optional

To do...	Use the command...	Remarks
Return to system view	quit	—
Return to user view	quit	—
Switch between management device and member device	cluster switch-to { <i>member-number</i> mac-address <i>H-H-H</i> administrator }	Optional You can use this command switch to the view of a member device and switch back.
Configure the MAC address of the management device	administrator-address <i>mac-address name name</i>	Optional By default, a switch does not belong to any cluster.
Trace a device through MAC address or IP address	tracemac { by-mac <i>mac-address</i> vlan <i>vlan-id</i> by-ip <i>ip-address</i> } [nondp]	Optional Available in any view

Configuring the Enhanced Cluster Features

Enhanced cluster feature overview

1) Cluster topology management function

After the cluster topology becomes stable, you can use the topology management commands on the cluster administrative device to save the topology of the current cluster as the standard topology and back up the standard topology on the Flash memory of the administrative device.

When errors occur to the cluster topology, you can replace the current topology with the standard cluster topology and restore the administrative device using the backup topology on the Flash memory, so that the devices in the cluster can resume normal operation.

With the **display cluster current-topology** command, the switch can display the topology of the current cluster in a tree structure. The output formats include:

- Display the tree structure three layers above or below the specified node.
- Display the topology between two connected nodes.



Note

The topology information is saved as **topology.top** in the Flash memory to the administrative device. You cannot specify the file name manually.

2) Cluster device blacklist function

To ensure stability and security of the cluster, you can use the blacklist to restrict the devices to be added to the cluster. After you add the MAC address of the device that you need to restrict into the cluster blacklist, even if the cluster function is enabled on this device and the device is normally connected to the current cluster, this device cannot join the cluster and participate in the unified management and configuration of the cluster.

Configuring the enhanced cluster features

Complete the following tasks to configure the enhanced cluster feature:

Task	Remarks
Configuring cluster topology management function	Required
Configuring cluster device blacklist	Required

Configuring cluster topology management function

1) Configuration prerequisites

Before configuring the cluster topology management function, make sure that:

- The basic cluster configuration is completed.
- Devices in the cluster work normally.

2) Configuration procedure

Follow these steps to configure cluster topology management function on a management device:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter cluster view	cluster	—
Check the current topology and save it as the standard topology.	topology accept { all [save-to local-flash] mac-address <i>mac-address</i> member-id <i>member-id</i> administrator }	Required
Save the standard topology to the Flash memory of the administrative device	topology save-to local-flash	Required
Restore the standard topology from the Flash memory of the administrative device	topology restore-from local-flash	Optional
Display the detailed information about a single device	display ntdp single-device mac-address <i>mac-address</i>	Optional These commands can be executed in any view.
Display the topology of the current cluster	display cluster current-topology [mac-address <i>mac-address1</i> [to-mac-address <i>mac-address2</i>]] member-id <i>member-id1</i> [to-member-id <i>member-id2</i>]]	
Display the information about the base topology of the cluster	display cluster base-topology [mac-address <i>mac-address</i> member <i>member-id</i>]	
Display the information about all the devices in the base cluster topology	display cluster base-members	



Note

If the management device of a cluster is a slave device in an IRF fabric, the standard topology information is saved only to the local Flash of the master device in the IRF fabric.

Configuring cluster device blacklist

Follow these steps to configure the cluster device blacklist on a management device:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter cluster view	cluster	—
Add the MAC address of a specified device to the cluster blacklist	black-list add-mac <i>mac-address</i>	Optional By default, the cluster blacklist is empty.
Delete the specified MAC address from the cluster blacklist	black-list delete-mac <i>mac-address</i>	Optional
Delete a device from the cluster add this device to the cluster blacklist	delete-member <i>member-id</i> [to-black-list]	Optional
Displays the information about the devices in the cluster blacklist	display cluster black-list	Optional This command can be executed in any view.

Configuring the Cluster Synchronization Function

After a cluster is established, to simplify the access and management to the cluster, you can synchronize the SNMP configurations on the management device and the local user configurations to the member devices of the cluster by configuring the cluster synchronization function.

SNMP configuration synchronization

With this function, you can configure the public SNMP community name, SNMP group, SNMP users and MIB views. These configurations will be synchronized to the member devices of the cluster automatically, which not only simplifies the configurations on the member devices, but also enables the network management station (NMS) to access any member device of the cluster conveniently.



Note

For the SNMP configurations, refer to the *SNMP-RMON Operation* part in this manual.

- 1) Configuration prerequisites

- NDP and NTDP have been enabled on the management device and member devices, and NDP- and NTDP-related parameters have been configured.
- A cluster is established, and you can manage the member devices through the management device.

2) Configuration procedure

Perform the following operations on the management device to synchronize SNMP configurations:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter cluster view	cluster	—
Create a public SNMP community for the cluster	cluster-snmp-agent community { read write } community-name [mib-view view-name]	Required Not configured by default.
Create a public SNMPv3 group for the cluster	cluster-snmp-agent group v3 group-name [authentication privacy] [read-view read-view] [write-view write-view] [notify-view notify-view]	Required Not configured by default.
Add a public SNMPv3 user to the group	cluster-snmp-agent usm-user v3 username groupname [authentication-mode { md5 sha } authpassstring [privacy-mode { des56 privpassstring }]]	Required Not configured by default.
Create or update the public MIB view information for the cluster	cluster-snmp-agent mib-view included view-name oid-tree	Required Not configured by default.



Note

- Perform the above operations on the management device of the cluster.
- Configuring the public SNMP information is equal to executing these configurations on both the management device and the member devices (refer to the *SNMP-RMON Operation* part in this manual), and these configurations will be saved to the configuration files of the management device and the member devices.
- The public SNMP configurations cannot be synchronized to the devices that are on the cluster blacklist.
- If a member device leaves the cluster, the public SNMP configurations will not be removed.

3) Configuration example

Configure the public SNMP information for the cluster on the management device, including the following:

- The read community name is **read_a**
- The write community name is **write_a**
- The group name is **group_a**

- The MIB view name is **mib_a**, which includes all objects of the subtree **org**
- The SNMPv3 user is **user_a**, which belongs to the group **group_a**.

Create a community with the name of **read_a**, allowing read-only access right using this community name.

```
[test_0.Sysname-cluster] cluster-snmp-agent community read read_a
Member 2 succeeded in the read-community configuration.
Member 1 succeeded in the read-community configuration.
Finish to synchronize the command.
```

Create a community with the name of **write_a**, allowing read and write access right using this community name.

```
[test_0.Sysname-cluster] cluster-snmp-agent community write write_a
Member 2 succeeded in the write-community configuration.
Member 1 succeeded in the write-community configuration.
Finish to synchronize the command.
```

Create an SNMP group **group_a**.

```
[test_0.Sysname-cluster] cluster-snmp-agent group v3 group_a
Member 2 succeeded in the group configuration.
Member 1 succeeded in the group configuration.
Finish to synchronize the command.
```

Create a MIB view **mib_a**, which includes all objects of the subtree **org**.

```
[test_0.Sysname-cluster] cluster-snmp-agent mib-view included mib_a org
Member 2 succeeded in the mib-view configuration.
Member 1 succeeded in the mib-view configuration.
Finish to synchronize the command.
```

Add a user **user_a** to the SNMPv3 group **group_a**.

```
[test_0.Sysname-cluster] cluster-snmp-agent usm-user v3 user_a group_a
Member 2 succeeded in the usm-user configuration.
Member 1 succeeded in the usm-user configuration.
Finish to synchronize the command.
```

After the above configuration, you can see that the public SNMP configurations for the cluster are saved to the management device and member devices by viewing the configuration files.

- Configuration file content on the management device (only the SNMP-related information is displayed)

```
[test_0.Sysname-cluster] display current-configuration
#
cluster
 cluster-snmp-agent community read read_a
 cluster-snmp-agent community write write_a
 cluster-snmp-agent group v3 group_a
 cluster-snmp-agent mib-view included mib_a org
 cluster-snmp-agent usm-user v3 user_a group_a
#
snmp-agent
snmp-agent local-engineid 800007DB000FE22405626877
snmp-agent community read read_a@cm0
```

```
snmp-agent community write write_a@cm0
snmp-agent sys-info version all
snmp-agent group v3 group_a
snmp-agent mib-view included mib_a org
snmp-agent usm-user v3 user_a group_a
undo snmp-agent trap enable standard
```

- Configuration file content on a member device (only the SNMP-related information is displayed)

```
<test_2.Sysname> display current-configuration
```

```
#
```

```
snmp-agent
snmp-agent local-engineid 800007DB000FE224055F6877
snmp-agent community read read_a@cm2
snmp-agent community write write_a@cm2
snmp-agent sys-info version all
snmp-agent group v3 group_a
snmp-agent mib-view included mib_a org
snmp-agent usm-user v3 user_a group_a
```

Local user configuration synchronization

With this function, you can create a public local user for the cluster on the management device, and the username and password will be synchronized to the member devices of the cluster, which is equal to creating this local user on all member devices.

The configured local user is a Telnet user, and you can use the public username and password to manage all member devices through Web.

1) Configuration prerequisites

- NDP and NTDP have been enabled on the management device and member devices, and NDP- and NTDP-related parameters have been configured.
- A cluster is established, and you can manage the member devices through the management device.

2) Configuration procedure

Perform the following operations on the management device to synchronize local user configurations:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter cluster view	cluster	—
Create a public local user	cluster-local-user <i>username</i> password { cipher simple } <i>passwordstring</i>	Required Not configured by default.



Note

- Perform the above operations on the management device of the cluster.
- Creating a public local user is equal to executing these configurations on both the management device and the member devices (refer to the *AAA Operation* part in this manual), and these configurations will be saved to the configuration files of the management device and the member devices.
- The public local user configurations cannot be synchronized to the devices that are on the cluster blacklist.
- If a member device leaves the cluster, the public local user configurations will not be removed.

Displaying and Maintaining Cluster Configuration

To do...	Use the command...	Remarks
Display all NDP configuration and running information (including the interval to send NDP packets, the holdtime, and all neighbors discovered)	display ndp	Available in any view.
Display NDP configuration and running information on specified ports (including the neighbors discovered by NDP on the ports)	display ndp interface <i>port-list</i>	
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 <i>H-H-H</i> verbose]	
Display information about the member devices of the cluster	display cluster members [<i>member-number</i> verbose]	Available in user view.
Clear the statistics on NDP ports	reset ndp statistics [interface <i>port-list</i>]	



Note

When you display the cluster topology information, the devices attached to the switch that is listed in the blacklist will not be displayed.

Cluster Configuration Examples

Basic Cluster Configuration Example

Network requirements

Three switches compose a cluster, where:

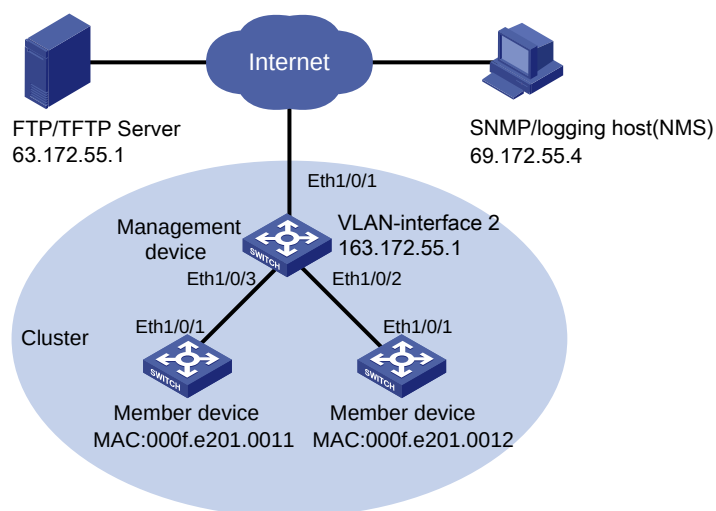
- An S3600 series switch serves as the management device.
- The rest are member devices.

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 Ethernet 1/0/2 and Ethernet 1/0/3.
- The management device connects to the Internet through Ethernet 1/0/1.
- Ethernet 1/0/1 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.

Network diagram

Figure 1-4 Network diagram for HGMP cluster configuration



Configuration procedure

1) Configure the member devices (taking one member as an example)

Enable NDP globally and on Ethernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] ndp enable
```

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] ndp enable
```

```
[Sysname-Ethernet1/0/1] quit
```

Enable NTDP globally and on Ethernet 1/0/1.

```
[Sysname] ntdp enable
```

```

[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] ntdp enable
[Sysname-Ethernet1/0/1] quit

# Enable the cluster function.

[Sysname] cluster enable
2) Configure the management device

# Add port Ethernet 1/0/1 to VLAN 2.

<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port Ethernet 1/0/1
[Sysname-vlan2] quit

# Configure the IP address of VLAN-interface 2 as 163.172.55.1.

[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] ip address 163.172.55.1 255.255.255.0
[Sysname-Vlan-interface2] quit

# Disable NDP on the uplink port Ethernet 1/0/1.

[Sysname] ndp enable
[Sysname] undo ndp enable interface Ethernet 1/0/1
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] undo ntdp enable
[Sysname-Ethernet1/0/1] quit

# Enable NDP on Ethernet 1/0/2 and Ethernet 1/0/3.

[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] ndp enable
[Sysname-Ethernet1/0/2] quit
[Sysname] interface Ethernet 1/0/3
[Sysname-Ethernet1/0/3] ndp enable
[Sysname-Ethernet1/0/3] quit

# Set the hold time of NDP information to 200 seconds.

[Sysname] ndp timer aging 200

# Set the interval between sending NDP packets to 70 seconds.

[Sysname] ndp timer hello 70

# Enable NTDP globally and on Ethernet 1/0/2 and Ethernet 1/0/3.

[Sysname] ntdp enable
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] ntdp enable
[Sysname-Ethernet1/0/2] quit
[Sysname] interface Ethernet 1/0/3
[Sysname-Ethernet1/0/3] ntdp enable
[Sysname-Ethernet1/0/3] quit

# Set the topology collection range to 2 hops.

[Sysname] ntdp hop 2

# Set the delay for a member device to forward topology collection requests to 150 ms.

```



```

[Sysname] ntdp timer hop-delay 150

# Set the delay for a member device port to forward topology collection requests to 15 ms.
[Sysname] ntdp timer port-delay 15

# Set the interval between collecting topology information to 3 minutes.
[Sysname] ntdp timer 3

# Enable the cluster function.
[Sysname] cluster enable

# Enter cluster view.
[Sysname] cluster
[Sysname-cluster]

# Configure a private IP address pool for the cluster. The IP address pool contains six IP addresses,
starting from 172.16.0.1.
[Sysname-cluster] ip-pool 172.16.0.1 255.255.255.248

# Name and build the cluster.
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster]

# Add the attached two switches to the cluster.
[aaa_0.Sysname-cluster] add-member 1 mac-address 000f-e201-0011
[aaa_0.Sysname-cluster] add-member 17 mac-address 000f-e201-0012

# Set the holdtime of member device information to 100 seconds.
[aaa_0.Sysname-cluster] holdtime 100

# Set the interval between sending handshake packets to 10 seconds.
[aaa_0.Sysname-cluster] timer 10

# Configure VLAN-interface 2 as the network management interface.
[aaa_0.Sysname-cluster] nm-interface Vlan-interface 2

# Configure the shared FTP server, TFTP server, logging host and SNMP host for the cluster.
[aaa_0.Sysname-cluster] ftp-server 63.172.55.1
[aaa_0.Sysname-cluster] tftp-server 63.172.55.1
[aaa_0.Sysname-cluster] logging-host 69.172.55.4
[aaa_0.Sysname-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 attached to 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.Sysname> ftp cluster

# Download the file named aaa.txt from the shared TFTP server of the cluster to the member device.
<aaa_1.Sysname> 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.Sysname> 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.

Network Management Interface Configuration Example

Network requirements

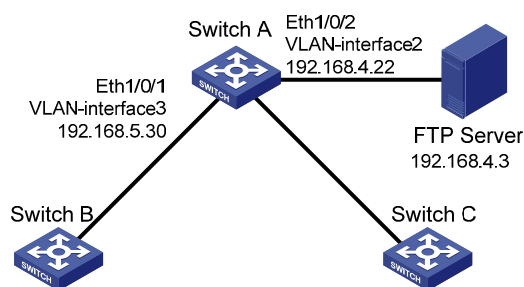
- Configure VLAN-interface 2 as the network management interface of the switch;
- Configure VLAN 3 as the management VLAN;
- The IP address of the FTP server is 192.168.4.3;
- Switch A operates as the management switch;
- Switch B and Switch C are member switches.

Table 1-2 Connection information of the management switch

VLAN	IP address	Connection port
VLAN 3 (connected to Switch B)	192.168.5.30/24	Ethernet 1/0/1
VLAN 2 (connected to FTP server)	192.168.4.22/24	Ethernet 1/0/2

Network diagram

Figure 1-5 Network diagram for network management interface configuration



Configuration procedure

Enter system view and configure VLAN 3 as the management VLAN.

```
<Sysname> system-view
```

```
[Sysname] management-vlan 3
```

```

# Add Ethernet 1/0/1 to VLAN 3.
[Sysname] vlan 3
[Sysname-vlan3] port Ethernet 1/0/1
[Sysname-vlan3] quit

# Set the IP address of VLAN-interface 3 to 192.168.5.30.
[Sysname] interface Vlan-interface 3
[Sysname-Vlan-interface3] ip address 192.168.5.30 255.255.255.0
[Sysname-Vlan-interface3] quit

# Add Ethernet 1/0/2 to VLAN 2.
[Sysname] vlan 2
[Sysname-vlan2] port Ethernet 1/0/2
[Sysname-vlan2] quit

# Set the IP address of VLAN-interface 2 to 192.168.4.22.
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] ip address 192.168.4.22 255.255.255.0
[Sysname-Vlan-interface2] quit

# Enable the cluster function.
[Sysname] cluster enable

# Enter cluster view.
[Sysname] cluster
[Sysname-cluster]

# Configure a private IP address pool for the cluster. The IP address pool contains 30 IP addresses,
starting from 192.168.5.1.
[Sysname-cluster] ip-pool 192.168.5.1 255.255.255.224

# Name and build the cluster.
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster]

# Configure VLAN-interface 2 as the network management interface.
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] nm-interface Vlan-interface 2

```

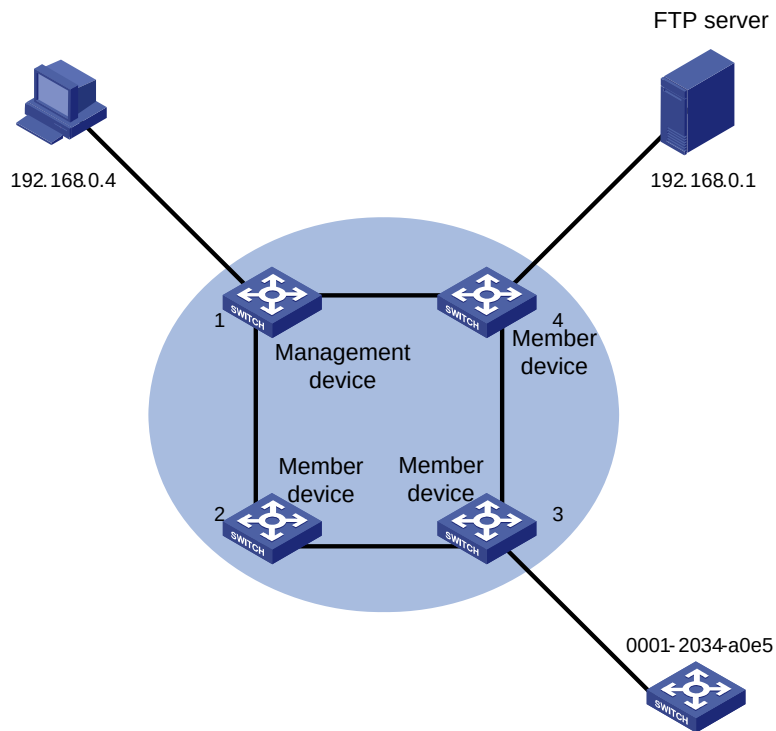
Enhanced Cluster Feature Configuration Example

Network requirements

- The cluster operates properly.
- Add the device with the MAC address 0001-2034-a0e5 to the cluster blacklist, that is, prevent the device from being managed and maintained by the cluster.
- Save the current cluster topology as the base topology and save it in the flash of the local management device in the cluster.

Network diagram

Figure 1-6 Network diagram for the enhanced cluster feature configuration



Configuration procedure

Enter cluster view.

```
<aaa_0.Sysname> system-view
```

```
[aaa_0.Sysname] cluster
```

Add the MAC address 0001-2034-a0e5 to the cluster blacklist.

```
[aaa_0.Sysname-cluster] black-list add-mac 0001-2034-a0e5
```

Backup the current topology.

```
[aaa_0.Sysname-cluster] topology accept all save-to local-flash
```

Table of Contents

1 PoE Configuration	1-1
PoE Overview	1-1
Introduction to PoE	1-1
PoE Features Supported by S3600	1-1
PoE Configuration	1-2
PoE Configuration Task List	1-2
Enabling the PoE Feature on a Port	1-3
Setting the Maximum Output Power on a Port	1-3
Setting PoE Management Mode and PoE Priority of a Port	1-4
Setting the PoE Mode on a Port	1-4
Configuring the PD Compatibility Detection Function	1-5
Configuring PoE Over-Temperature Protection on the Switch	1-5
Upgrading the PSE Processing Software Online	1-6
Upgrading the PSE Processing Software of Fabric Switches Online	1-6
Displaying PoE Configuration	1-7
PoE Configuration Example	1-7
PoE Configuration Example	1-7
2 PoE Profile Configuration	2-1
Introduction to PoE Profile	2-1
PoE Profile Configuration	2-1
Configuring PoE Profile	2-1
Displaying PoE Profile Configuration	2-3
PoE Profile Configuration Example	2-3
PoE Profile Application Example	2-3

1 PoE Configuration

When configuring PoE, go to these sections for information you are interested in:

- [PoE Overview](#)
- [PoE Configuration](#)
- [PoE Configuration Example](#)



Note

The newly added function is upgrading the PoE module of the fabric switch remotely. See [Upgrading the PSE Processing Software of Fabric Switches Online](#) for details.

PoE Overview

Introduction to PoE

Power over Ethernet (PoE)-enabled devices use twisted pairs through electrical ports to supply power to the remote powered devices (PD) in the network and implement power supply and data transmission simultaneously.

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, network cameras, and data collection system.

PoE components

PoE consists of three components: power sourcing equipment (PSE), PD, and power interface (PI).

- 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.
- 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, Wireless APs, network cameras and so on.
- PI: PIs are RJ45 interfaces which connect PSE/PDs to network cables.

PoE Features Supported by S3600

PoE-enabled S3600 series Ethernet switches include:

- S3600-28P-PWR-SI
- S3600-28P-PWR-EI
- S3600-52P-PWR-SI
- S3600-52P-PWR-EI

A PoE-enabled S3600 switch has the following features:

- As the PSE, it supports the IEEE802.3af standard. It can also supply power to the PDs that do not support the 802.3af standard.
- It can deliver data and current simultaneously through data wires (1,2,3,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 electrical 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. The switch 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 W/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°C (149°F) for self-protection, and restores the PoE feature on all its ports when the temperature drops below 60°C (140°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 you use the PoE-enabled S3600 switch to supply power, the PDs need no external power supply.
 - If a remote PD has an external power supply, the PoE-enabled S3600 switch and the external power supply will backup each other for the PD.
 - Only the 100 Mbps Ethernet electrical ports of the PoE-enabled S3600 switch support the PoE feature.
-

PoE Configuration

PoE Configuration Task List

Complete the following tasks to configure PoE configuration:

Task	Remarks
Enabling the PoE Feature on a Port	Required
Setting the Maximum Output Power on a Port	Optional
Setting PoE Management Mode and PoE Priority of a Port	Optional
Setting the PoE Mode on a Port	Optional
Configuring the PD Compatibility Detection Function	Optional
Configuring PoE Over-Temperature Protection on the Switch	Optional
Upgrading the PSE Processing Software Online	Optional
Upgrading the PSE Processing Software of Fabric Switches Online	Optional
Displaying PoE Configuration	Optional

Enabling the PoE Feature on a Port

Follow these steps to enable the PoE feature on a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the PoE feature on a port	poe enable	Required



Caution

- By default, the PoE function on a port is enabled by the default configuration file (config.def) 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.

Setting the Maximum Output Power on a Port

The maximum power that can be supplied by each Ethernet electrical port of 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.

Follow these steps to set the maximum output power on a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—

To do...	Use the command...	Remarks
Set the maximum output power on the port	poe max-power <i>max-power</i>	Required 15,400 mW by default.

Setting PoE Management Mode and PoE Priority of a Port

When a switch is close to its full load in supplying power, you can adjust the power supply of the switch through the cooperation of the PoE management mode and the port PoE priority settings. S3600 series switches support two PoE management modes, auto and manual. The auto mode is adopted by default.

- **auto:** 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 port number.
- **manual:** 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.

Follow these steps to set the PoE management mode and PoE priority of a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the PoE management mode for the switch	poe power-management { auto manual }	Required auto by default.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Set the PoE priority of a port	poe priority { critical high low }	Required low by default.

Setting the PoE Mode on a Port

PoE mode of a port falls into two types, signal mode and spare mode.

- Signal mode: DC power is carried over the data pairs (1,2,3,and 6) of category-3/5 twisted pairs.
- Spare mode: DC power is carried over the spare pairs (4,5,7,and 8) of category-3/5 twisted pairs.

Currently, S3600 series Ethernet switches do not support the spare mode.

After the PoE feature is enabled on the port, perform the following configuration to set the PoE mode on a port.

Follow these steps to set the PoE mode on a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Set the PoE mode on the port to signal	poe mode signal	Optional signal by default.

Configuring the PD Compatibility Detection Function

After the PD compatibility detection function is enabled, the switch can detect the PDs that do not conform to the 802.3af standard and supply power to them.

After the PoE feature is enabled, perform the following configuration to enable the PD compatibility detection function.

Follow these steps to configure the PD compatibility detection function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the PD compatibility detection function	poe legacy enable	Required Disabled by default.

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°C (149°F) for self-protection, and restores the PoE feature settings on all its ports when the temperature drops below 60°C (140°F).

Follow these steps to configure PoE over-temperature protection on the switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable PoE over-temperature protection on the switch	poe temperature-protection enable	Optional Enabled by default.



Note

- When the internal temperature of the switch decreases from X ($X > 65^{\circ}\text{C}$, or $X > 149^{\circ}\text{F}$) to Y ($60^{\circ}\text{C} \leq Y < 65^{\circ}\text{C}$, or $140^{\circ}\text{F} \leq Y < 149^{\circ}\text{F}$), the switch still keeps the PoE function disabled on all the ports.
- When the internal temperature of the switch increases from X ($X < 60^{\circ}\text{C}$, or $X < 140^{\circ}\text{F}$) to Y ($60^{\circ}\text{C} < Y \leq 65^{\circ}\text{C}$, or $140^{\circ}\text{F} < Y \leq 149^{\circ}\text{F}$), the switch still keeps the PoE function enabled on all the ports.

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. Before performing the following configuration, download the PSE processing software to the Flash of the switch.

Follow these steps to upgrade PSE processing software online:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Upgrade the PSE processing software online	poe update { refresh full } filename	Required The specified PSE processing software is a file with the extension .s19.



Note

- In the case that the PSE processing software is damaged (that is, no **PoE** command can be executed successfully), use the **full** update mode to upgrade and thus restore the software.
- The **refresh** update mode is to upgrade the original processing software in the PSE through refreshing the software, while the **full** update mode is to delete the original processing software in PSE completely and then reload the software.
- Generally, the **refresh** update mode is used to upgrade the PSE processing 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.

Upgrading the PSE Processing Software of Fabric Switches Online

You can update or repair the damaged PSE processing software through upgrading it.

By executing the following command on any device in the fabric, you can upgrade the PSE processing software of all devices in the fabric by using the specified PSE processing software. For details of fabric, see the IRF Fabric part of this manual.

Follow these steps to upgrade the PSE processing software online:

To do...	Use the command...	Remarks
Upgrade the PSE processing software of the fabric switch online	update fabric { file-url device-name file-url }	Optional

Displaying PoE Configuration

To do...	Use the command...	Remarks
Display the PoE status of a specific port or all ports of the switch	display poe interface [<i>interface-type interface-number</i>]	Available in any view
Display the PoE power information of a specific port or all ports of the switch	display poe interface power [<i>interface-type interface-number</i>]	
Display the PSE parameters	display poe powersupply	
Display the status (enabled/disabled) of the PoE over-temperature protection feature on the switch	display poe temperature-protection	

PoE Configuration Example

PoE Configuration Example

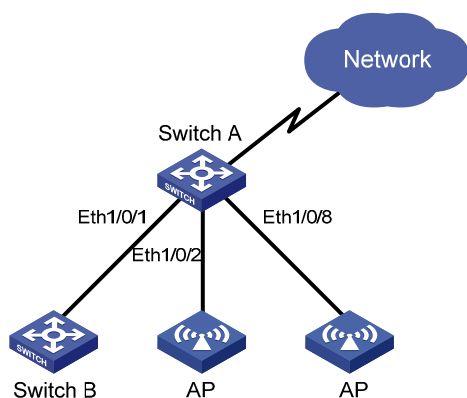
Network requirements

Switch A is an S3600 series Ethernet switch supporting PoE, Switch B can be PoE powered.

- The Ethernet 1/0/1 and Ethernet 1/0/2 ports of Switch A are connected to Switch B and an AP respectively; the Ethernet 1/0/8 port is intended to be connected with an important AP.
- The PSE processing software of Switch A is first upgraded online. The remotely accessed PDs are powered by Switch A.
- The power consumption of the accessed AP is 2,500 mW, and the maximum power consumption of Switch B is 12,000 mW.
- It is required to guarantee the power feeding to the PDs connected to the Ethernet 1/0/8 port even when Switch A is under full load.

Network diagram

Figure 1-1 Network diagram for PoE



Configuration procedure

Upgrade the PSE processing software online.

```
<SwitchA> system-view
```

```
[SwitchA] poe update refresh 0290_021.s19
```

Enable the PoE feature on Ethernet 1/0/1, and set the PoE maximum output power of Ethernet 1/0/1 to 12,000 mW.

```
[SwitchA] interface Ethernet 1/0/1
[SwitchA-Ethernet1/0/1] poe enable
[SwitchA-Ethernet1/0/1] poe max-power 12000
[SwitchA-Ethernet1/0/1] quit
```

Enable the PoE feature on Ethernet 1/0/2, and set the PoE maximum output power of Ethernet 1/0/2 to 2500 mW.

```
[SwitchA] interface Ethernet 1/0/2
[SwitchA-Ethernet1/0/2] poe enable
[SwitchA-Ethernet1/0/2] poe max-power 2500
[SwitchA-Ethernet1/0/2] quit
```

Enable the PoE feature on Ethernet 1/0/8, and set the PoE priority of Ethernet 1/0/8 to critical.

```
[SwitchA] interface Ethernet 1/0/8
[SwitchA-Ethernet1/0/8] poe enable
[SwitchA-Ethernet1/0/8] poe priority critical
[SwitchA-Ethernet1/0/8] quit
```

Set the PoE management mode on the switch to auto (it is the default mode, so this step can be omitted).

```
[SwitchA] poe power-management auto
```

Enable the PD compatibility detect of the switch to allow the switch to supply power to the devices noncompliant with the 802.3af standard.

```
[SwitchA] poe legacy enable
```

2 PoE Profile Configuration

When configuring PoE profile, go to these sections for information you are interested in:

- [Introduction to PoE Profile](#)
- [PoE Profile Configuration](#)
- [Displaying PoE Profile Configuration](#)
- [PoE Profile Configuration Example](#)

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. A PoE profile is a set of PoE configurations, including multiple PoE 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.

PoE Profile Configuration

Configuring PoE Profile

Follow these steps to configure PoE profile:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a PoE profile and enter PoE profile view	poe-profile <i>profilename</i>	Required If the PoE file is created, you will enter PoE profile view directly through the command.

To do...			Use the command...	Remarks
Configure the relevant features in PoE profile	Enable the PoE feature on a port		poe enable	Required Disabled by default.
	Configure PoE mode for Ethernet ports		poe mode { signal spare }	Optional signal by default.
	Configure the PoE priority for Ethernet ports		poe priority { critical high low }	Optional low by default.
	Configure the maximum power for Ethernet ports		poe max-power <i>max-power</i>	Optional 15,400 mW by default.
Quit system view			quit	—
Apply the existing PoE profile to the specified Ethernet port	In system view		apply poe-profile <i>profile-name</i> interface <i>interface-type</i> <i>interface-number</i> [to <i>interface-type interface-number</i>]	Use either approach.
	In Ethernet port view	Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	
		Apply the existing PoE profile to the port	apply poe-profile <i>profile-name</i>	

Note the following during the configuration:

- When the **apply poe-profile** command is used to apply a PoE profile to a port, some PoE features in the PoE profile can be applied successfully while some 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 profile is applied to a port. However, the command cannot be used to query which PoE features in a PoE profiles are applied successfully.
- 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.

Displaying PoE Profile Configuration

To do...	Use the command...	Remarks
Display the detailed information about the PoE profiles created on the switch	display poe-profile { all-profile interface <i>interface-type interface-number</i> name <i>profile-name</i> }	Available in any view

PoE Profile Configuration Example

PoE Profile Application Example

Network requirements

Switch A is an S3600 series Ethernet switch supporting PoE.

Ethernet 1/0/1 through Ethernet 1/0/10 of Switch A are used by users of group A, who have the following requirements:

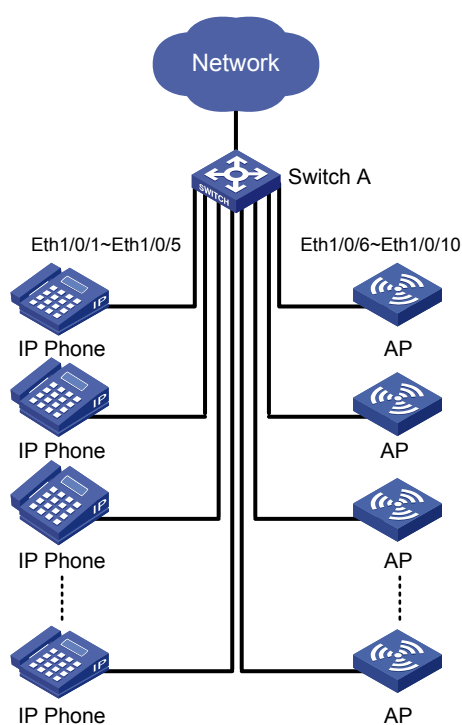
- The PoE function can be enabled on all ports in use.
- Signal mode is used to supply power.
- The PoE priority for Ethernet 1/0/1 through Ethernet 1/0/5 is Critical, whereas the PoE priority for Ethernet 1/0/6 through Ethernet 1/0/10 is High.
- The maximum power for Ethernet 1/0/1 through Ethernet 1/0/5 ports is 3000 mW, whereas the maximum power for Ethernet 1/0/6 through Ethernet 1/0/10 is 15400 mW.

Based on the above requirements, two PoE profiles are made for users of group A.

- Apply PoE profile 1 for Ethernet 1/0/1 through Ethernet 1/0/5;
- Apply PoE profile 2 for Ethernet 1/0/6 through Ethernet 1/0/10.

Network diagram

Figure 2-1 PoE profile application



Configuration procedure

Create Profile 1, and enter PoE profile view.

```
<SwitchA> system-view  
[SwitchA] poe-profile Profile1
```

In Profile 1, add the PoE policy configuration applicable to Ethernet 1/0/1 through Ethernet 1/0/5 ports for users of group A.

```
[SwitchA-poe-profile-Profile1] poe enable  
[SwitchA-poe-profile-Profile1] poe mode signal  
[SwitchA-poe-profile-Profile1] poe priority critical  
[SwitchA-poe-profile-Profile1] poe max-power 3000  
[SwitchA-poe-profile-Profile1] quit
```

Display detailed configuration information for Profile1.

```
[SwitchA] display poe-profile name Profile1  
Poe-profile: Profile1, 3 action  
poe enable  
poe max-power 3000  
poe priority critical
```

Create Profile 2, and enter PoE profile view.

```
[SwitchA] poe-profile Profile2
```

In Profile 2, add the PoE policy configuration applicable to Ethernet 1/0/6 through Ethernet 1/0/10 ports for users of group A.

```
[SwitchA-poe-profile-Profile2] poe enable  
[SwitchA-poe-profile-Profile2] poe mode signal
```

```
[SwitchA-poe-profile-Profile2] poe priority high
[SwitchA-poe-profile-Profile2] poe max-power 15400
[SwitchA-poe-profile-Profile2] quit
```

Display detailed configuration information for Profile2.

```
[SwitchA] display poe-profile name Profile2
Poe-profile: Profile2, 2 action
poe enable
poe priority high
```

Apply the configured Profile 1 to Ethernet 1/0/1 through Ethernet 1/0/5 ports.

```
[SwitchA] apply poe-profile Profile1 interface Ethernet1/0/1 to Ethernet1/0/5
```

Apply the configured Profile 2 to Ethernet 1/0/6 through Ethernet 1/0/10 ports.

```
[SwitchA] apply poe-profile Profile2 interface Ethernet1/0/6 to Ethernet1/0/10
```

Table of Contents

1 UDP Helper Configuration	1-1
Introduction to UDP Helper	1-1
Configuring UDP Helper	1-2
Displaying and Maintaining UDP Helper	1-3
UDP Helper Configuration Example	1-3
Cross-Network Computer Search Through UDP Helper	1-3

1 UDP Helper Configuration

When configuring UDP helper, go to these sections for information you are interested in:

- [Introduction to UDP Helper](#)
- [Configuring UDP Helper](#)
- [Displaying and Maintaining UDP Helper](#)
- [UDP Helper Configuration Example](#)



Note

Support for the UDP Helper TTL-keep function is added. For details, refer to [Configuring UDP Helper](#).

Introduction to UDP Helper

Sometimes, a host needs to forward broadcasts to obtain network configuration information or request the names of other devices on the network. However, if the server or the device to be requested is located in another broadcast domain, the host cannot obtain such information through broadcast.

To solve this problem, S3600 series Ethernet switches provide the UDP Helper function to relay specified UDP packets. In other words, UDP Helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specified destination server.

With UDP Helper enabled, the device decides whether to forward a received UDP broadcast packet according to the UDP destination port number of the packet.

- If the destination port number of the packet matches the one pre-configured on the device, 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 the upper layer protocol for processing.

By default, to prevent IP broadcast storm, S3600 series Ethernet switches do not forward IP packets with the TTL field being 0 or 1. In some cases, however, you may need to enable UDP Helper to forward broadcasts with the TTL field being 1. To meet this need, S3600 series Ethernet switches provide the UDP Helper TTL-keep feature, which allows forwarding of broadcasts with the TTL field being 1 without decrementing the TTL value by one.



Note

Relay forwarding of BOOTP/DHCP broadcast packets is implemented by the DHCP relay function using UDP ports 67 and 68, so these two ports cannot be configured as UDP Helper relay ports.

By default, with UDP Helper enabled, the device forwards broadcast packets with the six UDP destination port numbers listed in [Table 1-1](#).

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

Configuring UDP Helper

Follow these steps to configure UDP Helper:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable UDP Helper	udp-helper enable	Required Disabled by default.
Specify a UDP port number	udp-helper port { <i>port-number</i> <i>dns</i> <i>netbios-ds</i> <i>netbios-ns</i> <i>tacacs</i> <i>tftp</i> <i>time</i> }	Optional By default, the device enabled with UDP Helper forwards the broadcast packets containing any of the six port numbers 53, 138, 137, 49, 69 and 37.
Enable the UDP Helper TTL-keep function	udp-helper ttl-keep enable	Optional Disabled by default. That is, UDP Helper does not forward IP broadcasts with the TTL field being 1.
Enter VLAN interface view	interface <i>Vlan-interface</i> <i>vlan-id</i>	—
Specify the destination server to which the UDP packets are to be forwarded	udp-helper server <i>ip-address</i>	Required No destination server is specified by default.



Note

- On an S3600 Series Ethernet Switch, the reception of directed broadcast packets to a directly connected network is disabled by default. As a result, UDP Helper is available only when the **ip forward-broadcast** command is configured in system view. For details about the **ip forward-broadcast** command, refer to the *IP Address and Performance* part of this manual.
- You need to enable UDP Helper before specifying any UDP port to match UDP broadcasts; otherwise, the configuration fails. When the UDP helper function is disabled, all configured UDP ports are disabled, including the default ports.
- 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.
- You can specify up to 20 destination server addresses on a VLAN interface.
- If UDP Helper is enabled after a destination server is configured for a VLAN interface, the broadcasts from interfaces belonging to the VLAN and having a matching UDP port will be unicast to the destination server.

Displaying and Maintaining UDP Helper

To do...	Use the command...	Remarks
Display the UDP broadcast relay forwarding information of a specified VLAN interface on the switch	display udp-helper server [interface vlan-interface <i>vlan-id</i>]	Available in any view
Clear statistics about packets forwarded by UDP Helper	reset udp-helper packet	Available in user view

UDP Helper Configuration Example

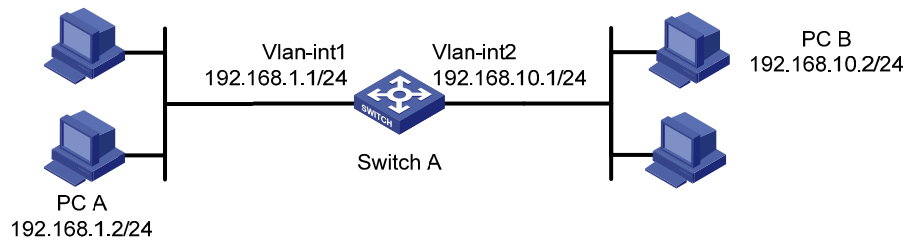
Cross-Network Computer Search Through UDP Helper

Network requirements

PC A resides on network segment 192.168.1.0/24 and PC B on 192.168.10.0/24; they are connected through Switch A and are routable to each other. It is required to configure UDP Helper on the switch, so that PC A can find PC B through computer search. (Broadcasts with UDP port 137 are used for searching.)

Network diagram

Figure 1-1 Network diagram for UDP Helper configuration



Configuration procedure

Enable Switch A to receive directed broadcasts to a directly connected network.

```
<SwitchA> system-view
```

```
[SwitchA] ip forward-broadcast
```

Enable UDP Helper on Switch A.

```
[SwitchA] udp-helper enable
```

Configure the switch to forward broadcasts containing the destination UDP port number 137. (By default, the device enabled with UDP Helper forwards the broadcasts containing the destination UDP port number 137.)

```
[SwitchA] udp-helper port 137
```

Specify the destination server IP address on Vlan-interface 1.

```
[SwitchA] interface Vlan-interface 1
```

```
[SwitchA-Vlan-interface1] udp-helper server 192.168.10.2
```

Enable the UDP Helper TTL-keep function on Switch A.

```
[SwitchA] udp-helper ttl-keep enable
```

Table of Contents

1 SNMP Configuration	1-1
SNMP Overview	1-1
SNMP Operation Mechanism	1-1
SNMP Versions	1-1
Supported MIBs	1-2
Configuring Basic SNMP Functions	1-3
Configuring Trap-Related Functions	1-6
Configuring Basic Trap Functions	1-6
Configuring Extended Trap Function	1-6
Enabling Logging for Network Management	1-7
Displaying SNMP	1-7
SNMP Configuration Example	1-8
SNMP Configuration Example	1-8
2 RMON Configuration	2-1
Introduction to RMON	2-1
Working Mechanism of RMON	2-1
Commonly Used RMON Groups	2-2
RMON Configuration	2-3
Displaying RMON	2-4
RMON Configuration Example	2-4

1 SNMP Configuration

When configuring SNMP, go to these sections for information you are interested in:

- [SNMP Overview](#)
- [Configuring Basic SNMP Functions](#)
- [Configuring Trap-Related Functions](#)
- [Enabling Logging for Network Management](#)
- [Displaying SNMP](#)
- [SNMP Configuration Example](#)

SNMP Overview

The Simple Network Management Protocol (SNMP) 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 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.

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 (such as switches).

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 on the managed object (MIB, Management Information Base) according to the message types, generates the corresponding Response packets and returns them to the NMS.

When a network device operates improperly or changes to other state, the agent on it can also send traps on its own initiative to the NMS to report the events.

SNMP Versions

Currently, SNMP agent on a switch 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.

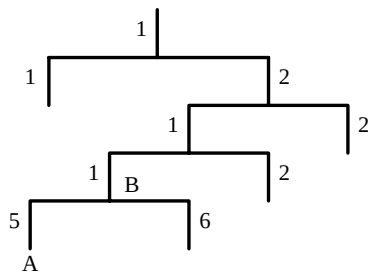
- Specifying MIB view that a community can access.

- 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 the switch information, while those with read-write permission can configure the switch as well.
- Set the basic ACL specified by the community name.

Supported MIBs

An SNMP packet carries management variables with it. Management variable is used to describe the management objects of a switch. To uniquely identify the management objects of the switch, 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



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 (OID) of the managed object. The common MIBs supported by switches 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	RFC 1213
	BRIDGE MIB	RFC 1493
		RFC 2675
	RIP MIB	RFC 1724
	RMON MIB	RFC 2819
	Ethernet MIB	RFC 2665
	OSPF MIB	RFC 1253
	IF MIB	RFC 1573
Private MIB	DHCP MIB QACL MIB MSTP MIB VLAN MIB IPV6 ADDRESS MIB MIRRORGROUP MIB QINQ MIB 802.x MIB HGMP MIB NTP MIB Device management Interface management	—

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 the following two tables.

Switches now support configuring SNMPv3 users by using the Advanced Encryption Standard (AES), which is the new encryption standard in place of Data Encryption Standard (DES).

Follow these steps to configure basic SNMP functions (SNMPv1 and SNMPv2c):

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable SNMP agent	snmp-agent	Optional Disabled by default. You can enable SNMP agent by executing this command or any of the commands used to configure SNMP agent.

To do...			Use the command...	Remarks
Set system information, and specify to enable SNMPv1 or SNMPv2c on the switch			snmp-agent sys-info { contact <i>sys-contact</i> location <i>sys-location</i> version { { v1 v2c v3 }* all } }	Required By default, the contact information for system maintenance is "Hangzhou H3C Technologies Co., Ltd.", the system location is "Hangzhou China", and the SNMP version is SNMPv3.
Set a community name and access permission	Direct configuration	Set a community name	snmp-agent community { read write } <i>community-name</i> [acl <i>acl-number</i> mib-view <i>view-name</i>]*	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.
	Indirect configuration	Set an SNMP group	snmp-agent group { v1 v2c } <i>group-name</i> [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-number</i>]	
		Add a user to an SNMP group	snmp-agent usm-user { v1 v2c } <i>user-name</i> <i>group-name</i> [acl <i>acl-number</i>]	
Set the maximum size of an SNMP packet for SNMP agent to receive or send			snmp-agent packet max-size <i>byte-count</i>	Optional 1,500 bytes by default.
Set the device engine ID			snmp-agent local-engineid <i>engineid</i>	Optional By default, the device engine ID is “enterprise number + device information”.
Create/Update the view information			snmp-agent mib-view { included excluded } <i>view-name</i> <i>oid-tree</i> [mask <i>mask-value</i>]	Optional By default, the view name is ViewDefault and OID is 1.

Follow these steps to configure basic SNMP functions (SNMPv3):

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable SNMP agent	snmp-agent	Optional Disabled by default. You can enable SNMP agent by executing this command or any of the commands used to configure SNMP agent.

To do...	Use the command...	Remarks
Set system information and specify to enable SNMPv3 on the switch	snmp-agent sys-info { contact <i>sys-contact</i> location <i>sys-location</i> version { { v1 v2c v3 }* all } }	Optional By default, the contact information for system maintenance is "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 <i>group-name</i> [authentication privacy] [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-number</i>]	Required
Encrypt a plain-text password to generate a cipher-text one	snmp-agent calculate-password <i>plain-password</i> mode { md5 sha } { local-engineid specified-engineid <i>engineid</i> }	Optional This command is used if password in cipher-text is needed for adding a new user.
Add a user to an SNMP group	snmp-agent usm-user v3 <i>user-name</i> <i>group-name</i> [[cipher] authentication-mode { md5 sha } <i>auth-password</i> [privacy-mode { des56 aes128 } <i>priv-password</i>]] [acl <i>acl-number</i>]	Required
Set the maximum size of an SNMP packet for SNMP agent to receive or send	snmp-agent packet max-size <i>byte-count</i>	Optional 1,500 bytes by default.
Set the device engine ID	snmp-agent local-engineid <i>engineid</i>	Optional By default, the device engine ID is "enterprise number + device information".
Create or update the view information	snmp-agent mib-view { included excluded } <i>view-name</i> <i>oid-tree</i> [mask <i>mask-value</i>]	Optional By default, the view name is ViewDefault and OID is 1.



Note

An S3600 Ethernet switch provides the following functions to prevent attacks through unused UDP ports.

- Executing the **snmp-agent** command or any of the commands used to configure SNMP agent enables the SNMP agent, and at the same opens UDP port 161 used by SNMP agents and the UDP port used by SNMP trap respectively.
- Executing the **undo snmp-agent** command disables the SNMP agent and closes UDP ports used by SNMP agent and SNMP trap as well.

Configuring Trap-Related Functions

Configuring Basic Trap Functions

traps 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).

Note that basic SNMP configuration is performed before you configure basic trap function.

Follow these steps to configure basic trap function:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enable the switch to send traps to NMS		snmp-agent trap enable [configuration flash ospf [<i>process-id</i>] [<i>ospf-trap-list</i>]] 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 traps	Enter port view or interface view	interface <i>interface-type interface-number</i>	
	Enable the port or interface to send traps	enable snmp trap updown	
	Quit to system view	quit	
Set the destination for traps		snmp-agent target-host trap address udp-domain { <i>ip-address</i> } [udp-port <i>port-number</i>] params securityname <i>security-string</i> [v1 v2c v3 [authentication privacy]]	Required
Set the source address for traps		snmp-agent trap source <i>interface-type interface-number</i>	Optional
Set the size of the queue used to hold the traps to be sent to the destination host		snmp-agent trap queue-size <i>size</i>	Optional The default is 100.
Set the aging time for traps		snmp-agent trap life <i>seconds</i>	Optional 120 seconds by default.

Configuring Extended Trap Function

The extended trap function refers to adding “interface description” and “interface type” into the linkUp/linkDown trap. When receiving this extended trap, NMS can immediately determine which interface on the device fails according to the interface description and type.

Follow these steps to configure extended trap function:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the extended trap function	snmp-agent trap ifmib link extended	Optional By default, the linkUp/linkDown trap adopts the standard format defined in IF-MIB. For details, refer to RFC 1213.

Enabling Logging for Network Management

Follow these steps to enable logging for network management:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable logging for network management	snmp-agent log { set-operation get-operation all }	Optional Disabled by default.



Note

- When SNMP logging is enabled on a device, SNMP logs are output to the information center of the device. With the output destinations of the information center set, the output destinations of SNMP logs will be decided.
- The severity level of SNMP logs is informational, that is, the logs are taken as general prompt information of the device. To view SNMP logs, you need to enable the information center to output system information with **informational** level.
- For detailed description on system information and information center, refer to the *Information Center Configuration* part in this manual.

Displaying SNMP

To do...	Use the command...	Remarks
Display the SNMP information about the current device	display snmp-agent sys-info [contact location version]*	Available 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 [<i>group-name</i>]	
Display SNMP user information	display snmp-agent usm-user [engineid <i>engineid</i> username <i>user-name</i> group <i>group-name</i>]*	

To do...	Use the command...	Remarks
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]	

SNMP Configuration Example

SNMP Configuration Example

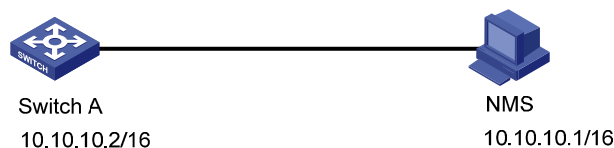
Network requirements

- An NMS and Switch A (SNMP agent) 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 traps.

Thus, the NMS is able to access Switch A and receive the traps sent by Switch A.

Network diagram

Figure 1-2 Network diagram for SNMP configuration



Network procedure

Enable SNMP agent, and set the SNMPv1 and SNMPv2c community names.

```

<Sysname> system-view
[Sysname] snmp-agent
[Sysname] snmp-agent sys-info version all
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
  
```

Set the access right of the NMS to the MIB of the SNMP agent.

```
[Sysname] snmp-agent mib-view include internet 1.3.6.1
```

For SNMPv3, set:

- SNMPv3 group and user
- security to the level of needing authentication and encryption
- authentication protocol to **HMAC-MD5**
- authentication password to **passmd5**
- encryption protocol to **AES**
- encryption password to **cfb128cfb128**

```
[Sysname] snmp-agent group v3 managev3group privacy write-view internet
```



```
[Sysname] snmp-agent usm-user v3 managev3user managev3group authentication-mode md5 passmd5  
privacy-mode aes128 cfb128cfb128
```

Set the VLAN-interface 2 as the interface used by NMS. Add port Ethernet 1/0/2, which is to be used for network management, to VLAN 2. Set the IP address of VLAN-interface 2 as 10.10.10.2.

```
[Sysname] vlan 2  
[Sysname-vlan2] port Ethernet 1/0/2  
[Sysname-vlan2] quit  
[Sysname] interface Vlan-interface 2  
[Sysname-Vlan-interface2] ip address 10.10.10.2 255.255.255.0  
[Sysname-Vlan-interface2] quit
```

Enable the SNMP agent to send traps to the NMS whose IP address is 10.10.10.1. The SNMP community name to be used is **public**.

```
[Sysname] snmp-agent trap enable standard authentication  
[Sysname] snmp-agent trap enable standard coldstart  
[Sysname] snmp-agent trap enable standard linkup  
[Sysname] snmp-agent trap enable standard linkdown  
[Sysname] snmp-agent target-host trap address udp-domain 10.10.10.1 udp-port 5000 params  
securityname public
```

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.

2 RMON Configuration

When configuring RMON, go to these sections for information you are interested in:

- [Introduction to RMON](#)
- [RMON Configuration](#)
- [Displaying RMON](#)
- [RMON Configuration Example](#)

Introduction to RMON

Remote Monitoring (RMON) is a kind of MIB defined by Internet Engineering Task Force (IETF). It is an 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 SNMP architecture. It is compatible with the current SNMP implementations.
- 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 SNMP agents can be reduced, thus facilitating the management of large-scale internetworks.

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 H3C 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.

Commonly Used RMON Groups

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 traps to the NMS
- Logging the event and sending traps to the NMS
- No processing

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 then triggers the network device to act in the way defined in the events. 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

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.

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.

Statistics group

Statistics group contains the statistics of each monitored port on a switch. 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.

RMON Configuration

Before performing RMON configuration, make sure the SNMP agents are correctly configured. For the information about SNMP agent configuration, refer to section [Configuring Basic SNMP Functions](#).

Follow these steps to configure RMON:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Add an event entry	rmon event <i>event-entry</i> [description <i>string</i>] { log trap <i>trap-community</i> log-trap <i>log-trapcommunity</i> none } [owner <i>text</i>]	Optional
Add an alarm entry	rmon alarm <i>entry-number alarm-variable</i> <i>sampling-time</i> { delta absolute } rising_threshold <i>threshold-value1</i> <i>event-entry1</i> falling_threshold <i>threshold-value2</i> <i>event-entry2</i> [owner <i>text</i>]	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 <i>entry-number</i> <i>prialarm-formula</i> <i>prialarm-des</i> <i>sampling-timer</i> { delta absolute changeratio } rising_threshold <i>threshold-value1</i> <i>event-entry1</i> falling_threshold <i>threshold-value2</i> <i>event-entry2</i> entrytype { forever cycle <i>cycle-period</i> } [owner <i>text</i>]	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 <i>interface-type interface-number</i>	—
Add a history entry	rmon history <i>entry-number</i> buckets <i>number</i> interval <i>sampling-interval</i> [owner <i>text</i>]	Optional
Add a statistics entry	rmon statistics <i>entry-number</i> [owner <i>text</i>]	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.

Displaying RMON

To do...	Use the command...	Remarks
Display RMON statistics	display rmon statistics [<i>interface-type</i> <i>interface-number</i> unit <i>unit-number</i>]	Available in any view.
Display RMON history information	display rmon history [<i>interface-type</i> <i>interface-number</i> unit <i>unit-number</i>]	
Display RMON alarm information	display rmon alarm [<i>entry-number</i>]	
Display extended RMON alarm information	display rmon prialarm [<i>prialarm-entry-number</i>]	
Display RMON events	display rmon event [<i>event-entry</i>]	
Display RMON event logs	display rmon eventlog [<i>event-entry</i>]	

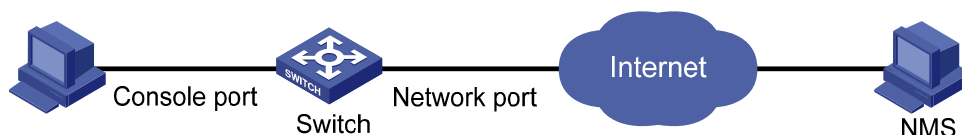
RMON Configuration Example

Network requirements

- The switch to be tested is connected to a remote NMS through the Internet. Ensure that the SNMP agents are correctly configured before performing RMON configuration.
- Create an entry in the extended alarm table to monitor the information of statistics on the Ethernet port, if the change rate of which exceeds the set threshold, the alarm events will be triggered.

Network diagram

Figure 2-1 Network diagram for RMON configuration



Configuration procedures

Add the statistics entry numbered 1 to take statistics on Ethernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] rmon statistics 1
[Sysname-Ethernet1/0/1] quit
```

Add the event entries numbered 1 and 2 to the event table, which will be triggered by the following extended alarm.

```
[Sysname] rmon event 1 log
```

```
[Sysname] rmon event 2 trap 10.21.30.55
```

Add an entry numbered 2 to the extended alarm table to allow the system to calculate the alarm variables with the (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1) formula to get the numbers of all the oversize and undersize packets received by Ethernet 1/0/1 that are in correct data format and sample it in every 10 seconds. When the change ratio between samples reaches the rising threshold of 50, event 1 is triggered; when the change ratio drops under the falling threshold, event 2 is triggered.

```
[Sysname] rmon prialarm 2 (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1) test 10
changeratio rising_threshold 50 1 falling_threshold 5 2 entrytype forever owner user1
```

Display the RMON extended alarm entry numbered 2.

```
[Sysname] display rmon prialarm 2
```

Prialarm table 2 owned by user1 is VALID.

Samples type : changeratio

Variable formula : (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1)

Description : test

Sampling interval : 10(sec)

Rising threshold : 100(linked with event 1)

Falling threshold : 10(linked with event 2)

When startup enables : risingOrFallingAlarm

This entry will exist : forever.

Latest value : 0

Table of Contents

1 NTP Configuration	1-1
Introduction to NTP	1-1
Applications of NTP	1-1
Implementation Principle of NTP	1-2
NTP Implementation Modes	1-3
NTP Configuration Task List	1-6
Configuring NTP Implementation Modes	1-6
Configuring NTP Server/Client Mode	1-7
Configuring the NTP Symmetric Peer Mode	1-8
Configuring NTP Broadcast Mode	1-8
Configuring NTP Multicast Mode	1-9
Configuring Access Control Right	1-10
Configuration Prerequisites	1-10
Configuration Procedure	1-11
Configuring NTP Authentication	1-11
Configuration Prerequisites	1-11
Configuration Procedure	1-12
Configuring Optional NTP Parameters	1-13
Configuring an Interface on the Local Switch to Send NTP messages	1-14
Configuring the Number of Dynamic Sessions Allowed on the Local Switch	1-14
Disabling an Interface from Receiving NTP messages	1-14
Displaying NTP Configuration	1-15
Configuration Examples	1-15
Configuring NTP Server/Client Mode	1-15
Configuring NTP Symmetric Peer Mode	1-16
Configuring NTP Broadcast Mode	1-18
Configuring NTP Multicast Mode	1-19
Configuring NTP Server/Client Mode with Authentication	1-21

1 NTP Configuration

When configuring NTP, go to these sections for information you are interested in:

- [Introduction to NTP](#)
- [NTP Configuration Task List](#)
- [Configuring NTP Implementation Modes](#)
- [Configuring Access Control Right](#)
- [Configuring NTP Authentication](#)
- [Configuring Optional NTP Parameters](#)
- [Displaying NTP Configuration](#)
- [Configuration Examples](#)

Introduction to NTP

Network Time Protocol (NTP) is a time synchronization protocol defined in RFC 1305. It is used for time synchronization between a set of distributed time servers and clients. Carried over UDP, 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 (see section [Applications of NTP](#)).

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 messages.

Applications of NTP

As setting the system time manually in a network with many devices leads to a lot of workload and cannot ensure 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 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.

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 (see section [Configuring Access Control Right](#)) and MD5 encrypted authentication (see section [Configuring NTP 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 be set as a reference clock. It can serve as a reference clock source to synchronize the clock of other devices only after it is synchronized.
-

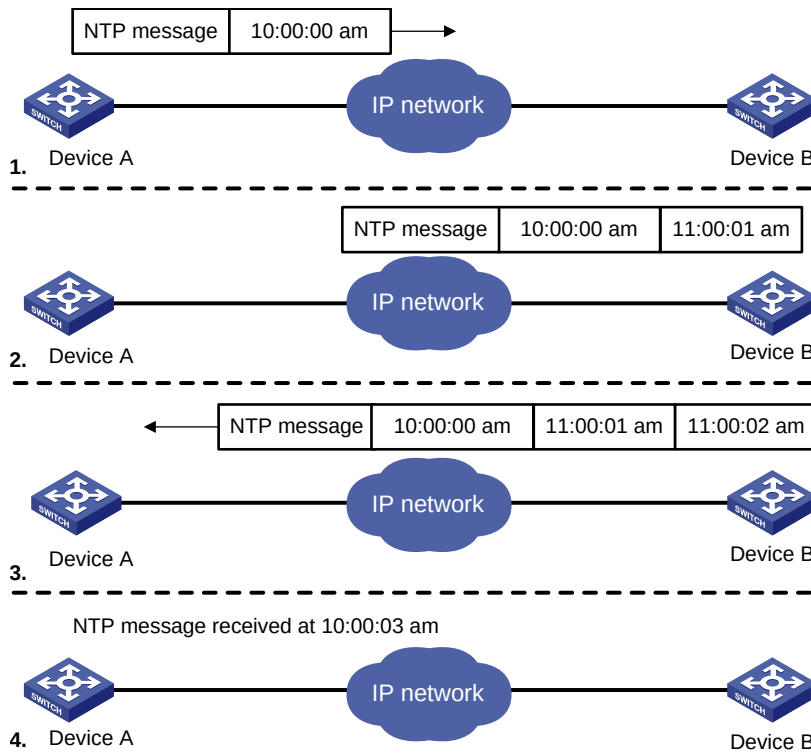
Implementation Principle of NTP

[Figure 1-1](#) shows the implementation principle of NTP.

Ethernet switch A (Device A) is connected to Ethernet switch B (Device B) through Ethernet ports. Both having their own system clocks, 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 Device A and Device B are synchronized, the clock of Device A is set to 10:00:00 am, and the clock of Device B is set to 11:00:00 am.
- Device B serves as the NTP server, that is, the clock of Device A will be synchronized to that of Device B.
- It takes one second to transfer an NTP message from Device A to Device B or from Device B to Device A.

Figure 1-1 Implementation principle of NTP



The procedure of synchronizing the system clock is as follows:

- Device A sends an NTP message to Device B, with a timestamp 10:00:00 am (T_1) identifying when it is sent.
- When the message arrives at Device B, Device B inserts its own timestamp 11:00:01 am (T_2) into the packet.
- When the NTP message leaves Device B, Device B inserts its own timestamp 11:00:02 am (T_3) into the packet.
- When Device A receives the NTP message, the local time of Device A is 10:00:03am (T_4).

At this time, Device A has enough information to calculate the following two parameters:

- Delay for an NTP message to make a round trip between Device A and Device B:

$$\text{Delay} = (T_4 - T_1) - (T_3 - T_2).$$

- Time offset of Device A relative to Device B:

$$\text{Offset} = ((T_2 - T_1) + (T_3 - T_4))/2.$$

Device A can then set its own clock according to the above information to synchronize its clock to that of Device B.

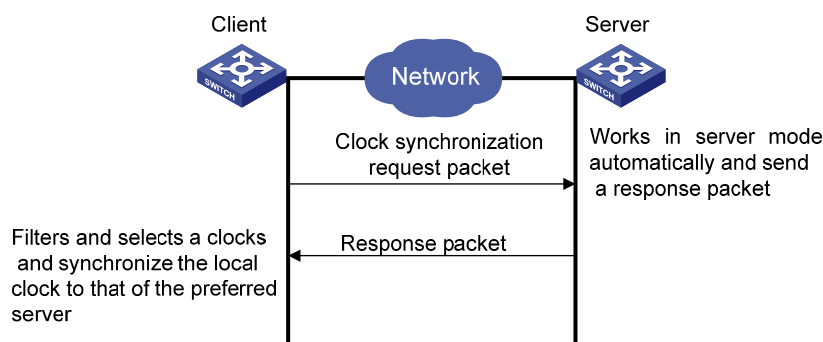
For detailed information, refer to RFC 1305.

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.

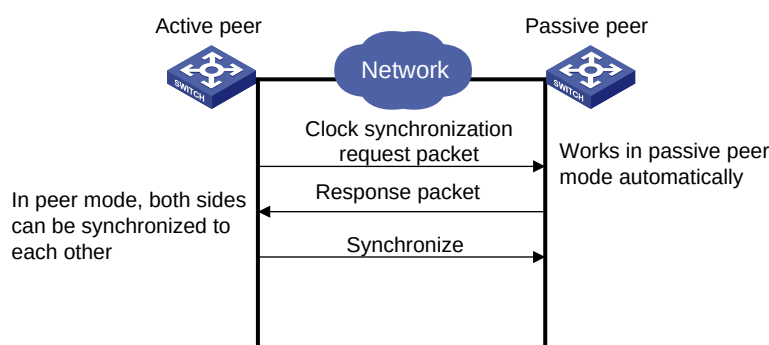
Server/client mode

Figure 1-2 Server/client mode



Symmetric peer mode

Figure 1-3 Symmetric peer mode

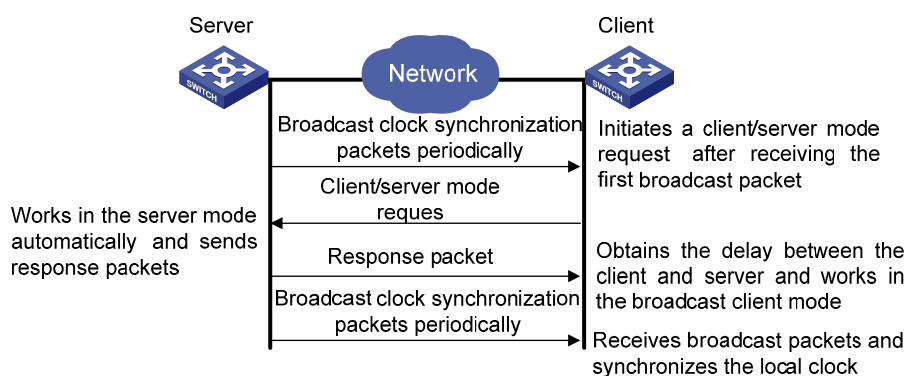


In the symmetric peer mode, the local S3600 Ethernet switch serves as the symmetric-active peer and sends clock synchronization request first, while the remote server serves as the symmetric-passive peer automatically.

If both of the peers have reference clocks, the one with a smaller stratum number is adopted.

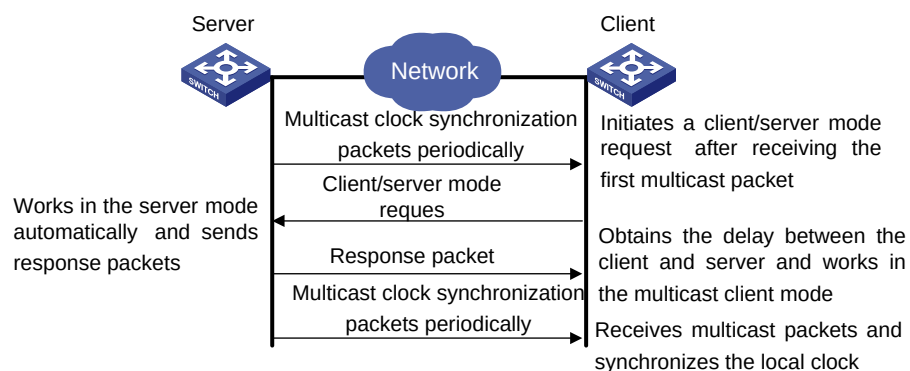
Broadcast mode

Figure 1-4 Broadcast mode



Multicast mode

Figure 1-5 Multicast mode



[Table 1-1](#) describes how the above mentioned NTP modes are implemented on H3C S3600 series Ethernet switches.

Table 1-1 NTP implementation modes on H3C S3600 series Ethernet switches

NTP implementation mode	Configuration on S3600 series switches
Server/client mode	Configure the local S3600 Ethernet switch to work in the NTP client mode. In this mode, the remote server serves as the local time server, while the local switch serves as the client.
Symmetric peer mode	Configure the local S3600 switch to work in NTP symmetric peer mode. In this mode, the remote server serves as the symmetric-passive peer of the S3600 switch, and the local switch serves as the symmetric-active peer.
Broadcast mode	- Configure the local S3600 Ethernet switch to work in NTP broadcast server mode. In this mode, the local switch broadcasts NTP messages through the VLAN interface configured on the switch. - Configure the S3600 switch to work in NTP broadcast client mode. In this mode, the local S3600 switch receives broadcast NTP messages through the VLAN interface configured on the switch.
Multicast mode	- Configure the local S3600 Ethernet switch to work in NTP multicast server mode. In this mode, the local switch sends multicast NTP messages through the VLAN interface configured on the switch. - Configure the local S3600 Ethernet switch to work in NTP multicast client mode. In this mode, the local switch receives multicast NTP messages through the VLAN interface configured on the switch.

**Caution**

- When an H3C S3600 Ethernet switch works in server mode or symmetric passive mode, you need not to perform related configurations on this switch but do that on the client or the symmetric-active peer.
 - The NTP server mode, NTP broadcast mode, or NTP multicast mode takes effect only after the local clock of the H3C S3600 Ethernet switch has been synchronized.
 - When symmetric peer mode is configured on two Ethernet switches, to synchronize the clock of the two switches, make sure at least one switch's clock has been synchronized.
-

NTP Configuration Task List

Complete the following tasks to configure NTP:

Task	Remarks
Configuring NTP Implementation Modes	Required
Configuring Access Control Right	Optional
Configuring NTP Authentication	Optional
Configuring Optional NTP Parameters	Optional
Displaying NTP Configuration	Optional

Configuring NTP Implementation Modes

An S3600 Ethernet switch can work in one of the following NTP modes:

- [Configuring NTP Server/Client Mode](#)
- [Configuring the NTP Symmetric Peer Mode](#)
- [Configuring NTP Broadcast Mode](#)
- [Configuring NTP Multicast Mode](#)



Note

To protect unused sockets against attacks by malicious users and improve security, H3C S3600 series Ethernet switches provide the following functions:

- UDP port 123 is opened only when the NTP feature is enabled.
- UDP port 123 is closed as the NTP feature is disabled.

These functions are implemented as follows:

- Execution of one of the **ntp-service unicast-server**, **ntp-service unicast-peer**, **ntp-service broadcast-client**, **ntp-service broadcast-server**, **ntp-service multicast-client**, and **ntp-service multicast-server** commands enables the NTP feature and opens UDP port 123 at the same time.
- Execution of the **undo** form of one of the above six commands disables all implementation modes of the NTP feature and closes UDP port 123 at the same time.

Configuring NTP Server/Client Mode

For switches working in the server/client mode, you only need to perform configurations on the clients, and not on the servers.

Follow these steps to configure an NTP client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure an NTP client	ntp-service unicast-server { <i>remote-ip</i> <i>server-name</i> } [authentication-keyid <i>key-id</i> priority source-interface <i>Vlan-interface</i> <i>vlan-id</i> version <i>number</i>]*	Required By default, the switch is not configured to work in the NTP client mode.



Note

- The remote server specified by *remote-ip* or *server-name* serves as the NTP server, and the local switch serves as the NTP client. The clock of the NTP client will be synchronized by but will not synchronize that of the NTP server.
- *remote-ip* cannot be a broadcast address, a multicast address or the IP address of the local clock.
- After you specify an interface for sending NTP messages through the **source-interface** keyword, the source IP address of the NTP message will be configured as the primary IP address of the specified interface.
- A switch can act as a server to synchronize the clock of other switches only after its clock has been synchronized. If the clock of a server has a stratum level lower than or equal to that of a client's clock, the client will not synchronize its clock to the server's.
- You can configure multiple servers by repeating the **ntp-service unicast-server** command. The client will choose the optimal reference source.

Configuring the NTP Symmetric Peer Mode

For switches working in the symmetric peer mode, you need to specify a symmetric-passive peer on the symmetric-active peer.

Follow these steps to configure a symmetric-active switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify a symmetric-passive peer for the switch	ntp-service unicast-peer { <i>remote-ip</i> <i>peer-name</i> } [authentication-keyid <i>key-id</i> priority source-interface Vlan-interface <i>vlan-id</i> version <i>number</i>]*	Required By default, a switch is not configured to work in the symmetric mode.



Note

- In the symmetric peer mode, you need to execute the related NTP configuration commands (refer to section [Configuring NTP Implementation Modes](#) for details) to enable NTP on a symmetric-passive peer; otherwise, the symmetric-passive peer will not process NTP messages from the symmetric-active peer.
- The remote device specified by *remote-ip* or *peer-name* serves as the peer of the local Ethernet switch, and the local switch works in the symmetric-active mode. In this case, the clock of the local switch and that of the remote device can be synchronized to each other.
- *remote-ip* must not be a broadcast address, a multicast address or the IP address of the local clock.
- After you specify an interface for sending NTP messages through the **source-interface** keyword, the source IP address of the NTP message will be configured as the IP address of the specified interface.
- Typically, the clock of at least one of the symmetric-active and symmetric-passive peers should be synchronized first; otherwise the clock synchronization will not proceed.
- You can configure multiple symmetric-passive peers for the local switch by repeating the **ntp-service unicast-peer** command. The clock of the peer with the smallest stratum will be chosen to synchronize with the local clock of the switch.

Configuring NTP Broadcast Mode

For switches working in the broadcast mode, you need to configure both the server and clients. The broadcast server periodically sends NTP broadcast messages to the broadcast address 255.255.255.255. The switches working in the NTP broadcast client mode will respond to the NTP messages, so as to start the clock synchronization.

An H3C S3600 series Ethernet switch can work as a broadcast server or a broadcast client.



Note

A broadcast server can synchronize broadcast clients only after its clock has been synchronized.

Configuring a switch to work in the NTP broadcast server mode

Follow these steps to configure a switch to work in the NTP broadcast server mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	—
Configure the switch to work in the NTP broadcast server mode	ntp-service broadcast-server [authentication-keyid <i>key-id</i> version <i>number</i>]*	Required Not configured by default.

Configuring a switch to work in the NTP broadcast client mode

Follow these steps to configure a switch to work in the NTP broadcast client mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	—
Configure the switch to work in the NTP broadcast client mode	ntp-service broadcast-client	Required Not configured by default.

Configuring NTP Multicast Mode

For switches working in the multicast mode, you need to configure both the server and clients. The multicast server periodically sends NTP multicast messages to multicast clients. The switches working in the NTP multicast client mode will respond to the NTP messages, so as to start the clock synchronization.

An H3C S3600 series Ethernet switch can work as a multicast server or a multicast client.



Note

- A multicast server can synchronize multicast clients only after its clock has been synchronized.
- An S3600 series switch working in the multicast server mode supports up to 1,024 multicast clients.

Configuring a switch to work in the multicast server mode

Follow these steps to configure a switch to work in the NTP multicast server mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	—
Configure the switch to work in the NTP multicast server mode	ntp-service multicast-server [<i>ip-address</i>] [authentication-keyid <i>keyid</i> ttl <i>tvl-number</i> version <i>number</i>]*	Required Not configured by default.

Configuring a switch to work in the multicast client mode

Follow these steps to configure a switch to work in the NTP multicast client mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	—
Configure the switch to work in the NTP multicast client mode	ntp-service multicast-client [<i>ip-address</i>]	Required Not configured by default.

Configuring Access Control Right

With the following command, you can configure the NTP service access-control right to the local switch for a peer device. There are four access-control rights, as follows:

- **query**: Control query right. This level of right permits the peer device to perform control query to the NTP service on the local device but does not permit the peer device to synchronize its clock to the local device. The so-called “control query” refers to query of state of the NTP service, including alarm information, authentication status, clock source information, and so on.
- **synchronization**: Synchronization right. This level of right permits the peer device to synchronize its clock to the local switch but does not permit the peer device to perform control query.
- **server**: Server right. This level of right permits the peer device to perform synchronization and control query to the local switch but does not permit the local switch to synchronize its clock to the peer device.
- **peer**: Peer access. This level of right permits the peer device to perform synchronization and control query to the local switch and also permits the local switch to synchronize its clock to the peer device.

NTP service access-control rights from the highest to the lowest are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it will perform an access-control right match in this order and use the first matched right.

Configuration Prerequisites

Prior to configuring the NTP service access-control right to the local switch for peer devices, you need to create and configure an ACL associated with the access-control right. For the configuration of ACL, refer to *ACL Configuration* in *Security Volume*.

Configuration Procedure

Follow these steps to configure the NTP service access-control right to the local device for peer devices:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the NTP service access-control right to the local switch for peer devices	ntp-service access { peer server synchronization query } acl-number	Optional peer by default



Note

The access-control right mechanism provides only a minimum degree of security protection for the local switch. A more secure method is identity authentication.

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 clock of the client is synchronized only to that of the server that passes the authentication. This improves network security. [Table 1-2](#) shows the roles of devices in the NTP authentication function.

Table 1-2 Description on the roles of devices in NTP authentication function

Role of device	Working mode
Client	Client in the server/client mode
	Client in the broadcast mode
	Client in the multicast mode
	Symmetric-active peer in the symmetric peer mode
Server	Server in the server/client mode
	Server in the broadcast mode
	Server in the multicast mode
	Symmetric-passive peer in the symmetric peer mode

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 clock of 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 properly performed).
- For the NTP authentication function to take effect, a trusted key needs to be configured on both the client and server after the NTP authentication is enabled on them.
- The local clock of the client is only synchronized to the server that provides a trusted key.
- In addition, for the server/client mode and the symmetric peer mode, you need to associate a specific key on the client (the symmetric-active peer in the symmetric peer mode) with the corresponding NTP server (the symmetric-passive peer in the symmetric peer mode); for the NTP broadcast/multicast mode, you need to associate a specific key on the broadcast/multicast server with the corresponding NTP broadcast/multicast client. Otherwise, NTP authentication cannot be enabled normally.
- Configurations on the server and the client must be consistent.

Configuration Procedure

Configuring NTP authentication on the client

Follow these steps to configure NTP authentication on the client:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enable the NTP authentication function		ntp-service authentication enable	Required Disabled by default.
Configure the NTP authentication key		ntp-service authentication-keyid <i>key-id</i> authentication-model md5 <i>value</i>	Required By default, no NTP authentication key is configured.
Configure the specified key as a trusted key		ntp-service reliable authentication-keyid <i>key-id</i>	Required By default, no trusted key is configured.
Associate the specified key with the corresponding NTP server	Configure on the client in the server/client mode	ntp-service unicast-server { <i>remote-ip</i> <i>server-name</i> } authentication-keyid <i>key-id</i>	Required For the client in the NTP broadcast/multicast mode, you just need to associate the specified key with the client on the corresponding server.
	Configure on the symmetric-active peer in the symmetric peer mode	ntp-service unicast-peer { <i>remote-ip</i> <i>peer-name</i> } authentication-keyid <i>key-id</i>	



Note

NTP authentication requires that the authentication keys configured for the server and the client be the same. Besides, the authentication keys must be trusted keys. Otherwise, the clock of the client cannot be synchronized with that of the server.

Configuring NTP authentication on the server

Follow these steps to configure NTP authentication on the server:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enable NTP authentication		ntp-service authentication enable	Required Disabled by default.
Configure an NTP authentication key		ntp-service authentication-keyid <i>key-id</i> authentication-mode md5 <i>value</i>	Required By default, no NTP authentication key is configured.
Configure the specified key as a trusted key		ntp-service reliable authentication-keyid <i>key-id</i>	Required By default, no trusted authentication key is configured.
Enter VLAN interface view		interface Vlan-interface <i>vlan-id</i>	—
Associate the specified key with the corresponding broadcast/multicast client	Configure on the NTP broadcast server	ntp-service broadcast-server authentication-keyid <i>key-id</i>	• In NTP broadcast server mode and NTP multicast server mode, you need to associate the specified key with the corresponding broadcast/multicast client • You can associate an NTP broadcast/multicast client with an authentication key while configuring NTP mode. You can also use this command to associate them after configuring the NTP mode.
	Configure on the NTP multicast server	ntp-service multicast-server authentication-keyid <i>key-id</i>	



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.

Configuring Optional NTP Parameters

Complete the following tasks to configure optional NTP parameters:

Task	Remarks
Configuring an Interface on the Local Switch to Send NTP messages	Optional
Configuring the Number of Dynamic Sessions Allowed on the Local Switch	Optional
Disabling an Interface from Receiving NTP messages	Optional

Configuring an Interface on the Local Switch to Send NTP messages

Follow these steps to configure an interface on the local switch to send NTP messages:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure an interface on the local switch to send NTP messages	ntp-service source-interface Vlan-interface <i>vlan-id</i>	Required



Caution

If you have specified an interface in the **ntp-service unicast-server** or **ntp-service unicast-peer** command, this interface will be used for sending NTP messages.

Configuring the Number of Dynamic Sessions Allowed on the Local Switch

A single device can have a maximum of 128 associations at the same time, including static associations and dynamic associations. A static association refers to an association that a user has manually created by using an NTP command, while a dynamic association is a temporary association created by the system during operation. A dynamic association will be removed if the system fails to receive messages from it over a specific long time.

In the server/client mode, for example, when you carry out a command to synchronize the time to a server, the system will create a static association, and the server will just respond passively upon the receipt of a message, rather than creating an association (static or dynamic). In the symmetric mode, static associations will be created at the symmetric-active peer side, and dynamic associations will be created at the symmetric-passive peer side; In the broadcast or multicast mode, static associations will be created at the server side, and dynamic associations will be created at the client side.

Follow these steps to configure the number of dynamic sessions allowed on the local switch:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the maximum number of dynamic sessions that can be established on the local switch	ntp-service max-dynamic-sessions <i>number</i>	Required By default, up to 100 dynamic sessions can be established locally.

Disabling an Interface from Receiving NTP messages

Follow these steps to disable an interface from receiving NTP messages:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	—

To do...	Use the command...	Remarks
Disable an interface from receiving NTP messages	ntp-service in-interface disable	Required By default, a VLAN interface receives NTP messages.

Displaying NTP Configuration

To do...	Use the command...	Remarks
Display the status of NTP services	display ntp-service status	Available 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	

Configuration Examples

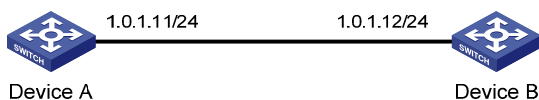
Configuring NTP Server/Client Mode

Network requirements

- The local clock of Device A (a switch) is to be used as a master clock, with the stratum level of 2.
- Device A is used as the NTP server of Device B (an S3600 Ethernet switch)
- Configure Device B to work in the client mode, and then Device A will automatically work in the server mode.

Network diagram

Figure 1-6 Network diagram for the NTP server/client mode configuration



Configuration procedure

Perform the following configurations on Device B.

View the NTP status of Device B before synchronization.

```

<DeviceB> display ntp-service status
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
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 Device A as the NTP server of Device B.

<DeviceB> system-view
[DeviceB] ntp-service unicast-server 1.0.1.11

# (After the above configurations, Device B is synchronized to Device A.) View the NTP status of Device B.

[DeviceB] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 0.66 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Apr 2 2007 (BF422AE4.05AEA86C)

```

The above output information indicates that Device B is synchronized to Device A, and the stratum level of its clock is 3, one level lower than that of Device A.

View the information about NTP sessions of Device B. (You can see that Device B establishes a connection with Device A.)

```

[DeviceB] display ntp-service sessions

```

	source	reference	stra	reach	poll	now	offset	delay	disper

[12345]	1.0.1.11	127.127.1.0	2	1	64	1	350.1	15.1	0.0

```

note:  1  source(master),2  source(peer),3  selected,4  candidate,5  configured  Total
associations :  1

```

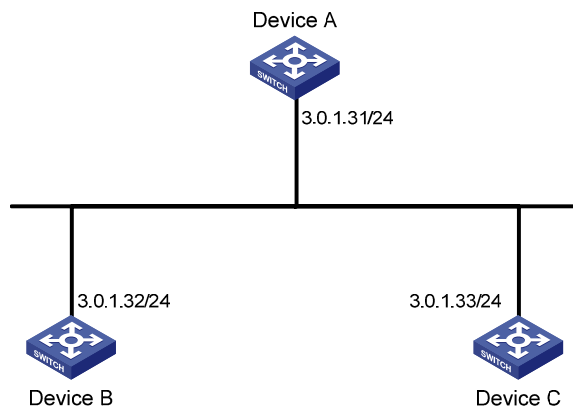
Configuring NTP Symmetric Peer Mode

Network requirements

- The local clock of Device A is set as the NTP master clock, with the clock stratum level of 2.
- Device C (an S3600 Ethernet switch) uses Device A as the NTP server, and Device A works in server mode automatically.
- The local clock of Device B is set as the NTP master clock, with the clock stratum level of 1. Set Device C as the peer of Device B.

Network diagram

Figure 1-7 Network diagram for NTP peer mode configuration



Configuration procedure

1) Configure Device C.

Set Device A as the NTP server.

```
<DeviceC> system-view
[DeviceC] ntp-service unicast-server 3.0.1.31
```

2) Configure Device B (after the Device C is synchronized to Device A).

Enter system view.

```
<DeviceB> system-view
# Set Device C as the peer of Device B.
[DeviceB] ntp-service unicast-peer 3.0.1.33
```

Device C and Device B are symmetric peers after the above configuration. Device B works in symmetric active mode, while Device C works in symmetric passive mode. Because the stratum level of the local clock of Device B is 1, and that of Device C is 3, the clock of Device C is synchronized to that of Device B.

View the status of Device C after the clock synchronization.

```
[DeviceC] display ntp-service status
Clock status: synchronized
Clock stratum: 2
Reference clock ID: 3.0.1.32
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 0.66 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Apr 2 2007 (BF422AE4.05AEA86C)
```

The output information indicates that the clock of Device C is synchronized to that of Device B and the stratum level of its local clock is 2, one level lower than Device B.

View the information about the NTP sessions of Device C (you can see that a connection is established between Device C and Device B).

```
[DeviceC] display ntp-service sessions
```

source	reference	strata	reach	poll	now	offset	delay	disper

[1234]3.0.1.32	LOCL	1	95	64	42	-14.3	12.9	2.7
[25]3.0.1.31	127.127.1.0	2	1	64	1	4408.6	38.7	0.0

note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 2

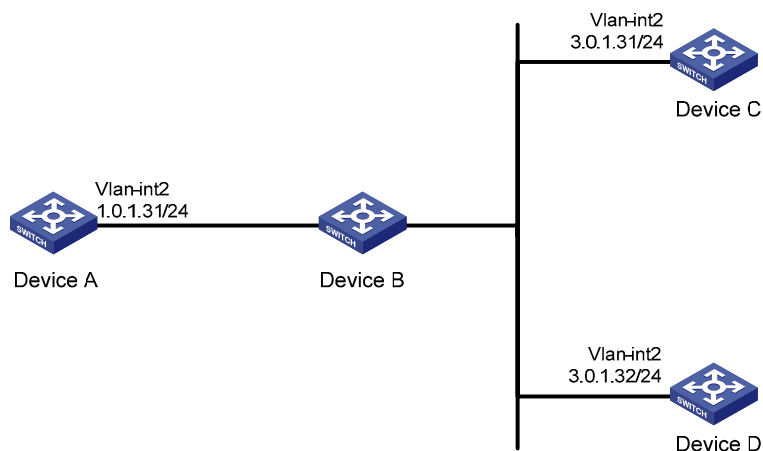
Configuring NTP Broadcast Mode

Network requirements

- The local clock of Device C is set as the NTP master clock, with a stratum level of 2. Configure Device C to work in the NTP broadcast server mode and send NTP broadcast messages through VLAN-interface 2.
- Device A and Device D are two S3600 Ethernet switches. Configure Device A and Device D to work in the NTP broadcast client mode and listen to broadcast messages through their own VLAN-interface 2.

Network diagram

Figure 1-8 Network diagram for the NTP broadcast mode configuration



Configuration procedure

1) Configure Device C.

Enter system view.

```
<DeviceC> system-view
```

Set Device C as the broadcast server, which sends broadcast messages through VLAN-interface 2.

```
[DeviceC] interface Vlan-interface 2
```

```
[DeviceC-Vlan-interface2] ntp-service broadcast-server
```

2) Configure Device A. (Perform the same configuration on Device D.)

Enter system view.

```
<DeviceA> system-view
```

Set Device A as a broadcast client.

```
[DeviceA] interface Vlan-interface 2
[DeviceA-Vlan-interface2] ntp-service broadcast-client
```

After the above configurations, Device A and Device D will listen to broadcast messages through their own VLAN-interface 2, and Device C will send broadcast messages through VLAN-interface 2. Because Device A and Device C do not share the same network segment, Device A cannot receive broadcast messages from Device C, while Device D is synchronized to Device C after receiving broadcast messages from Device C.

View the NTP status of Device D after the clock synchronization.

```
[DeviceD] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 198.7425 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Apr 2 2007 (BF422AE4.05AEA86C)
```

The output information indicates that Device D is synchronized to Device C, with the clock stratum level of 3, one level lower than that of Device C.

View the information about the NTP sessions of Device D and you can see that a connection is established between Device D and Device C.

```
[DeviceD] display ntp-service sessions
      source           reference      stra reach poll  now offset   delay disper
*****
[1234]3.0.1.31      127.127.1.0      2    1    64   377    26.1   199.53   9.7
note:  1  source(master),2  source(peer),3  selected,4  candidate,5  configured  Total
associations :  1
```

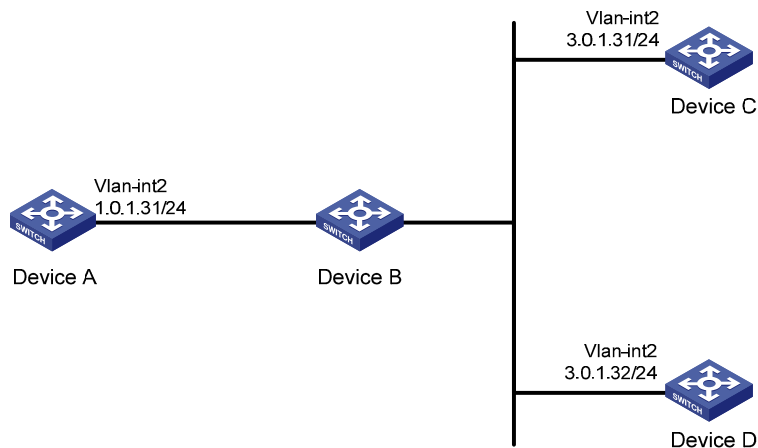
Configuring NTP Multicast Mode

Network requirements

- The local clock of Device C is set as the NTP master clock, with a clock stratum level of 2. Configure Device C to work in the NTP multicast server mode and advertise multicast NTP messages through VLAN-interface 2.
- Device A and Device D are two S3600 Ethernet switches. Configure Device A and Device D to work in the NTP multicast client mode and listen to multicast messages through their own VLAN-interface 2.

Network diagram

Figure 1-9 Network diagram for NTP multicast mode configuration



Configuration procedure

1) Configure Device C.

Enter system view.

```
<DeviceC> system-view
```

Set Device C as a multicast server to send multicast messages through VLAN-interface 2.

```
[DeviceC] interface Vlan-interface 2
```

```
[DeviceC-Vlan-interface2] ntp-service multicast-server
```

2) Configure Device A (perform the same configuration on Device D).

Enter system view.

```
<DeviceA> system-view
```

Set Device A as a multicast client to listen to multicast messages through VLAN-interface 2.

```
[DeviceA] interface Vlan-interface 2
```

```
[DeviceA-Vlan-interface2] ntp-service multicast-client
```

After the above configurations, Device A and Device D respectively listen to multicast messages through their own VLAN-interface 2, and Device C advertises multicast messages through VLAN-interface 2. Because Device A and Device C do not share the same network segment, Device A cannot receive multicast messages from Device C, while Device D is synchronized to Device C after receiving multicast messages from Device C.

View the NTP status of Device D after the clock synchronization.

```
[DeviceD] display ntp-service status
```

```
Clock status: synchronized
```

```
Clock stratum: 3
```

```
Reference clock ID: 3.0.1.31
```

```
Nominal frequency: 100.0000 Hz
```

```
Actual frequency: 100.0000 Hz
```

```
Clock precision: 2^18
```

```
Clock offset: 198.7425 ms
```

```
Root delay: 27.47 ms
```

```

Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Apr 2 2007 (BF422AE4.05AEA86C)

```

The output information indicates that Device D is synchronized to Device C, with a clock stratum level of 3, one stratum level lower than that Device C.

View the information about the NTP sessions of Device D (you can see that a connection is established between Device D and Device C).

```

[DeviceD] display ntp-service sessions
      source          reference          stra reach poll  now offset  delay disper
*****
[1234]3.0.1.31      127.127.1.0          2    1    64    377  26.1   199.53  9.7
note:  1  source(master),2  source(peer),3  selected,4  candidate,5  configured  Total
associations :  1

```

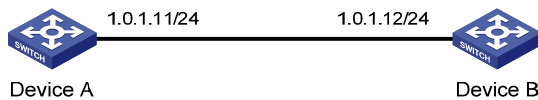
Configuring NTP Server/Client Mode with Authentication

Network requirements

- The local clock of Device A is set as the NTP master clock, with a clock stratum level of 2.
- Device B is an S3600 Ethernet switch and uses Device A as the NTP server. Device B is set to work in client mode, while Device A works in server mode automatically.
- The NTP authentication function is enabled on Device A and Device B.

Network diagram

Figure 1-10 Network diagram for NTP server/client mode with authentication configuration



Configuration procedure

1) Configure Device B.

Enter system view.

```
<DeviceB> system-view
```

Enable the NTP authentication function.

```
[DeviceB] ntp-service authentication enable
```

Configure an MD5 authentication key, with the key ID being 42 and the key being aNiceKey.

```
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

Specify the key 42 as a trusted key.

```
[DeviceB] ntp-service reliable authentication-keyid 42
```

Associate the trusted key with the NTP server (Device A).

```
[DeviceB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

After the above configurations, Device B is ready to synchronize with Device A. Because the NTP authentication function is not enabled on Device A, the clock of Device B will fail to be synchronized to that of Device A.

2) To synchronize Device B, you need to perform the following configurations on Device A.

Enable the NTP authentication function.

```
<DeviceA> system-view
```

```
[DeviceA] ntp-service authentication enable
```

Configure an MD5 authentication key, with the key ID being 42 and the key being aNiceKey.

```
[DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

Specify the key 42 as a trusted key.

```
[DeviceA] ntp-service reliable authentication-keyid 42
```

(After the above configurations, the clock of Device B can be synchronized to that of Device A.) View the status of Device B after synchronization.

```
[DeviceB] display ntp-service status
```

```
  Clock status: synchronized
```

```
  Clock stratum: 3
```

```
  Reference clock ID: 1.0.1.11
```

```
  Nominal frequency: 100.0000 Hz
```

```
  Actual frequency: 100.1000 Hz
```

```
  Clock precision: 2^18
```

```
  Clock offset: 0.66 ms
```

```
  Root delay: 27.47 ms
```

```
  Root dispersion: 208.39 ms
```

```
  Peer dispersion: 9.63 ms
```

```
  Reference time: 17:03:32.022 UTC Apr 2 2007 (BF422AE4.05AEA86C)
```

The output information indicates that the clock of Device B is synchronized to that of Device A, with a clock stratum level of 3, one stratum level lower than that Device A.

View the information about NTP sessions of Device B (you can see that a connection is established between Device B and Device A).

```
<DeviceB> 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	8	2.8	17.7	1.2

note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured

Total associations : 1

Table of Contents

1 SSH Configuration	1-1
SSH Overview	1-1
Introduction to SSH	1-1
Algorithm and Key	1-1
SSH Operating Process	1-2
SSH Server and Client	1-4
Configuring the SSH Server	1-5
Configuring the User Interfaces for SSH Clients	1-6
Configuring the SSH Management Functions	1-7
Configuring the SSH Server to Be Compatible with SSH1 Clients	1-8
Configuring Key Pairs	1-8
Creating an SSH User and Specifying an Authentication Type	1-9
Specifying a Service Type for an SSH User on the Server	1-11
Configuring the Public Key of a Client on the Server	1-12
Assigning a Public Key to an SSH User	1-12
Exporting the Host Public Key to a File	1-13
Configuring the SSH Client	1-14
SSH Client Configuration Task List	1-14
Configuring an SSH Client that Runs SSH Client Software	1-14
Configuring an SSH Client Assumed by an SSH2-Capable Switch	1-21
Displaying and Maintaining SSH Configuration	1-24
Comparison of SSH Commands with the Same Functions	1-24
SSH Configuration Examples	1-25
When Switch Acts as Server for Local Password Authentication	1-25
When Switch Acts as Server for Password and RADIUS Authentication	1-28
When Switch Acts as Server for Password and HWTACACS Authentication	1-32
When Switch Acts as Server for Publickey Authentication	1-34
When Switch Acts as Client for Password Authentication	1-40
When Switch Acts as Client for Publickey Authentication	1-41
When Switch Acts as Client and First-Time Authentication is not Supported	1-43

1 SSH Configuration

When configuring SSH, go to these sections for information you are interested:

- [SSH Overview](#)
- [SSH Server and Client](#)
- [Displaying and Maintaining SSH Configuration](#)
- [Comparison of SSH Commands with the Same Functions](#)
- [SSH Configuration Examples](#)

SSH Overview

Introduction to SSH

Secure Shell (SSH) is a protocol that provides secure remote login and other security services in insecure network environments, allowing for secure access to the Command Line Interface (CLI) of a switch for configuration and management. In an SSH connection, data are encrypted before being sent out and decrypted after they reach the destination. This prevents attacks such as plain text password interception. SSH also provides powerful user authentication functions that prevent attacks such as DNS and IP spoofing. Besides, SSH can also provide data compression to increase transmission speed, take the place of Telnet and provide a secure “channel” for transfers using File Transfer Protocol (FTP).

SSH adopts the client-server model. The switch can be configured as an SSH client, an SSH server, or both at the same time. As an SSH server, the switch provides secure connections to multiple clients. As an SSH client, the switch allows the remote server to establish a secure SSH connection for remote login.

Algorithm and Key

Algorithm is a set of transformation rules for encryption and decryption. Information without being encrypted is known as plain text, while information that is encrypted is known as cipher text. Encryption and decryption are performed using a string of characters called a key, which controls the transformation between plain text and cipher text, for example, changing the plain text into cipher text or cipher text into plain text.

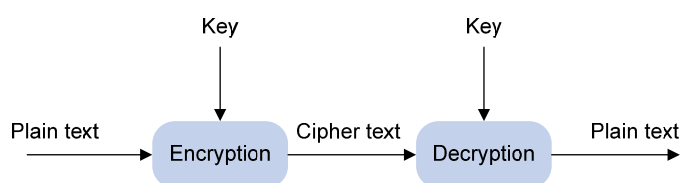


Figure 1-1 Encryption and decryption

There are two types of key algorithms:

- Symmetric key algorithm

The same key is used for both encryption and decryption. Supported symmetric key algorithms include DES, 3DES, and AES, which can effectively prevent data eavesdropping.

- Asymmetric key algorithm

Asymmetric key algorithm is also called public key algorithm. Both ends have their own key pair, consisting of a private key and a public key. The private key is kept secret while the public key may be distributed widely. The private key cannot be practically derived from the public key. The information encrypted with the public key/private key can be decrypted only with the corresponding private key/public key.

Asymmetric key algorithm encrypts data using the public key and decrypts the data using the private key, thus ensuring data security.

You can also use the asymmetric key algorithm for data signature. For example, user 1 adds his signature to the data using the private key, and then sends the data to user 2. User 2 verifies the signature using the public key of user 1. If the signature is correct, this means that the data originates from user 1.

Both Revest-Shamir-Adleman Algorithm (RSA) and Digital Signature Algorithm (DSA) are asymmetric key algorithms. RSA is used for data encryption and signature, whereas DSA is used for adding signature. Currently the switch supports RSA and DSA.



Note

Symmetric key algorithms are used for encryption and decryption of the data transferred on the SSH channel while asymmetric key algorithms are used for digital signature and identity authentication.

SSH Operating Process

The session establishment between an SSH client and the SSH server involves the following five stages:

Table 1-1 Stages in establishing a session between the SSH client and server

Stages	Description
Version negotiation	SSH1 and SSH2 are supported. The two parties negotiate a version to use.
Key and algorithm negotiation	SSH supports multiple algorithms. The two parties negotiate an algorithm for communication.
Authentication	The SSH server authenticates the client in response to the client's authentication request.
Session request	This client sends a session request to the server.
Data exchange	The client and the server start to communicate with each other.



Caution

- Currently, the switch that serves as an SSH server supports two SSH versions: SSH2 and SSH1, and the switch that serves as an SSH client supports only SSH2.
 - Unless otherwise noted, SSH refers to SSH2 throughout this document.
-

I. Version negotiation

- The server opens port 22 to listen to connection requests from clients.
 - The client sends a TCP connection request to the server. After the TCP connection is established, the server sends the first packet to the client, which includes a version identification string in the format of "SSH-<primary protocol version number>.<secondary protocol version number>.<software version number>". The primary and secondary protocol version numbers constitute the protocol version number, while the software version number is used for debugging.
 - The client receives and resolves the packet. If the protocol version of the server is lower but supportable, the client uses the protocol version of the server; otherwise, the client uses its own protocol version.
 - The client sends to the server a packet that contains the number of the protocol version it decides to use. The server compares the version carried in the packet with that of its own to determine whether it can cooperate with the client.
 - If the negotiation is successful, the server and the client go on to the key and algorithm negotiation. If not, the server breaks the TCP connection.
-



Note

All the packets above are transferred in plain text.

Key negotiation

- The server and the client send algorithm negotiation packets to each other, which contain public key algorithm lists supported by the server and the client, encrypted algorithm list, message authentication code (MAC) algorithm list, and compressed algorithm list.
- The server and the client calculate the final algorithm according to the algorithm lists supported.
- The server and the client generate the session key and session ID based on the Diffie-Hellman (DH) exchange algorithm and the host key pair.
- Then, the server and the client get the same session key and use it for data encryption and decryption to secure data communication.

Authentication negotiation

The negotiation steps are as follows:

- The client sends an authentication request to the server. The authentication request contains username, authentication type, and authentication-related information. For example, if the authentication type is **password**, the content is the password.

- The server starts to authenticate the user. If authentication fails, the server sends an authentication failure message to the client, which contains the list of methods used for a new authentication process.
- The client selects an authentication type from the method list to perform authentication again.
- The above process repeats until the authentication succeeds, or the connection is torn down when the authentication times reach the upper limit.

SSH provides two authentication methods: password authentication and publickey authentication.

- In password authentication, the client encrypts the username and password, encapsulates them into a password authentication request, and sends the request to the server. Upon receiving the request, the server decrypts the username and password, compares them with those it maintains, and then informs the client of the authentication result.
- The publickey authentication method authenticates clients using digital signatures. Currently, the device supports two publickey algorithms to implement digital signatures: RSA and DSA. The client sends to the server a publickey authentication request containing its user name, public key and algorithm. The server verifies the public key. If the public key is invalid, the authentication fails; otherwise, the server generates a digital signature to authenticate the client, and then sends back a message to inform the success or failure of the authentication.

Session request

After passing authentication, the client sends a session request to the server, while the server listens to and processes the request from the client. If the client passes authentication, the server sends back to the client an SSH_MSG_SUCCESS packet and goes on to the interactive session stage with the client. Otherwise, the server sends back to the client an SSH_MSG_FAILURE packet, indicating that the processing fails or it cannot resolve the request. The client sends a session request to the server, which processes the request and establishes a session.

Data exchange

In this stage, the server and the client exchanges data in this way:

- The client encrypts and sends the command to be executed to the server.
- The server decrypts and executes the command, and then encrypts and sends the result to the client.
- The client decrypts and displays the result on the terminal.

SSH Server and Client

To use SSH for secure login to a switch from a device, the switch must be configured as an SSH server and the device must be configured as an SSH client. As shown in [Figure 1-2](#), Host A, Host B, and Host D are configured as SSH clients to securely access the Switch A, which is acting as the SSH server.

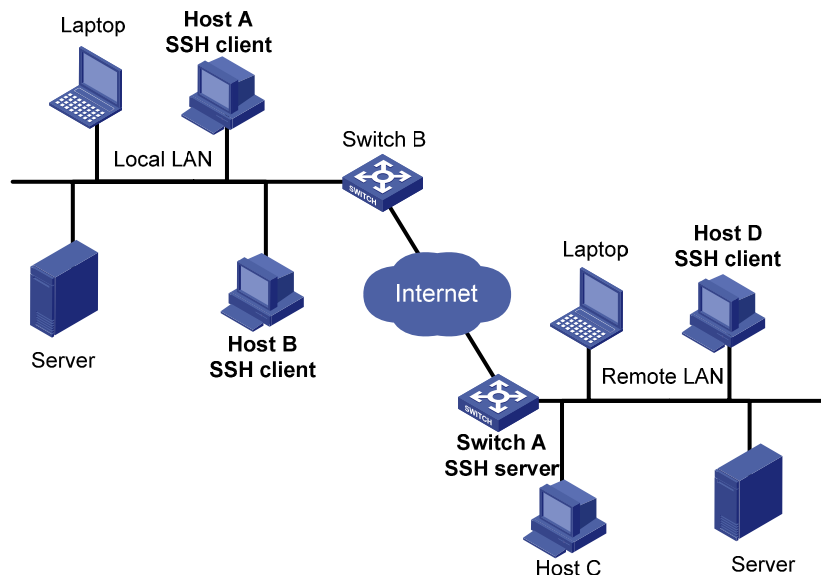


Figure 1-2 Network diagram for SSH connections

Configure the devices accordingly This document describes two cases:

- The switch acts as the SSH server to cooperate with software that supports the SSH client functions.
- The switch acts as the SSH server to cooperate with another switch that acts as an SSH client.

Complete the following tasks to configure the SSH server and clients:

Server	Client	Server side configuration	Client side configuration
switch	Software that supports the SSH client functions	Configuring the SSH Server	Configuring an SSH Client that Runs SSH Client Software
switch	Another switch	Configuring the SSH Server	Configuring an SSH Client Assumed by an SSH2-Capable Switch



Note

An SSH server forms a secure connection with each SSH client. The following describe steps for configuring an SSH client and an SSH server to form an SSH connection in between. If multiple SSH servers need to form connections with multiple SSH clients, configure each client and each server accordingly.

Configuring the SSH Server

The session establishment between an SSH client and the SSH server involves five stages. Similarly, SSH server configuration involves five aspects, as shown in the following table.

Complete the following tasks to configure the SSH server:

Task		Remarks
Preparation	Configuring the User Interfaces for SSH Clients	Required

Task		Remarks
	Configuring the SSH Management Functions	Optional
Version	Configuring the SSH Server to Be Compatible with SSH1 Clients	Optional This task determines which SSH versions the server should support. By default, the SSH server is compatible with SSH1 clients.
Key	Configuring Key Pairs	Required
Authentication	Creating an SSH User and Specifying an Authentication Type	Required
Authorization	Specifying a Service Type for an SSH User on the Server	Optional By default, an SSH user can use the service type of stelnet .
Data exchange	Configuring the Public Key of a Client on the Server	• Not necessary when the authentication mode is password. • Required when the authentication mode is publickey.
	Assigning a Public Key to an SSH User	• Not necessary when the authentication mode is password. • Required when the authentication mode is publickey.
	Exporting the Host Public Key to a File	Optional If a client does not support first-time authentication, you need to export the server's public key and configure the key on the client.



Note

The SSH server needs to cooperate with an SSH client to complete the interactions between them. For SSH client configuration, refer to [Configuring the SSH Client](#).

Configuring the User Interfaces for SSH Clients

An SSH client will access the device through a terminal “VTY” user interface. Therefore, you need to configure the device user interface to accept SSH clients and allow SSH login. Note that the configuration takes effect at the next login.

Follow these steps to configure the device user interface for SSH clients:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter user interface view of one or more user interfaces	user-interface vty <i>first-number</i> [<i>last-number</i>]	—

To do...	Use the command...	Remarks
Configure the authentication mode as scheme	authentication-mode scheme [command-authorization]	Required By default, the user interface authentication mode is password.
Specify the supported protocol(s)	protocol inbound { all ssh }	Optional By default, both Telnet and SSH are supported.



Caution

- If you have configured a user interface to support SSH protocol, you must configure AAA authentication for the user interface by using the **authentication-mode scheme** command to ensure successful login.
- On a user interface, if the **authentication-mode password** or **authentication-mode none** command has been executed, the **protocol inbound ssh** command is not available. Similarly, if the **protocol inbound ssh** command has been executed, the **authentication-mode password** and **authentication-mode none** commands are not available.

Configuring the SSH Management Functions

The SSH server provides a number of management functions to prevent illegal operations such as malicious password guess, guaranteeing the security of SSH connections. You can specify the IP address or the interface corresponding to the IP address for the SSH server to provide SSH access services for clients. In this way, the SSH client accesses the SSH server only using the specified IP address. This increases the service manageability when the SSH server has multiple interfaces and IP addresses.

Follow these steps to configure SSH management functions:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the SSH authentication timeout time	ssh server timeout <i>seconds</i>	Optional By default, the SSH authentication timeout time is 60 seconds.
Set the number of SSH authentication retry attempts	ssh server authentication-retries <i>times</i>	Optional By default, the number of SSH authentication retry attempts is 3.
Set the RSA server key update interval	ssh server rekey-interval <i>hours</i>	Optional By default, the system does not update the RSA server keys.
Configure a login header	header shell <i>text</i>	Optional By default, no login header is configured.

To do...	Use the command...	Remarks
Specify a source IP address for the SSH server	ssh-server source-ip <i>ip-address</i>	Optional By default, no source IP address is configured.
Specify a source interface for the SSH server	ssh-server source-interface <i>interface-type</i> <i>interface-number</i>	Optional By default, no source interface is configured.



Caution

- You can configure a login header only when the service type is **stelnet**. For configuration of service types, refer to [Specifying a Service Type for an SSH User on the Server](#).
- For details of the **header** command, refer to the corresponding section in *Login Command*.

Configuring the SSH Server to Be Compatible with SSH1 Clients

Follow these steps to configure the SSH server to be compatible with SSH1 clients:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the SSH server to be compatible with SSH1 clients	ssh server compatible-ssh1x enable	Optional By default, the SSH server is compatible with SSH1 clients.

Configuring Key Pairs

The SSH server's key pairs are for generating session keys and for SSH clients to authenticate the server. The SSH client's key pairs are for the SSH server to authenticate the SSH clients in publickey authentication mode. Both RSA and DSA key pairs are supported.

As different clients may support different public key algorithms, the key pairs negotiated between the server and clients may be different. Therefore, you need to generate both RSA and DSA key pairs on the server to ensure that clients can log in to the server successfully.

You can specify an algorithm for publickey authentication as needed.

Generating key pairs

When generating a key pair, you will be prompted to enter the key length in bits, which is between 512 and 2048. The default length is 1024. If the key pair already exists, the system will ask whether to overwrite it.

Follow these steps to create key pairs:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...		Use the command...	Remarks
Generate key pair(s)	Generate an RSA key pairs	public-key local create rsa	Required By default, no key pairs are generated.
	Generate a DSA key pair	public-key local create dsa	



Note

- The command for generating a key pair can survive a reboot. You only need to configure it once.
- It takes more time to encrypt and decrypt data with a longer key, which, however, ensures higher security. Therefore, specify the length of the key pair accordingly.
- For a fabric made up of multiple devices, you need to create the key pairs on the device to ensure that all devices in the fabric have the same local RSA key pairs.
- Some third-party software, for example, WinSCP, requires that the modulo of a public key must be greater than or equal to 768. Therefore, a local key pair of more than 768 bits is recommended.

Destroying key pairs

The RSA or DSA keys may be exposed, and you may want to destroy the keys and generate new ones. Follow these steps to destroy key pairs:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Destroy key pair(s)	Destroy the RSA key pairs	public-key local destroy rsa	Optional
	Destroy the DSA key pair	public-key local destroy dsa	

Creating an SSH User and Specifying an Authentication Type

This task is to create an SSH user and specify an authentication type. Specifying an authentication type for a new user is a must to get the user login.

An SSH user is represented as a set of user attributes on the SSH server. This set is uniquely identified with the SSH username. When a user logs in to the SSH server from the SSH client, a username is required so that the server can look up the database for matching the username. If a match is found, it authenticates the user using the authentication mode specified in the attribute set. If not, it tears down the connection.

To prevent illegal users from logging in to the device, SSH supports the authentication modes of password, publickey, and password-publickey.

- Password authentication

SSH uses the authentication function of AAA to authenticate the password of the user that is logging in. Based on the AAA authentication scheme, password authentication can be done locally or remotely. For local authentication, the SSH server saves the user information and implements the authentication. For remote authentication, the user information is saved on an authentication server (such as a RADIUS server) and authentication is implemented through the cooperation of the SSH server and the authentication server. For AAA details, refer to *AAA Operation*.

- Publickey authentication

Publickey authentication provides more secure SSH connections than password authentication does. At present, the device supports RSA and DSA for publickey authentication. After configuration, authentication is implemented automatically without asking you to enter the password. In this mode, you need to create a key pair on each client, and configure each client's public key on the server. This may be complicated when multiple SSH clients want to access one SSH server in the network.

- Password-publickey authentication

An SSH user must pass both types of authentication before logging in. In this mode, you do not need to create a key pair on each client. You can configure the clients to use the same key pair that is created on one client for publickey authentication. With the AAA function in password authentication, the level of commands available to a logged-in SSH user is determined by the AAA scheme..

Follow these steps to configure an SSH user and specify an authentication type for the user:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify the default authentication type for all SSH users	ssh authentication-type default { all password password-publickey publickey }	Use either command. By default, no SSH user is created and no authentication type is specified.
	ssh user <i>username</i>	Note that: If both commands are used and different authentication types are specified, the authentication type specified with the ssh user authentication-type command takes precedence.
Create an SSH user, and specify an authentication type for it	ssh user <i>username</i> authentication-type { all password password-publickey publickey }	



Caution

- For **password** authentication type, the *username* argument must be consistent with the valid user name defined in AAA; for **publickey** authentication, the *username* argument 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.
- Under the **publickey** authentication mode, the level of commands available to a logged-in SSH user can be configured using the **user privilege level** command on the server, and all the users with this authentication mode will enjoy this level.
- Under the **password** or **password-publickey** authentication mode, the level of commands available to a logged-in SSH user is determined by the AAA scheme. Meanwhile, for different users, the available levels of commands are also different.
- Under the **all** authentication mode, the level of commands available to a logged-in SSH user is determined by the actual authentication method used for the user.

Specifying a Service Type for an SSH User on the Server

At present, the switch supports two service types for SSH: stelnet (secure Telnet) and SFTP.

- The secure Telnet service is a basic application of SSH protocol. It uses the secure channel of SSH to provide remote login.
- The SFTP service is an extended application of SSH protocol. It uses the secure channel of SSH to perform remote FTP operations.

Follow these steps to specify the service type for an SSH user:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify a service type for an SSH user	ssh user <i>username</i> service-type { stelnet sftp all }	Required By default, an SSH user can use the service type of stelnet .



Caution

If the **ssh user service-type** command is executed with a username that does not exist, the system will automatically create the SSH user. However, the user cannot log in unless you specify an authentication type for it.

Configuring the Public Key of a Client on the Server



Note

This configuration is not necessary if the **password** authentication mode is configured for SSH users.

With the **publickey** authentication mode configured for an SSH client, you must configure the client's RSA or DSA host public key(s) on the server for authentication.

You can manually configure the public key or import it from a public key file. In the former case, you can manually copy the client's public key to the server. In the latter case, the system automatically converts the format of the public key generated by the client to complete the configuration on the server, but the client's public key should be transferred from the client to the server beforehand through FTP/TFTP.

Follow these steps to configure the public key of a client manually:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter public key view	public-key peer <i>keyname</i>	Required
Enter public key edit view	public-key-code begin	—
Configure a public key for the client	Enter the content of the public key	When you input the key, 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	—
Exit public key view and return to system view	peer-public-key end	—

Follow these steps to import the public key from a public key file:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Import the public key from a public key file	public-key peer <i>keyname</i> import sshkey <i>filename</i>	Required

Assigning a Public Key to an SSH User



Caution

This configuration task is unnecessary if the SSH user's authentication mode is **password**.

For the **publickey** authentication mode, you must specify the client's public key on the server for authentication.

Follow these steps to assign a public key for an SSH user:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Assign a public key to an SSH user	ssh user <i>username</i> assign publickey <i>keyname</i>	Required If you issue this command multiple times, the last command overrides the previous ones.

Exporting the Host Public Key to a File

In tasks of [Configuring the Public Key of a Client on the Server](#) or [Configuring whether first-time authentication is supported](#), an SSH client's or an SSH server's host public key can be imported from a public key file. This task allows you to export the host public key to a file on the client or server device with key pairs generated.

Follow these steps to export the RSA host public key:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Export the RSA host public key to a specified file	public-key local export rsa { openssh ssh1 ssh2 } [<i>filename</i>]	Required

Follow these steps to export the DSA host public key:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Export the DSA host public key to a specified file	public-key local export dsa { openssh ssh2 } [<i>filename</i>]	Required



Note

- With the *filename* argument specified, you can export the RSA or DSA host public key to a file so that you can configure the key at a remote end by importing the file. If the *filename* argument is not specified, this command displays the host public key information on the screen in a specified format.
- The RSA host public key format can be SSH1, SSH2 and OpenSSH, while the DSA host public key format can be SSH2 and OpenSSH. DSA does not support the format of SSH1.

Configuring the SSH Client

The configurations required on the SSH client are related to the authentication mode that the SSH server uses. In addition, if an SSH client does not support first-time authentication, you need to configure the public key of the server on the client, so that the client can authenticate the server.

SSH Client Configuration Task List

Complete the following tasks to configure the SSH client:

Scenario	SSH client configuration task	
	For a client running SSH client software	For a client assumed by an SSH2-capable switch
The authentication mode is password	Configuring an SSH Client that Runs SSH Client Software	Configuring an SSH Client Assumed by an SSH2-Capable Switch
The authentication mode is publickey	Configuring an SSH Client that Runs SSH Client Software	Configuring an SSH Client Assumed by an SSH2-Capable Switch
Whether first-authentication is supported	—	Configuring an SSH Client Assumed by an SSH2-Capable Switch

Configuring an SSH Client that Runs SSH Client Software

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, use the following commands:

Complete the following tasks to configure an SSH client that runs SSH client software:

Task	Remarks
Generating a client key	Required for publickey authentication; unnecessary for password authentication
Specifying the IP address of the Server	Required
Selecting a protocol for remote connection	Required
Selecting an SSH version	Required

Task	Remarks
Opening an SSH connection with password authentication	Required for password authentication; unnecessary for publickey authentication
Opening an SSH connection with publickey authentication	Required for publickey authentication; unnecessary for password authentication



Note

- For putty, it is recommended to use PuTTY release 0.53; PuTTY release 0.58 is also supported. For OpenSSH, it is recommended to use OpenSSH_3.1p1; OpenSSH_4.2p1 is also supported. Any other version or other client, please be careful to use.
- 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 SSH2.0 now, select 2.0 or lower for the client.
- Specifying the private key file. On the server, if public key 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 and DSA key pairs are generated by a tool of the client software.

The following takes the client software of PuTTY Version 0.58 as an example to illustrate how to configure the SSH client:

Generating a client key

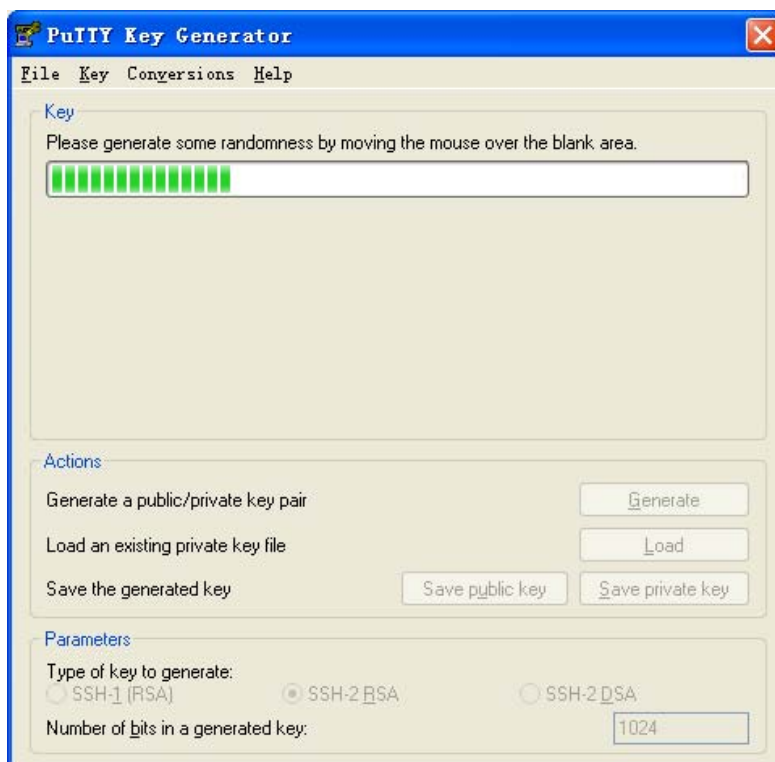
To generate a client key, run PuTTYGen.exe, and select from the **Parameters** area the type of key you want to generate, either SSH-2 RSA or SSH-2 DSA, then click **Generate**.

Figure 1-3 Generate a client key (1)



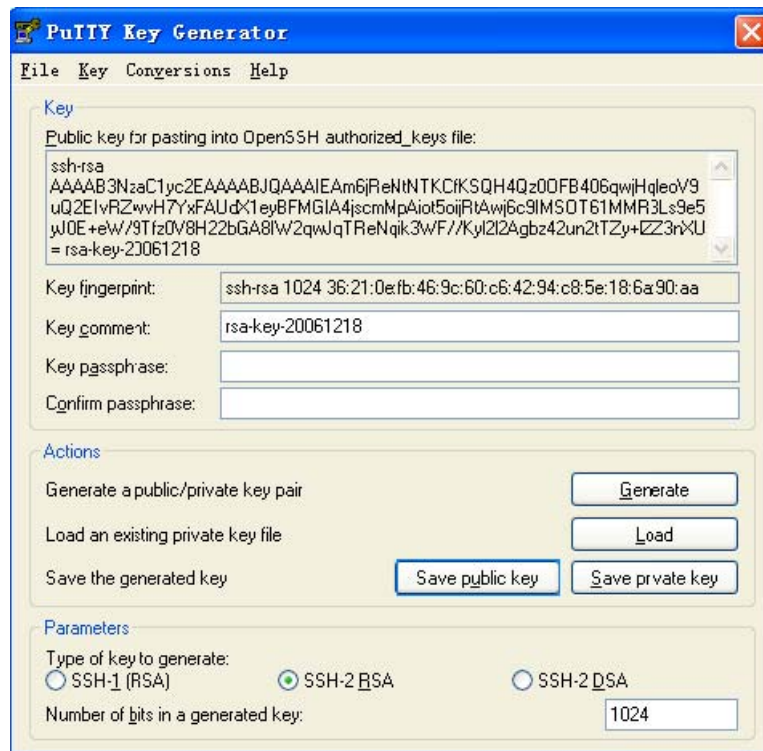
Note that while generating the key pair, you must move the mouse continuously and keep the mouse off the green process bar in the blue box of shown in [Figure 1-4](#). Otherwise, the process bar stops moving and the key pair generating process is stopped.

Figure 1-4 Generate the client keys (2)



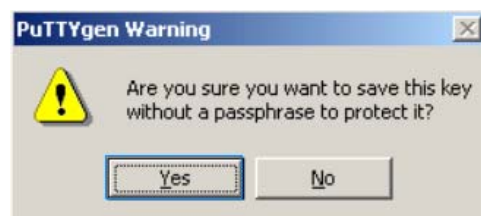
After the key pair is generated, click **Save public key** and enter the name of the file for saving the public key (**public** in this case) to save the public key.

Figure 1-5 Generate the client keys (3)



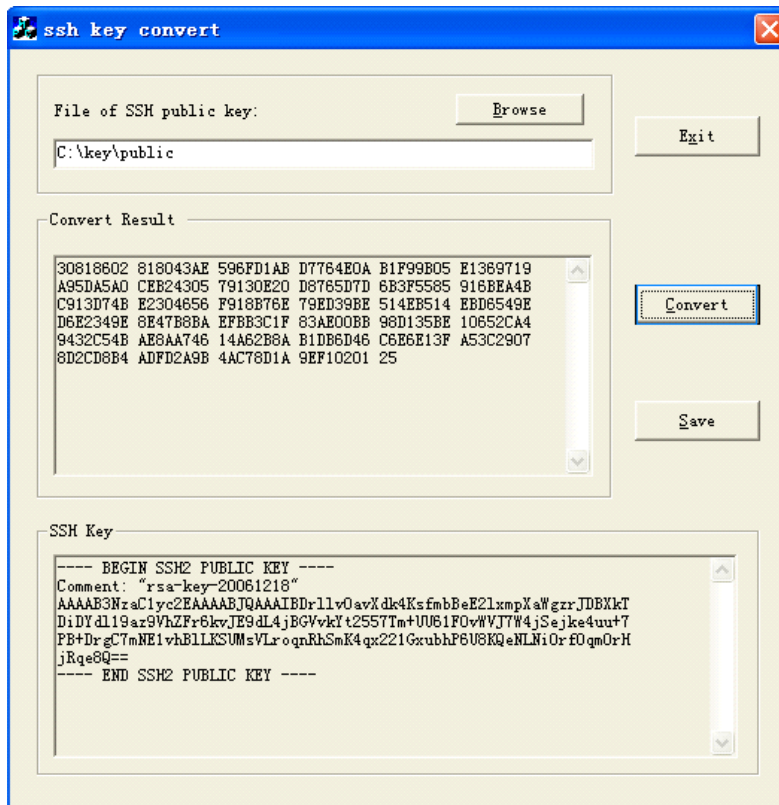
Likewise, to save the private key, click **Save private key**. A warning window pops up to prompt you whether to save the private key without any precaution. Click **Yes** and enter the name of the file for saving the private key ("private" in this case) to save the private key.

Figure 1-6 Generate 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**.

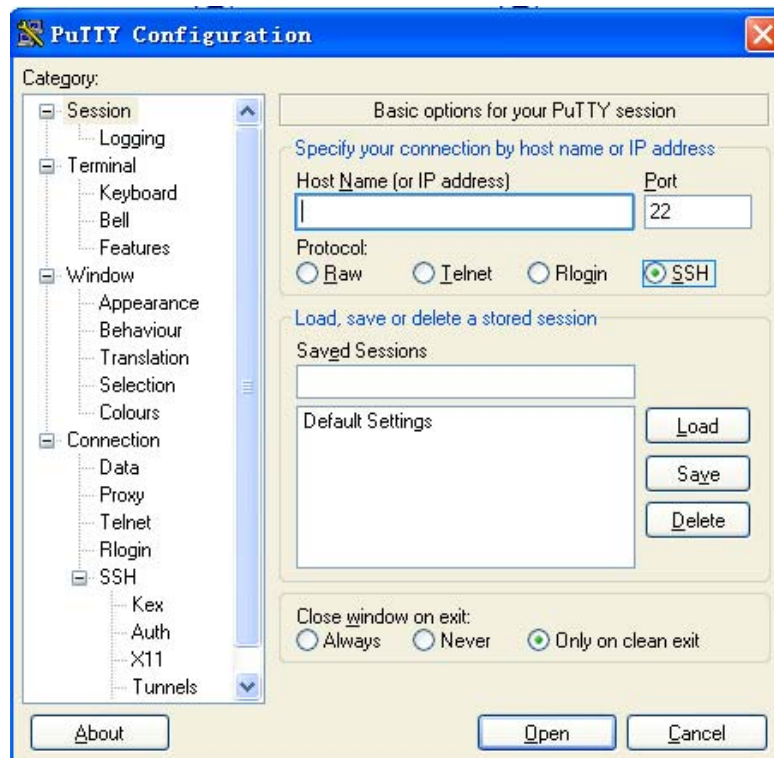
Figure 1-7 Generate the client keys (5)



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.

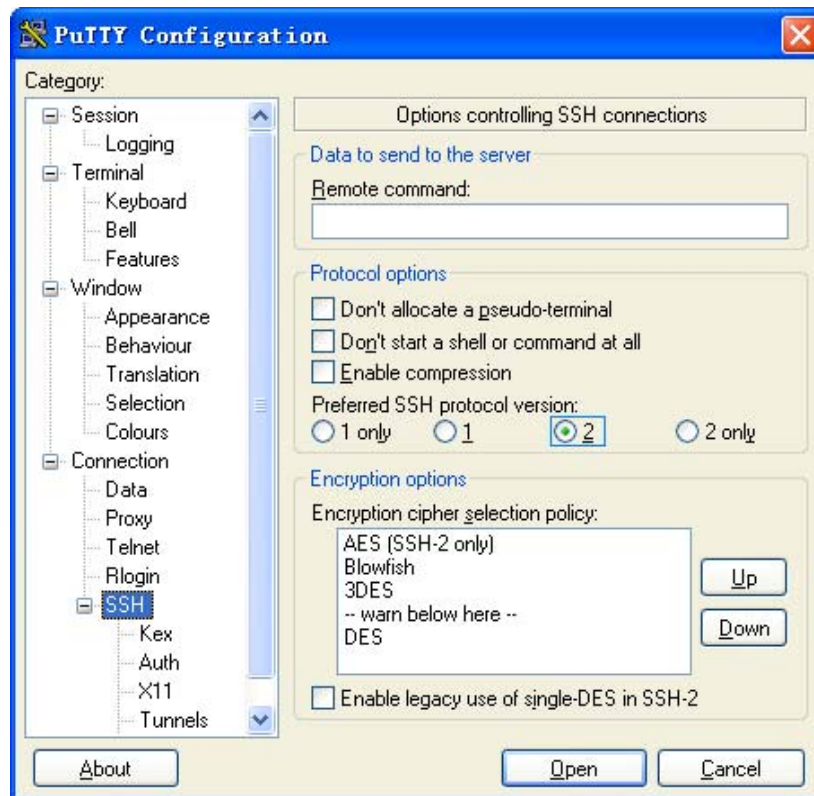
Selecting a protocol for remote connection

As shown in [Figure 1-8](#), select **SSH** under **Protocol**.

Selecting an 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.

Opening an SSH connection with password authentication

From the window shown in [Figure 1-9](#), click **Open**. If the connection is normal, you will be prompted to enter the username and password.

Enter the username and password to establish an SSH connection.

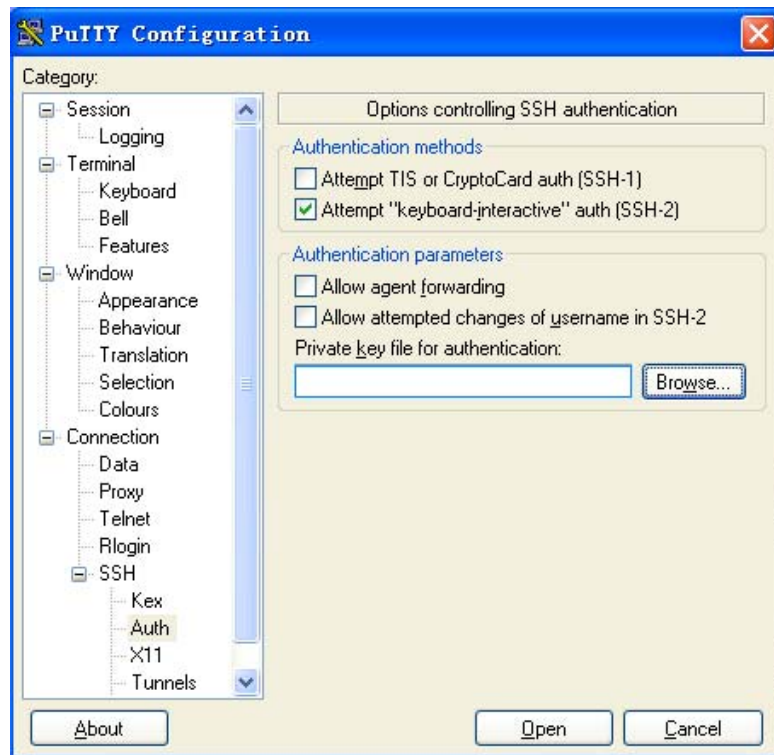
To log out, enter the **quit** command.

Opening an SSH connection with publickey authentication

If a user needs to be authenticated with a public key, the corresponding private key file must be specified. A private key file is not required for password-only authentication.

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 **Open**. If the connection is normal, a user will be prompted for a username. Once passing the authentication, the user can log in to the server.

Configuring an SSH Client Assumed by an SSH2-Capable Switch

Complete the following tasks to configure an SSH client that is assumed by an SSH2-capable switch:

Task	Remarks
Configuring the SSH client for publickey authentication	Required for publickey authentication; unnecessary for password authentication
Configuring whether first-time authentication is supported	Optional
Specifying a source IP address/interface for the SSH client	Optional
Establishing the connection between the SSH client and server	Required

Configuring the SSH client for publickey authentication

When the authentication mode is **publickey**, you need to configure the RSA or DSA public key of the client on the server:

- To generate a key pair on the client, refer to [Configuring Key Pairs](#).
- To export the RSA or DSA public key of the client, refer to [Exporting the Host Public Key to a File](#).

- To configure the public key of a client on the server, refer to [Configuring the Public Key of a Client on the Server](#).

Configuring whether first-time authentication is supported

When the device connects to the SSH server as an SSH client, you can configure whether the device supports first-time authentication.

- With first-time authentication enabled, an SSH client that is not configured with the server host public key can continue accessing the server when it accesses the server for the first time, and it will save the host public key on the client for use in subsequent authentications.
- With first-time authentication disabled, an SSH client that is not configured with the server host public key will be denied of access to the server. To access the server, a user must configure in advance the server host public key locally and specify the public key name for authentication.

Follow these steps to enable the device to support first-time authentication:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the device to support first-time authentication	ssh client first-time enable	Optional By default, the client is enabled to run first-time authentication.

Follow these steps to disable first-time authentication support:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Disable first-time authentication support	undo ssh client first-time	Required By default, the client is enabled to run first-time authentication.
Configure server public key	Refer to Configuring the Public Key of a Client on the Server	Required The method of configuring server public key on the client is similar to that of configuring client public key on the server.
Specify the host key name of the server	ssh client { server-ip server-name } assign publickey keyname	Required



Note

With first-time authentication enabled, an SSH client that is not configured with the SSH server's host public key saves the host public key sent by the server without authenticating the server. Attackers may exploit the vulnerability to initiate man-in-middle attacks by acting as an SSH server. Therefore, it is recommended to disable first-time authentication unless you are sure that the SSH server is reliable.

Specifying a source IP address/interface for the SSH client

You can configure a source IP address or the source IP address by specifying the corresponding interface for the client to use to access the SSH server. This improves the service manageability when the SSH client has multiple IP addresses and interfaces

Follow these steps to specify a source IP address/interface for the SSH client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify a source IP address for the SSH client	ssh2 source-ip <i>ip-address</i>	Optional By default, no source IP address is configured.
Specify a source interface for the SSH client	ssh2 source-interface <i>interface-type interface-number</i>	Optional By default, no source interface is configured.

Establishing the connection between the SSH client and server

The client's method of establishing an SSH connection to the SSH server varies with authentication types.

Follow these steps to establish an SSH connection:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Start the client to establish a connection with an SSH server	ssh2 { <i>host-ip</i> <i>host-name</i> } [<i>port-num</i>] [identity-key { <i>dsa</i> <i>rsa</i> } prefer_kex { <i>dh_group1</i> dh_exchange_group } prefer_ctos_cipher { <i>3des</i> <i>des</i> <i>aes128</i> } prefer_stoc_cipher { <i>3des</i> <i>des</i> <i>aes128</i> } prefer_ctos_hmac { <i>sha1</i> <i>sha1_96</i> <i>md5</i> <i>md5_96</i> } prefer_stoc_hmac { <i>sha1</i> <i>sha1_96</i> <i>md5</i> <i>md5_96</i> }] *	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 Note that: The identity-key keyword is unnecessary in password authentication and optional in public key authentication.



Note

When logging into the SSH server using public key authentication, an SSH client needs to read its local private key for authentication. As two algorithms (RSA or DSA) are available, the **identity-key** keyword must be used to specify one algorithm in order to get the correct private key.

Displaying and Maintaining SSH Configuration

To do...	Use the command...	Remarks
Display the public key information of the current switch's key pairs	display public-key local { dsa rsa } public	Available in any view
Display information about locally saved public keys of SSH peers	display public-key peer [brief name pubkey-name]	
Display information about SSH status and about sessions of active connections with SSH clients	display ssh server { session status }	
Display information about all SSH users	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 or the IP address of the source interface specified for the SSH Client.	display ssh2 source-ip	

Comparison of SSH Commands with the Same Functions

After the SSH protocol supports the DSA asymmetric key algorithm, some SSH configuration commands are changed. For the sake of SSH configuration compatibility, the original commands are still supported. [Table 1-2](#) lists both the original commands and current commands.

Table 1-2 List of SSH configuration commands with the same functions

Operation	Original commands	Current commands
Display local RSA public keys	display rsa local-key-pair public	display public-key local rsa public
Display information about the peer RSA public keys	display rsa peer-public-key [brief name keyname]	display public-key peer [brief name pubkey-name]
Generate RSA key pairs	rsa local-key-pair create	public-key local create rsa
Destroy RSA key pairs	rsa local-key-pair destroy	public-key local destroy rsa
Enter public key view	rsa peer-public-key keyname	public-key peer keyname
Import RSA public key from public key file	rsa peer-public-key keyname import sshkey filename	public-key peer keyname import sshkey filename
Specify publickey authentication as the default authentication type for all SSH clients	ssh authentication-type default rsa	ssh authentication-type default publickey

Operation	Original commands	Current commands
Specify on the client the host public key of the server to be connected	ssh client { <i>server-ip</i> <i>server-name</i> } assign rsa-key <i>keyname</i>	ssh client { <i>server-ip</i> <i>server-name</i> } assign publickey <i>keyname</i>
Assign a public key to an SSH user	ssh user <i>username</i> assign rsa-key <i>keyname</i>	ssh user <i>username</i> assign publickey <i>keyname</i>
Create an SSH user and specify publickey authentication as its authentication type	ssh user <i>username</i> authentication-type <i>rsa</i>	ssh user <i>username</i> authentication-type <i>publickey</i>



Note

- After RSA key pairs are generated, the **display rsa local-key-pair public** command displays two public keys (the host public key and server public key) when the switch is working in SSH1-compatible mode, but only one public key (the host public key) when the switch is working in SSH2 mode.
- The results of the **display rsa local-key-pair public** command or the public key converted with the SSHKEY tool contains no information such as the authentication type, so they cannot be directly used as parameters in the **public-key peer** command. For the same reason, neither can the results of the **display public-key local rsa public** command be used in the **rsa peer-public-key** command directly.

SSH Configuration Examples

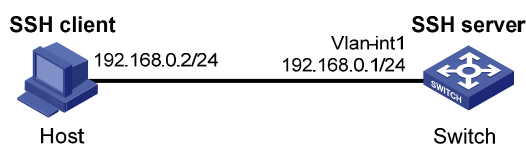
When Switch Acts as Server for Local Password Authentication

Network requirements

As shown in [Figure 1-11](#), establish an SSH connection between the host (SSH Client) and the switch (SSH Server) for secure data exchange. The host runs SSH2.0 client software. Password authentication is required.

Network diagram

Figure 1-11 Switch acts as server for local password authentication



Configuration procedure

- Configure the SSH server

Create a VLAN interface on the switch and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[Switch-Vlan-interface1] quit
```



Caution

Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

Generate RSA and DSA key pairs.

```
[Switch] public-key local create rsa
[Switch] public-key local create dsa
```

Set the authentication mode for the user interfaces to AAA.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

Create local client **client001**, and set the authentication password to **abc**, protocol type to SSH, and command privilege level to 3 for the client.

```
[Switch] local-user client001
[Switch-luser-client001] password simple abc
[Switch-luser-client001] service-type ssh level 3
[Switch-luser-client001] quit
```

Specify the authentication method of user client001 as password.

```
[Switch] ssh user client001 authentication-type password
```

- Configure the SSH client

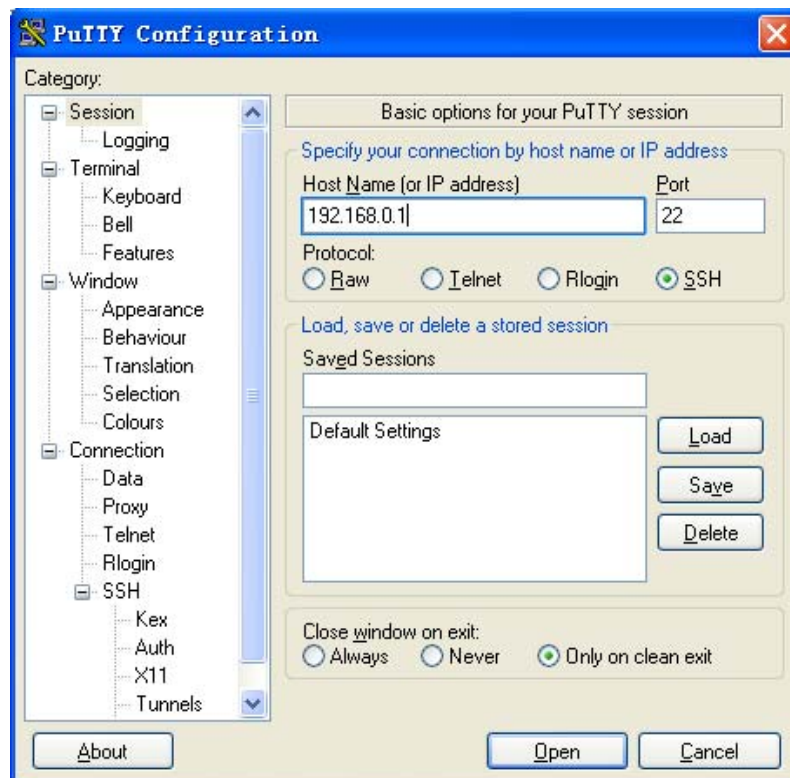
Configure an IP address (192.168.0.2 in this case) for the SSH client. This IP address and that of the VLAN interface on the switch must be in the same network segment.

Configure the SSH client software to establish a connection to the SSH server.

Take SSH client software **Putty** (version 0.58) as an example:

- 1) Run PuTTY.exe to enter the following configuration interface.

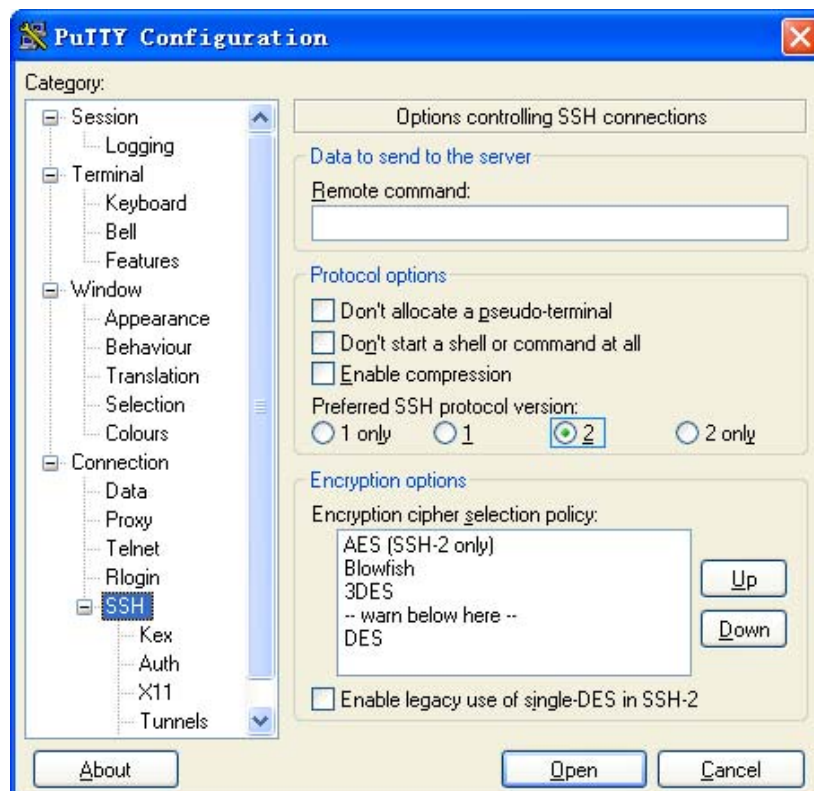
Figure 1-12 SSH client configuration interface (1)



In the **Host Name (or IP address)** text box, enter the IP address of the SSH server.

- 2) From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in [Figure 1-13](#) appears.

Figure 1-13 SSH client configuration interface (2)



Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

- 3) As shown in [Figure 1-13](#), click **Open**. If the connection is normal, you will be prompted to enter the user name **client001** and password **abc**. Once authentication succeeds, you will log in to the server.

When Switch Acts as Server for Password and RADIUS Authentication

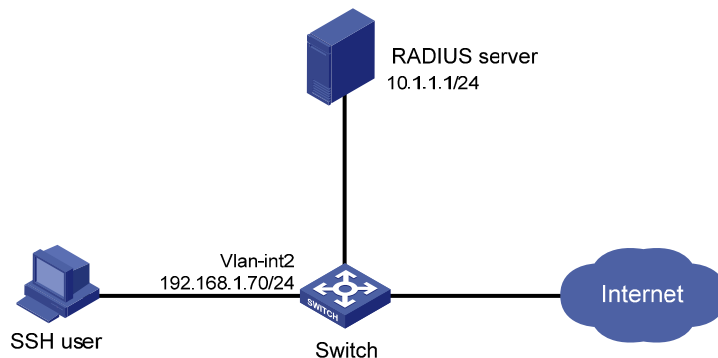
Network requirements

As shown in [Figure 1-14](#), an SSH connection is required between the host (SSH client) and the switch (SSH server) for secure data exchange. Password and RADIUS authentication is required.

- The host runs SSH2.0 client software to establish a local connection with the switch.
- The switch cooperates with a RADIUS server to authenticate SSH users.

Network diagram

Figure 1-14 Switch acts as server for password and RADIUS authentication



Configuration procedure

- 1) Configure the RADIUS server



Note

This document takes CAMS Version 2.10 as an example to show the basic RADIUS server configurations required.

Add an access device.

Log in to the CAMS management platform and select **System Management > System Configuration** from the navigation tree. In the **System Configuration** page, click **Modify** of the **Access Device** item, and then click **Add** to enter the **Add Access Device** page and perform the following configurations:

- Specify the IP address of the switch as 192.168.1.70.
- Set both the shared keys for authentication and accounting packets to **expert**.
- Select **LAN Access Service** as the service type.
- Specify the ports for authentication and accounting as 1812 and 1813 respectively.
- Select **Extensible Protocol** as the protocol type.

- Select **Standard** as the RADIUS packet type.

Figure 1-15 Add an access device

Add a user account for device management.

From the navigation tree, select **User Management > User for Device Management**, and then in the right pane, click **Add** to enter the **Add Account** page and perform the following configurations:

- Add a user named **hello**, and specify the password.
- Select **SSH** as the service type.
- Specify the IP address range of the hosts to be managed.

Figure 1-16 Add an account for device management

Configure the SSH server

Create a VLAN interface on the switch and assign it an IP address. This address will be used as the IP address of the SSH server for SSH connections.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```



Caution

Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

Generate RSA and DSA key pairs.

```
[Switch] public-key local create rsa
```

```
[Switch] public-key local create dsa
```

Set the authentication mode for the user interfaces to AAA.

```
[Switch] user-interface vty 0 4
```

```
[Switch-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh
```

```
[Switch-ui-vty0-4] quit
```

Configure the RADIUS scheme.

```
[Switch] radius scheme rad
```

```
[Switch-radius-rad] accounting optional
```

```
[Switch-radius-rad] primary authentication 10.1.1.1 1812
```

```
[Switch-radius-rad] key authentication expert
```

```
[Switch-radius-rad] server-type extended
```

```
[Switch-radius-rad] user-name-format without-domain
```

```
[Switch-radius-rad] quit
```

Apply the scheme to the ISP domain.

```
[Switch] domain bbb
```

```
[Switch-isp-bbb] scheme radius-scheme rad
```

```
[Switch-isp-bbb] quit
```

Configure an SSH user, specifying the switch to perform password authentication for the user.

```
[Switch] ssh user hello authentication-type password
```

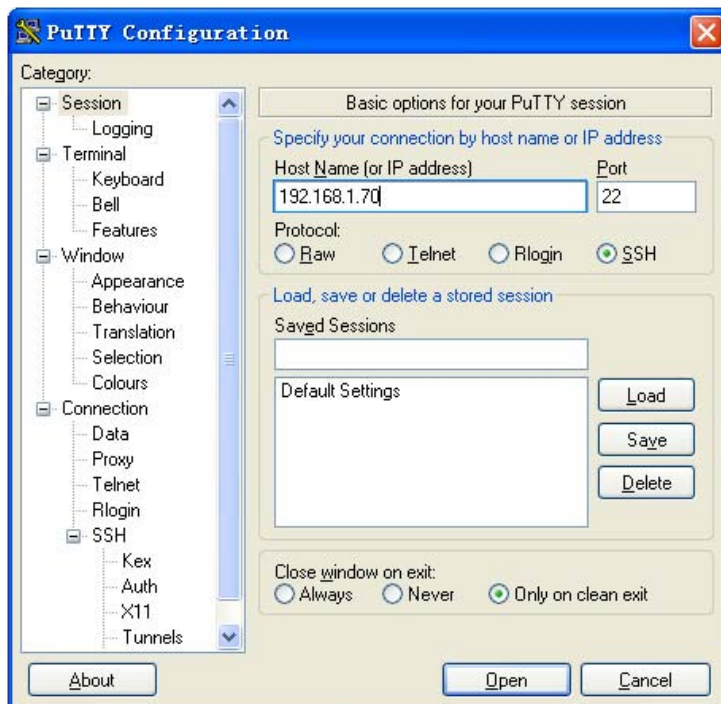
Configure the SSH client

Configure an IP address (192.168.1.1 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.

Configure the SSH client software to establish a connection to the SSH server. Take SSH client software PuTTY Version 0.58 as an example:

- Run PuTTY.exe to enter the following configuration interface.

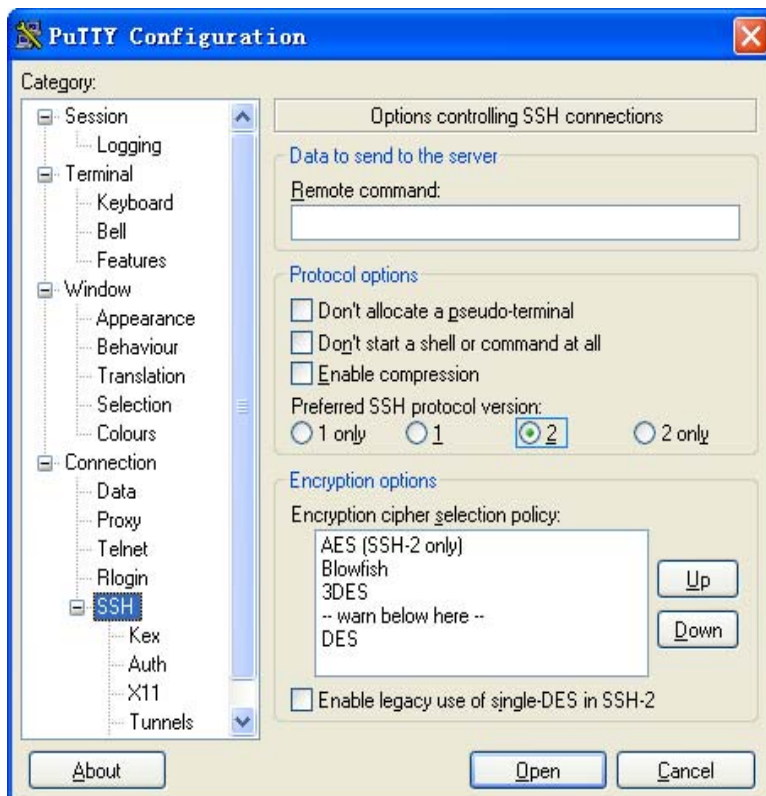
Figure 1-17 SSH client configuration interface (1)



In the **Host Name (or IP address)** text box, enter the IP address of the SSH server.

- From the category on the left pane of the window, select **Connection > SSH**. The window as shown in [Figure 1-18](#) appears.

Figure 1-18 SSH client configuration interface (2)



Under **Protocol options**, select **2** from **Preferred SSH protocol version**. Then, click **Open**. If the connection is normal, you will be prompted to enter the user name **hello** and the password. Once authentication succeeds, you will log in to the server. The level of commands that you can access after

login is authorized by the CAMS server. You can specify the level by setting the **EXEC Privilege Level** argument in the **Add Account** window shown in [Figure 1-16](#).

When Switch Acts as Server for Password and HWTACACS Authentication

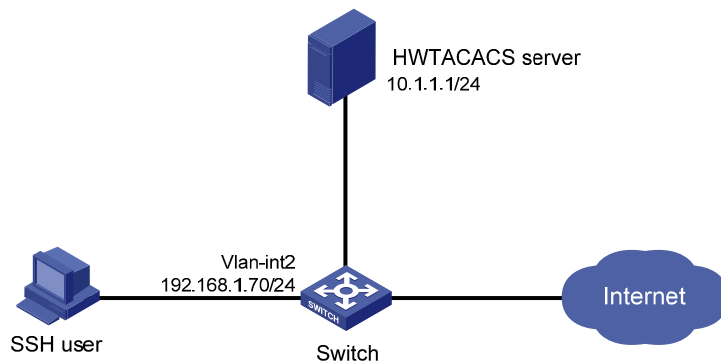
Network requirements

As shown in [Figure 1-19](#), an SSH connection is required between the host (SSH client) and the switch (SSH server) for secure data exchange. Password and HWTACACS authentication is required.

- The host runs SSH2.0 client software to establish a local connection with the switch.
- The switch cooperates with an HWTACACS server to authenticate SSH users.

Network diagram

Figure 1-19 Switch acts as server for password and HWTACACS authentication



Configuration procedure

- Configure the SSH server

Create a VLAN interface on the switch and assign it an IP address. This address will be used as the IP address of the SSH server for SSH connections.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```



Caution

Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

Generate RSA and DSA key pairs.

```
[Switch] public-key local create rsa
[Switch] public-key local create dsa
```

Set the authentication mode for the user interfaces to AAA.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh  
[Switch-ui-vty0-4] quit
```

Configure the HWTACACS scheme.

```
[Switch] hwtacacs scheme hwtac  
[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49  
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.1 49  
[Switch-hwtacacs-hwtac] key authentication expert  
[Switch-hwtacacs-hwtac] key authorization expert  
[Switch-hwtacacs-hwtac] user-name-format without-domain  
[Switch-hwtacacs-hwtac] quit
```

Apply the scheme to the ISP domain.

```
[Switch] domain bbb  
[Switch-isp-bbb] scheme hwtacacs-scheme hwtac  
[Switch-isp-bbb] quit
```

Configure an SSH user, specifying the switch to perform password authentication for the user.

```
[Switch] ssh user client001 authentication-type password
```

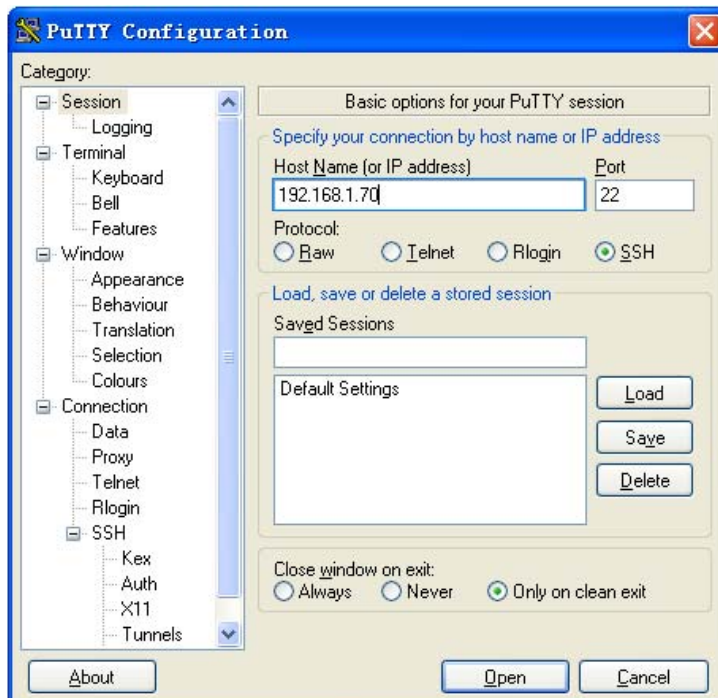
- Configure the SSH client

Configure an IP address (192.168.1.1 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.

Configure the SSH client software to establish a connection to the SSH server. Take SSH client software PuTTY Version 0.58 as an example:

- 1) Run PuTTY.exe to enter the following configuration interface.

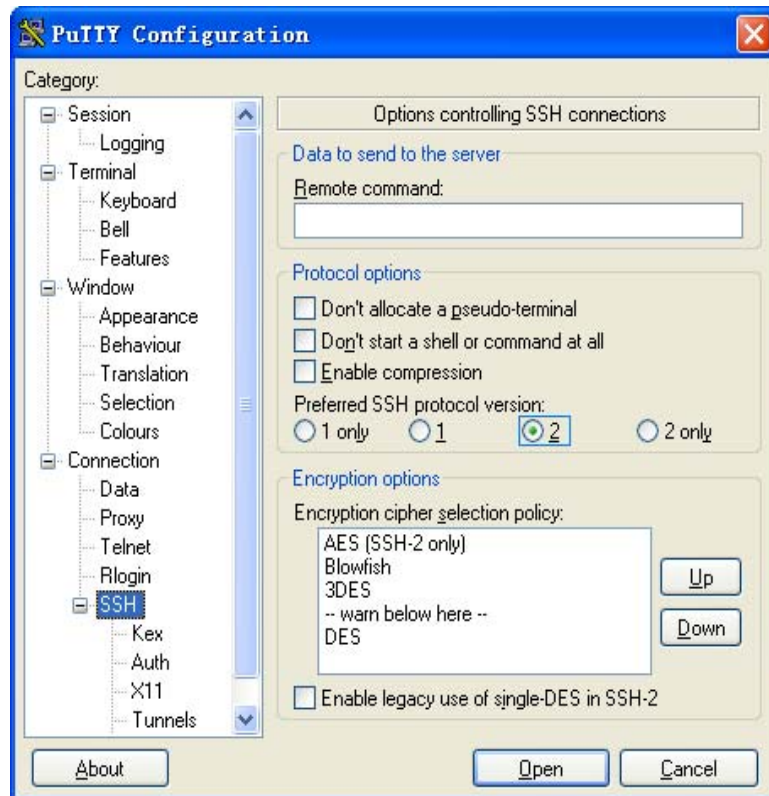
Figure 1-20 SSH client configuration interface (1)



In the **Host Name (or IP address)** text box, enter the IP address of the SSH server.

- 2) From the category on the left pane of the window, select **Connection > SSH**. The window as shown in [Figure 1-21](#) appears.

Figure 1-21 SSH client configuration interface (2)



Under **Protocol options**, select **2** from **Preferred SSH protocol version**. Then, click **Open**. If the connection is normal, you will be prompted to enter the user name **client001** and the password. Once authentication succeeds, you will log in to the server. The level of commands that you can access after login is authorized by the HWTACACS server. For authorization configuration of the HWTACACS server, refer to relevant HWTACACS server configuration manuals.

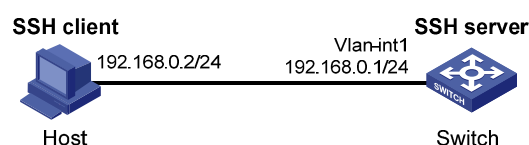
When Switch Acts as Server for Publickey Authentication

Network requirements

As shown in [Figure 1-22](#), establish an SSH connection between the host (SSH client) and the switch (SSH Server) for secure data exchange. The host runs SSH2.0 client software. Publickey authentication is required.

Network diagram

Figure 1-22 Switch acts as server for publickey authentication



Configuration procedure



Note

Under the **publickey** authentication mode, either the RSA or DSA public key can be generated for the server to authenticate the client. Here takes the RSA public key as an example.

- Configure the SSH server

Create a VLAN interface on the switch and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[Switch-Vlan-interface1] quit
```



Note

Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

Generate RSA and DSA key pairs.

```
[Switch] public-key local create rsa
[Switch] public-key local create dsa
```

Set the authentication mode for the user interfaces to AAA.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh
```

Set the client's command privilege level to 3

```
[Switch-ui-vty0-4] user privilege level 3
[Switch-ui-vty0-4] quit
```

Configure the authentication type of the SSH client named client 001 as publickey.

```
[Switch] ssh user client001 authentication-type publickey
```



Note

Before performing the following steps, you must generate an RSA public key pair (using the client software) on the client, save the key pair in a file named public, and then upload the file to the SSH server through FTP or TFTP. For details, refer to the SSH client configuration part. .

Import the client's public key named **Switch001** from file **public**.

```
[Switch] public-key peer Switch001 import sshkey public
```

Assign the public key **Switch001** to client **client001**.

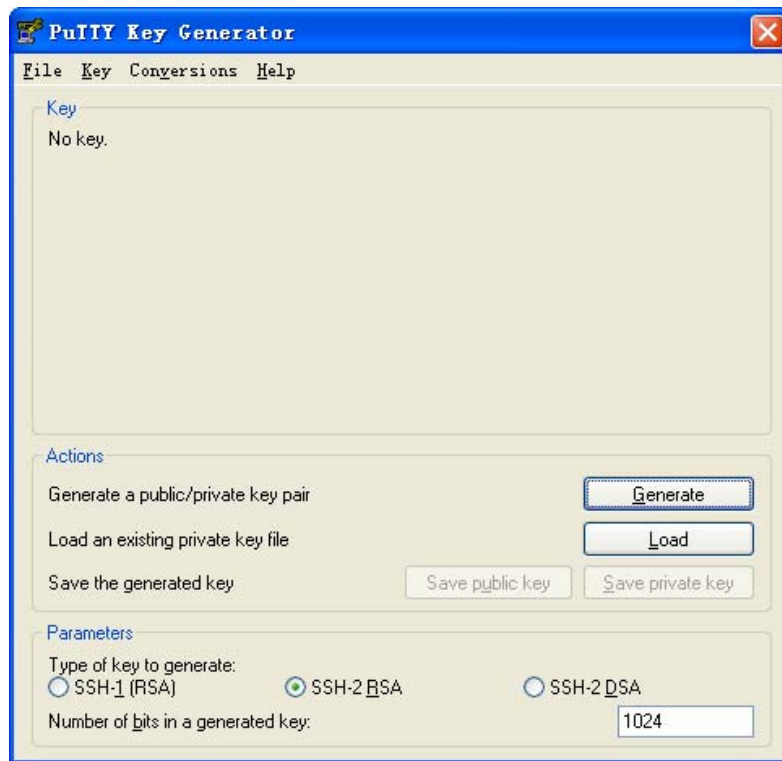
```
[Switch] ssh user client001 assign publickey Switch001
```

- Configure the SSH client (taking PuTTY version 0.58 as an example)

Generate an RSA key pair.

- 1) Run PuTTYGen.exe, choose **SSH2(RSA)** and click **Generate**.

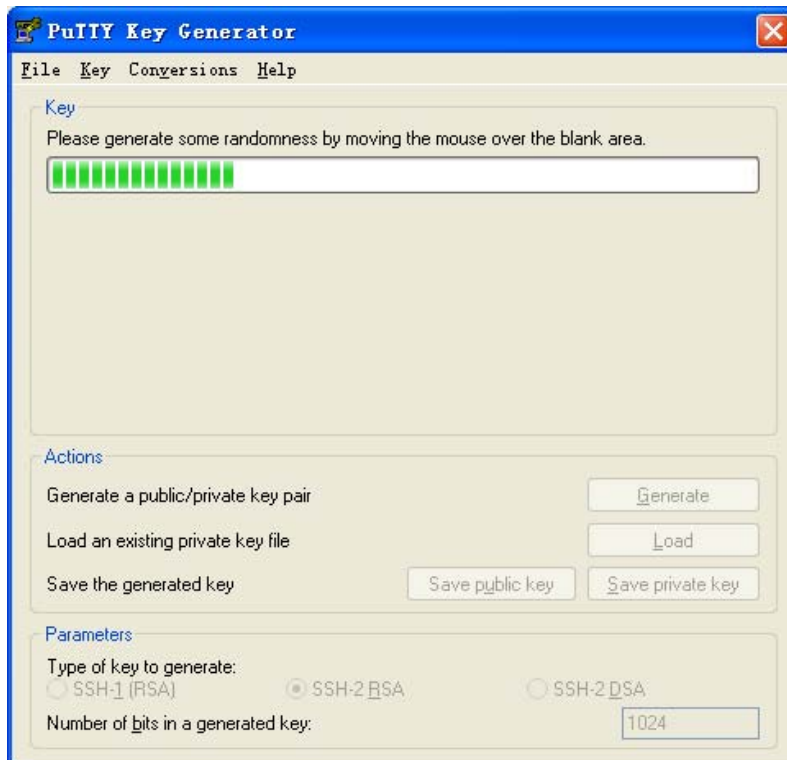
Figure 1-23 Generate a client key pair (1)



Note

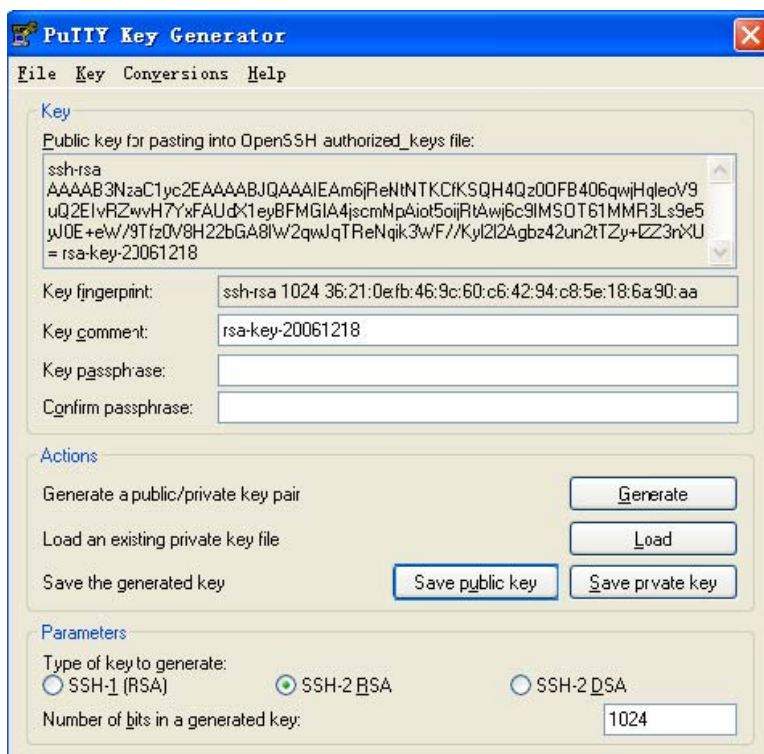
While generating the key pair, you must move the mouse continuously and keep the mouse off the green process bar shown in [Figure 1-24](#). Otherwise, the process bar stops moving and the key pair generating process is stopped.

Figure 1-24 Generate a client key pair (2)



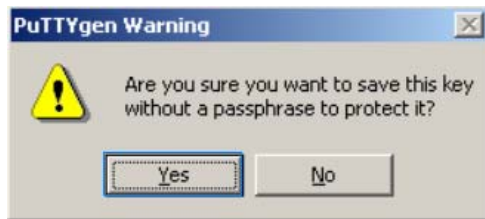
After the key pair is generated, click **Save public key** and enter the name of the file for saving the public key (**public** in this case).

Figure 1-25 Generate a client key pair (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 protection. Click **Yes** and enter the name of the file for saving the private key (**private.ppk** in this case).

Figure 1-26 Generate a client key pair (4)



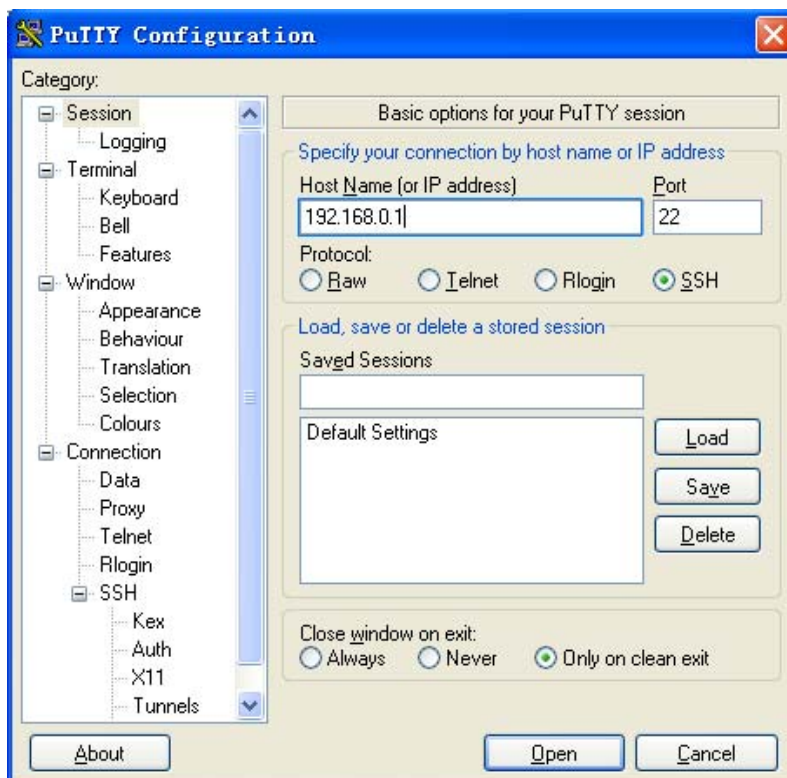
 Note

After a public key pair is generated, you need to upload the public key file to the server through FTP or TFTP, and complete the server end configuration before you continue to configure the client.

Establish a connection with the SSH server

2) Launch PuTTY.exe to enter the following interface.

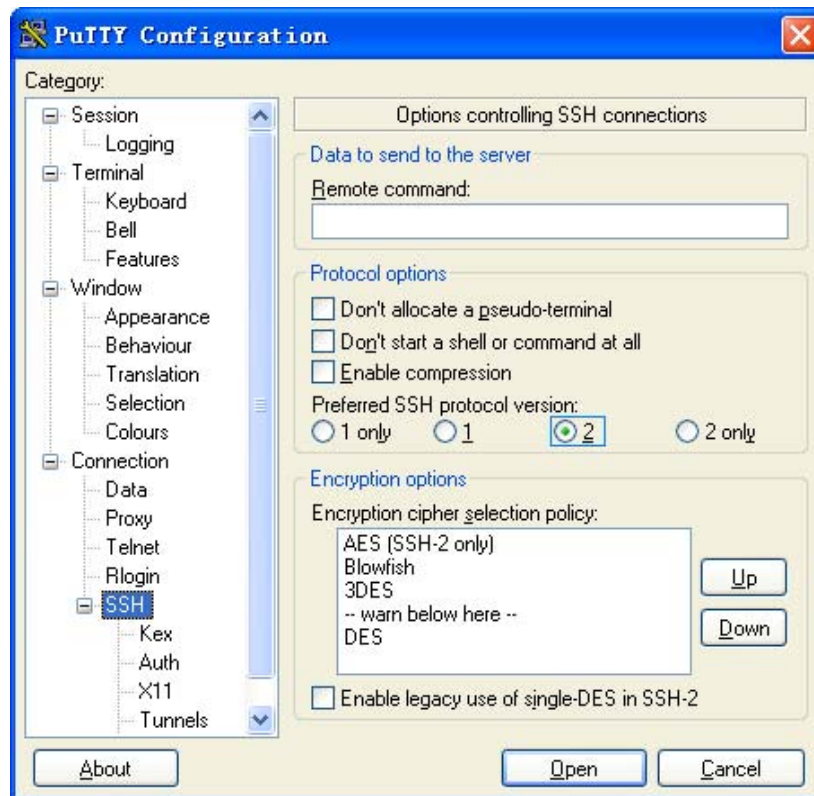
Figure 1-27 SSH client configuration interface (1)



In the **Host Name (or IP address)** text box, enter the IP address of the server.

3) From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in [Figure 1-28](#) appears.

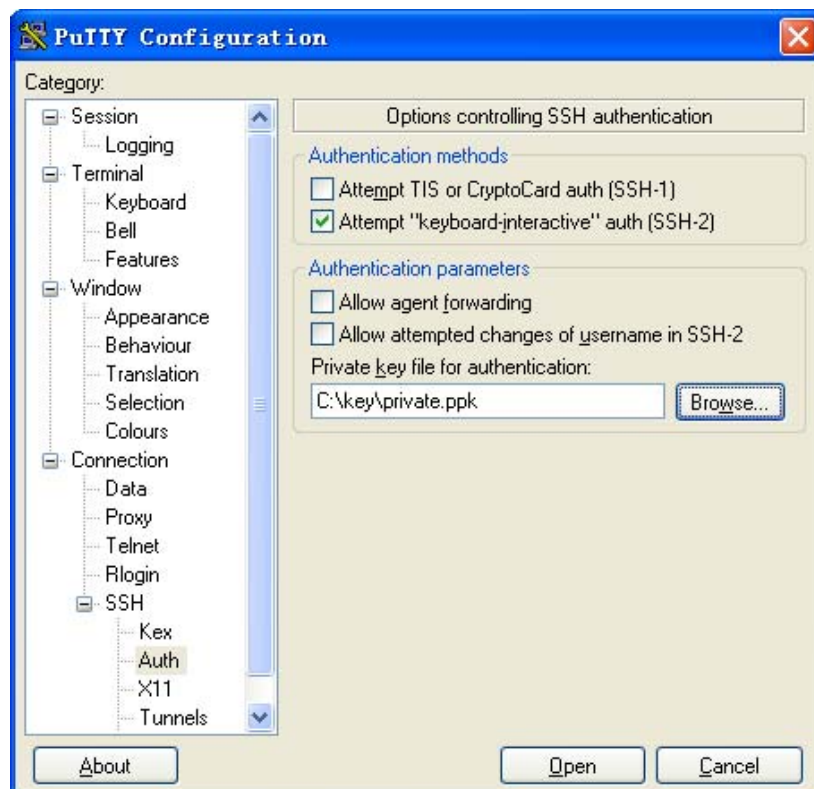
Figure 1-28 SSH client configuration interface (2)



Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

4) Select **Connection/SSH/Auth**. The following window appears.

Figure 1-29 SSH client configuration interface (3)



Click **Browse** to bring up the file selection window, navigate to the private key file and click **OK**.

- 5) From the window shown in [Figure 1-29](#), click **Open**. If the connection is normal, you will be prompted to enter the username.

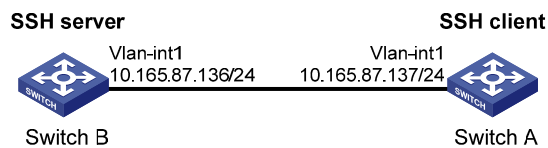
When Switch Acts as Client for Password Authentication

Network requirements

As shown in [Figure 1-30](#), establish an SSH connection between Switch A (SSH Client) and Switch B (SSH Server) for secure data exchange. The user name for login is client001 and the SSH server's IP address is 10.165.87.136. Password authentication is required.

Network diagram

Figure 1-30 Switch acts as client for password authentication



Configuration procedure

- Configure Switch B

Create a VLAN interface on the switch and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```



Note

Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

Generate RSA and DSA key pairs.

```
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
```

Set the authentication mode for the user interfaces to AAA.

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[SwitchB-ui-vty0-4] protocol inbound ssh
[SwitchB-ui-vty0-4] quit
```

Create local user **client001**, and set the authentication password to **abc**, the login protocol to SSH, and user command privilege level to 3.

```
[SwitchB] local-user client001
[SwitchB-luser-client001] password simple abc
[SwitchB-luser-client001] service-type ssh level 3
[SwitchB-luser-client001] quit
```

Configure the authentication type of user client001 as password.

```
[SwitchB] ssh user client001 authentication-type password
```

- Configure Switch A

Create a VLAN interface on the switch and assign an IP address, which serves as the SSH client's address in an SSH connection.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Establish a connection to the server 10.165.87.136.

```
[SwitchA] 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:
```

After you enter the correct password, you can log into Router B successfully.

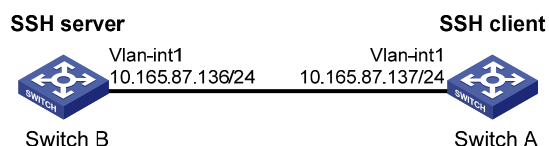
When Switch Acts as Client for Publickey Authentication

Network requirements

As shown in [Figure 1-31](#), establish an SSH connection between Switch A (SSH Client) and Switch B (SSH Server) for secure data exchange. The user name is client001 and the SSH server's IP address is 10.165.87.136. Publickey authentication is required.

Network diagram

Figure 1-31 Switch acts as client for publickey authentication



Configuration procedure

**Note**

In public key authentication, you can use either RSA or DSA public key. Here takes the DSA public key as an example.

- Configure Switch B

Create a VLAN interface on the switch and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

**Note**

Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

Generate RSA and DSA key pairs.

```
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
```

Set the authentication mode for the user interfaces to AAA.

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[SwitchB-ui-vty0-4] protocol inbound ssh
```

Set the user command privilege level to 3.

```
[SwitchB-ui-vty0-4] user privilege level 3
[SwitchB-ui-vty0-4] quit
```

Specify the authentication type of user client001 as publickey.

```
[SwitchB] ssh user client001 authentication-type publickey
```

**Note**

Before doing the following steps, you must first generate a DSA public key pair on the client and save the key pair in a file named Switch001, and then upload the file to the SSH server through FTP or TFTP. For details, refer to “Configure Switch A”.

Import the client public key pair named Switch001 from the file Switch001.

```
[SwitchB] public-key peer Switch001 import sshkey Switch001
```


Assign the public key Switch001 to user client001.

```
[SwitchB] ssh user client001 assign publickey Switch001
```

- Configure Switch A

Create a VLAN interface on the switch and assign an IP address, which serves as the SSH client's address in an SSH connection.

```
<SwitchA> system-view
```

```
[SwitchA] interface vlan-interface 1
```

```
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
```

```
[SwitchA-Vlan-interface1] quit
```

Generate a DSA key pair

```
[SwitchA] public-key local create dsa
```

Export the generated DSA key pair to a file named Switch001.

```
[SwitchA] public-key local export dsa ssh2 Switch001
```



Note

After the key pair is generated, you need to upload the public key file to the server through FTP or TFTP and complete the server end configuration before you continue to configure the client.

Establish an SSH connection to the server 10.165.87.136.

```
[SwitchA] ssh2 10.165.87.136 identity-key dsa
```

```
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
```

Later, you will find that you have logged into Switch B successfully.

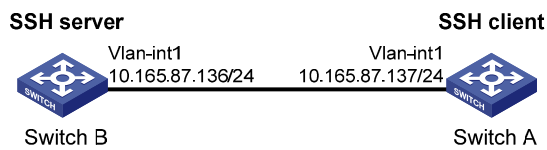
When Switch Acts as Client and First-Time Authentication is not Supported

Network requirements

As shown in [Figure 1-32](#), establish an SSH connection between Switch A (SSH Client) and Switch B (SSH Server) for secure data exchange. The user name is client001 and the SSH server's IP address is 10.165.87.136. The **publickey** authentication mode is used to enhance security.

Network diagram

Figure 1-32 Switch acts as client and first-time authentication is not supported



Configuration procedure

- Configure Switch B

Create a VLAN interface on the switch and assign an IP address for it to serve as the destination of the client.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```



Note

Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

Generate RSA and DSA key pairs.

```
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
      # Set AAA authentication on user interfaces.
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

Configure the user interfaces to support SSH.

```
[SwitchB-ui-vty0-4] protocol inbound ssh
# Set the user command privilege level to 3.
[SwitchB-ui-vty0-4] user privilege level 3
[SwitchB-ui-vty0-4] quit
```

Specify the authentication type for user client001 as publickey.

```
[SwitchB] ssh user client001 authentication-type publickey
```



Note

Before doing the following steps, you must first generate a DSA key pair on the client and save the key pair in a file named Switch001, and then upload the file to the SSH server through FTP or TFTP. For details, refer to the following “Configure Switch A”.

Import the client's public key file Switch001 and name the public key as Switch001.

```
[SwitchB] public-key peer Switch001 import sshkey Switch001
```

Assign public key Switch001 to user client001

```
[SwitchB] ssh user client001 assign publickey Switch001
```

Export the generated DSA host public key pair to a file named Switch002.

```
[SwitchB] public-key local export dsa ssh2 Switch002
```



When first-time authentication is not supported, you must first generate a DSA key pair on the server and save the key pair in a file named Switch002, and then upload the file to the SSH client through FTP or TFTP.

- Configure Switch A

Create a VLAN interface on the switch and assign an IP address, which serves as the SSH client's address in an SSH connection.

```
<SwitchA> system-view
```

```
[SwitchA] interface vlan-interface 1
```

```
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
```

```
[SwitchA-Vlan-interface1] quit
```

Generate a DSA key pair

```
[SwitchA] public-key local create dsa
```

Export the generated DSA key pair to a file named Switch001.

```
[SwitchA] public-key local export dsa ssh2 Switch001
```



After generating the key pair, you need to upload the key pair file to the server through FTP or TFTP and complete the server end configuration before you continue to configure the client.

Disable first-time authentication on the device.

```
[SwitchA] undo ssh client first-time
```



Note

When first-time authentication is not supported, you must first generate a DSA key pair on the server and save the key pair in a file named Switch002, and then upload the file to the SSH client through FTP or TFTP. For details, refer to the above part “Configure Switch B”.

Import the public key pair named Switch002 from the file Switch002.

```
[SwitchA] public-key peer Switch002 import sshkey Switch002
```

Specify the host public key pair name of the server.

```
[SwitchA] ssh client 10.165.87.136 assign publickey Switch002
```

Establish the SSH connection to server 10.165.87.136.

```
[SwitchA] ssh2 10.165.87.136 identity-key dsa
```

```
Username: client001
```

```
Trying 10.165.87.136 ...
```

```
Press CTRL+K to abort
```

```
Connected to 10.165.87.136 ...
```

Later, you will find that you have logged into Switch B successfully.

Table of Contents

1 File System Management Configuration	1-1
File System Configuration	1-1
Introduction to File System	1-1
File System Configuration Task List	1-1
Directory Operations	1-2
File Operations	1-3
Flash Memory Operations	1-4
Prompt Mode Configuration	1-4
File System Configuration Examples	1-5
File Attribute Configuration	1-6
Introduction to File Attributes	1-6
Bootting with the Startup File	1-7
Configuring File Attributes	1-7
Configuration File Backup and Restoration	1-8
Introduction to Configuration File Backup and Restoration	1-8
File Backup and Restoration	1-9

1 File System Management Configuration



Note

For information on the modification of the order for the device to select Web file when the device boots, refer to [Bootling with the Startup File](#).

When configuring file system management, go to these sections for information you are interested in:

- [File System Configuration](#)
- [File Attribute Configuration](#)
- [Configuration File Backup and Restoration](#)

File System Configuration

Introduction to File System

To facilitate management on the switch memory, S3600 series Ethernet switches provide the file system function, allowing you to access and manage the files and directories. You can create, remove, copy or delete a file through command lines, and you can manage files using directories.

File System Configuration Task List

Complete the following tasks to configure the file system:

Task	Remarks
Directory Operations	Optional
File Operations	Optional
Flash Memory Operations	Optional
Prompt Mode Configuration	Optional



Note

The S3600 series Ethernet switches support Intelligent Resilient Framework (IRF), and allow you to access a file on a switch in one of the following ways:

- To access a file on the specified unit, you need to specify the file in universal resource locator (URL) format and starting with **unit[No.]>flash:/**, where **[No.]** represents the unit ID of the switch. For example, if the unit ID of the switch is 1, the URL of a file named **text.txt** in the root directory of the switch is **unit1>flash:/text.txt**.
- To access a file on the current unit, you need to enter the file URL starting with **flash:/**. For example, the URL of file **text.txt** in the root directory of the Flash on the current unit is **flash:/text.txt**.
- To access a file in the current directory, enter the path name or file name directly. For example, to access file **text.txt** in the current directory, you can directly input the file name **text.txt** as the file URL.

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

Follow these steps to perform directory-related operations:

To do...	Use the command...	Remarks
Create a directory	mkdir <i>directory</i>	Optional Available in user view
Delete a directory	rmdir <i>directory</i>	Optional Available in user view
Display the current work directory	pwd	Optional Available in user view
Display the information about specific directories and files	dir [<i>/all</i>] [<i>/fabric</i> <i>file-url</i>]	Optional Available in user view
Enter a specified directory	cd <i>directory</i>	Optional Available in user view



Note

- Only empty directories can be deleted by using the **rmdir** command.
- In the output information of the **dir /all** command, deleted files (that is, those stored in the recycle bin) are embraced in brackets.

File Operations

Follow these steps to perform file-related operations:

To do...	Use the command...	Remarks
Delete a file	delete [/unreserved] <i>file-url</i> delete { running-files standby-files } [/fabric] [/unreserved]	Optional A deleted file can be restored by using the undelete command if you delete it by executing the delete command without specifying the /unreserved keyword. Available in user view
Restore a file in the recycle bin	undelete <i>file-url</i>	Optional Available in user view
Delete a file from the recycle bin	reset recycle-bin [<i>file-url</i>] [/force] reset recycle-bin [/fabric]	Optional Available in user view
Upgrade the software of the whole fabric	update fabric <i>file-name</i>	Optional Available in user view
Rename a file	rename <i>fileurl-source</i> <i>fileurl-dest</i>	Optional Available in user view
Copy a file	copy <i>fileurl-source</i> <i>fileurl-dest</i>	Optional Available in user view
Move a file	move <i>fileurl-source</i> <i>fileurl-dest</i>	Optional Available in user view
Display the content of a file	more <i>file-url</i>	Optional Available in user view Currently, the file system only supports displaying the contents of text files.
Display the information about a directory or a file	dir [/all] [/fabric <i>file-url</i>]	Optional Available in user view
Enter system view	system-view	—
Execute the specified batch file	execute <i>filename</i>	Optional Available 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 null configuration when it starts up next time.
-

Flash Memory Operations

Follow these steps to perform Flash memory operations:

To do...	Use the command...	Remarks
Format the Flash memory	format <i>device</i>	Required Available in user view
Restore space on the Flash memory	fixdisk <i>device</i>	Required Available in user view



Caution

The format operation leads to the loss of all files, including the configuration files, on the Flash memory and is irretrievable.

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.

Follow these steps to set the 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 .

File System Configuration Examples

Display all the files in the root directory of the file system on the local unit.

```
<Sysname> dir /all
```

```
Directory of unit1>flash:/
```

```

 1 (*)  -rw-   5822215  Jan 01 1970 00:07:03  test.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  testv1r1.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.

```
<Sysname> 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.

```
<Sysname> dir /all
```

```
Directory of unit1>flash:/
```

```

 1 (*)  -rw-   5822215  Jan 01 1970 00:07:03  test.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  testv1r1.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

<Sysname> 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

File Attribute Configuration

Introduction to File Attributes

The following three startup files support file attribute configuration:

- App files: An app file is an executable file, with .bin as the extension.
- Configuration files: A configuration file is used to store and restore configuration, with .cfg as the extension.
- Web files: A Web file is used for Web-based network management, with .web as the extension.

The app files, configuration files, and Web files support 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 preferred 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.

Note that, there can be only one app file, one configuration file and one Web file with the main attribute in the Flash memory. 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 lose its main attribute. 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 valid file with the same name as the deleted file to the flash memory, the file will possess the main attribute.

After the Boot ROM of a switch is upgraded, the original default app file has the main attribute.

Booting with the Startup File

The device selects the main startup file as the preferred startup file. If the device fails to boot with the main startup file, it boots with the backup startup file.

For the Web file and configuration file, Hangzhou H3C Technologies Co., Ltd (referred to as H3C hereinafter) may provide corresponding default file when releasing software versions. When booting, the device selects the startup files based on certain order. The device selects Web files in the following steps:

- 1) If the default Web file exists, the device will boot with the default Web file;
- 2) If the default Web file does not exist, but the main Web file exists, the device will boot with the main Web file;
- 3) If neither the default Web file nor the main Web file exists, but the backup Web exists, the device will boot with the backup Web file;
- 4) If neither of the default Web file, main Web file and backup Web exists, the device considers that no Web file exists.

For the selection of the configuration file when the device boots, refer to the *Configuration File Management* part in this manual.

Configuring File Attributes

You can configure and view the main attribute or backup attribute of the file used for the next startup of a switch, and change the main or backup attribute of the file.

Follow these steps to configure file attributes:

To do...	Use the command...	Remarks
Configure the app file with the main attribute for the next startup	boot boot-loader <i>file-url</i> [fabric]	Optional Available in user view
Configure the app file with the backup attribute for the next startup	boot boot-loader backup-attribute <i>file-url</i> [fabric]	Optional Available in user view

To do...	Use the command...	Remarks
Configure the Web file and its attribute	boot web-package <i>webfile</i> { backup main }	Optional Available in user view
Switch the file attributes between main and backup	boot attribute-switch { all app configuration web } fabric	Optional Available in user view
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. Available in user view
Display the information about the app file used as the startup file	display boot-loader [<i>unit unit-id</i>]	Optional Available in any view
Display information about the Web file used by the device	display web package	



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 or specify a new Web file by using the **boot web-package** command. Otherwise, Web server cannot function normally.
- Currently, a configuration file has the extension of *cfg* and resides in the root directory of the Flash memory.
- For the detailed configuration of configuration file attributes, refer to the *Configuration File Management* module in this manual.

Configuration File Backup and Restoration

Introduction to 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 file 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 form the startup configuration of the whole fabric.

File Backup and Restoration

Configuration prerequisites

Before performing the following operations, you must first ensure that:

- The relevant units support TFTP client.
- The TFTP server is started
- A route exists between the TFTP server and TFTP client.

Configuration procedure

Follow these steps to back up and restore configuration file:

To do...	Use the command...	Remarks
Back up the current configuration of a specified unit	backup unit <i>unit-id</i> current-configuration to { <i>dest-addr</i> <i>dest-hostname</i> } <i>filename.cfg</i>	Optional Available in user view
Back up the current configuration of the whole fabric system	backup fabric current-configuration to { <i>dest-addr</i> <i>dest-hostname</i> } <i>filename.cfg</i>	Optional Available in user view
Restore the startup configuration of a specified unit	restore unit <i>unit-id</i> startup-configuration from { <i>source-addr</i> <i>source-hostname</i> } <i>filename.cfg</i>	Optional Available in user view
Restore the startup configuration of the whole fabric system	restore fabric startup-configuration from { <i>source-addr</i> <i>source-hostname</i> } <i>filename.cfg</i>	Optional Available in user view

Table of Contents

1 FTP and SFTP Configuration	1-1
Introduction to FTP and SFTP	1-1
Introduction to FTP	1-1
Introduction to SFTP	1-2
FTP Configuration	1-3
FTP Configuration: A Switch Operating as an FTP Server	1-3
FTP Configuration: A Switch Operating as an FTP Client	1-7
Configuration Example: A Switch Operating as an FTP Server	1-9
FTP Banner Display Configuration Example	1-11
FTP Configuration: A Switch Operating as an FTP Client	1-12
SFTP Configuration	1-14
SFTP Configuration: A Switch Operating as an SFTP Server	1-15
SFTP Configuration: A Switch Operating as an SFTP Client	1-16
SFTP Configuration Example	1-18
2 TFTP Configuration	2-1
Introduction to TFTP	2-1
TFTP Configuration	2-2
TFTP Configuration: A Switch Operating as a TFTP Client	2-2
TFTP Configuration Example	2-3

1 FTP and SFTP Configuration

When configuring FTP and SFTP, go to these sections for information you are interested in:

- [Introduction to FTP and SFTP](#)
- [FTP Configuration](#)
- [SFTP Configuration](#)



Note

FTP banner is newly added. For details, see section [Configuring the banner for an FTP server](#).

Introduction to FTP and SFTP

Introduction to FTP

File Transfer Protocol (FTP) 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 client. 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:

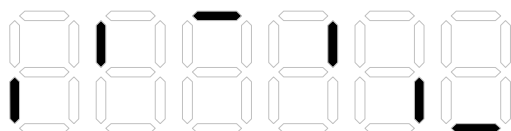
- Binary mode for program file transfer
- ASCII mode for text file transfer

An H3C S3600 series Ethernet switch can act as an FTP client or the FTP server in FTP-employed data transmission:

Table 1-1 Roles that an H3C S3600 series Ethernet switch acts as in FTP

Item	Description	Remarks
FTP server	An Ethernet switch can operate as an FTP server to provide file transmission services for FTP clients. You can log in to a switch operating as an FTP server by running an FTP client program on your PC to access files on the FTP server.	The prerequisite is that a route exists between the switch and the PC.
FTP client	In this case, you need to establish a connection between your PC and the switch through a terminal emulation program or Telnet, execute the ftp X.X.X.X command on your PC. (X.X.X.X is the IP address of an FTP server or a host name), and enter your user name and password in turn. A switch can operate as an FTP client, through which you can access files on the FTP server.	

- With an S3600 series Ethernet switch serving as an FTP server, the seven-segment digital LED on the front panel of the switch rotates clockwise when an FTP client is uploading files to the FTP server (the S3600 switch), and stops rotating when the file uploading is finished, as shown in [Figure 1-1](#).
- With an S3600 series Ethernet switch serving as an FTP client, the seven-segment digital LED on the front panel of the switch rotates clockwise when the FTP client (the S3600 switch) is downloading files from an FTP server, and stops rotating when the file downloading is finished, as shown in [Figure 1-1](#).

Figure 1-1 Clockwise rotating of the seven-segment digital LED

Introduction to SFTP

Secure FTP (SFTP) is established based on an SSH2 connection. It allows a remote user to log in to a switch to manage and transmit files, providing a securer guarantee for data transmission. In addition, since the switch can be used as a client, you can log in to remote devices to transfer files securely.

FTP Configuration

Complete the following tasks to configure FTP:

Task		Remarks
FTP Configuration: A Switch Operating as an FTP Server	Creating an FTP user	Required
	Enabling an FTP server	Required
	Configuring connection idle time	Optional
	Specifying the source interface and source IP address for an FTP server	Optional
	Disconnecting a specified user	Optional
	Configuring the banner for an FTP server	Optional
	Displaying FTP server information	Optional
FTP Configuration: A Switch Operating as an FTP Client	Basic configurations on an FTP client	—
	Specifying the source interface and source IP address for an FTP client	Optional

FTP Configuration: A Switch Operating as an FTP Server

Creating an FTP user

Configure the user name and password for the FTP user and set the service type to FTP. To use FTP services, a user must provide a user name and password for being authenticated by the FTP server. Only users that pass the authentication have access to the FTP server.

Follow these steps to create an FTP user:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Add a local user and enter local user view	local-user <i>user-name</i>	Required By default, no local user is configured.
Configure a password for the specified user	password { simple cipher } <i>password</i>	Optional By default, no password is configured.
Configure the service type as FTP	service-type ftp	Required By default, no service is configured.

Enabling an FTP server

Follow these steps to enable an FTP server:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the FTP server function	ftp server enable	Required Disabled by default.



Note

- Only one user can access an H3C S3600 series Ethernet switch at a given time when the latter operates as an FTP server.
- Operating as an FTP server, an H3C S3600 series 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.
- You cannot access an H3C S3600 series switch operating as an FTP server through Microsoft Internet Explorer. To do so, use other client software.



Note

To protect unused sockets against 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.

Configuring connection idle time

After the idle time is configured, if the server does not receive service requests from a client within a specified time period, it terminates the connection with the client, thus preventing a user from occupying the connection for a long time without performing any operation.

Follow these steps to configure connection idle time:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the connection idle time for the FTP server	ftp timeout <i>minutes</i>	Optional 30 minutes by default

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.

Follow these steps to specify the source interface and source IP address for an FTP server:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify the source interface for an FTP server	ftp-server source-interface <i>interface-type interface-number</i>	Use either command Not specified by default.
Specifying the source IP address for an FTP server	ftp-server source-ip <i>ip-address</i>	



Note

- The specified interface must be an existing one. Otherwise a prompt appears to show that the configuration fails.
- The value of the *ip-address* argument must be an IP address on the device where the configuration is performed. Otherwise a prompt appears to show that the configuration fails.
- You can 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.
- If the switch (FTP server) is the command switch or member switch in a cluster, do not use the **ftp-server source-ip** command to specify the private IP address of the cluster as the source IP address of the FTP server. Otherwise, FTP does not take effect.

Disconnecting a specified user

On the FTP server, you can disconnect a specified user from the FTP server to secure the network.

Follow these steps to disconnect a specified user:

To do...	Use the command...	Remarks
Enter system view	system-view	—
On the FTP server, disconnect a specified user from the FTP server	ftp disconnect <i>user-name</i>	Required



Note

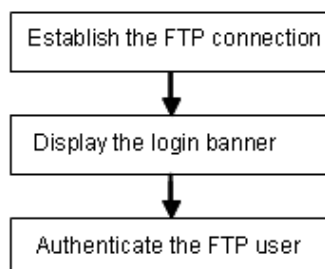
With an H3C S3600 series Ethernet switch acting as the FTP server, if a network administrator attempts to disconnect a user that is uploading/downloading data to/from the FTP server the S3600 Ethernet switch will disconnect the user after the data transmission is completed.

Configuring the banner for an FTP server

Displaying a banner: With a banner configured on the FTP server, when you access the FTP server through FTP, the configured banner is displayed on the FTP client. Banner falls into the following two types:

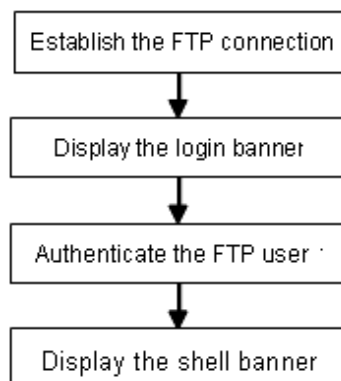
- Login banner: After the connection between an FTP client and an FTP server is established, the FTP server outputs the configured login banner to the FTP client terminal.

Figure 1-2 Process of displaying a login banner



- Shell banner: After the connection between an FTP client and an FTP server is established and correct user name and password are provided, the FTP server outputs the configured shell banner to the FTP client terminal.

Figure 1-3 Process of displaying a shell banner



Follow these steps to configure the banner display for an FTP server:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a login banner	header login text	Required Use either command or both. By default, no banner is configured.
Configure a shell banner	header shell text	



Note

For details about the **header** command, refer to the Login part of the manual.

Displaying FTP server information

To do...	Use the command...	Remarks
Display the information about FTP server configurations on a switch	display ftp-server	Available 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	

FTP Configuration: A Switch Operating as an FTP Client

Basic configurations on an FTP client

By default a switch can operate as an FTP client. In this case, you can connect the switch to the FTP server to perform FTP-related operations (such as creating/removing a directory) by executing commands on the switch.

Follow these steps to perform basic configurations on an FTP client:

To do...	Use the command...	Remarks
Enter FTP client view	ftp [cluster remote-server [port-number]]	—
Specify to transfer files in ASCII characters	ascii	Use either command. By default, files are transferred in ASCII characters.
Specify to transfer files in binary streams	binary	
Set the data transfer mode to passive	passive	Optional passive by default.

To do...	Use the command...	Remarks
Change the working directory on the remote FTP server	cd <i>pathname</i>	Optional
Change the working directory to be the parent directory	cdup	
Get the local working path on the FTP client	lcd	
Display the working directory on the FTP server	pwd	
Create a directory on the remote FTP server	mkdir <i>pathname</i>	
Remove a directory on the remote FTP server	rmdir <i>pathname</i>	
Delete a specified file	delete <i>remotefile</i>	
Query a specified file on the FTP server	dir [<i>remotefile</i>] [<i>localfile</i>]	Optional
	ls [<i>remotefile</i>] [<i>localfile</i>]	If no file name is specified, all the files in the current directory are displayed. The difference between these two commands is that the dir command can display the file name, directory as well as file attributes; while the ls command can display only the file name and directory.
Download a remote file from the FTP server	get <i>remotefile</i> [<i>localfile</i>]	Optional
Upload a local file to the remote FTP server	put <i>localfile</i> [<i>remotefile</i>]	
Rename a file on the remote server	rename <i>remote-source</i> <i>remote-dest</i>	
Log in with the specified user name and password	user <i>username</i> [<i>password</i>]	
Connect to a remote FTP server	open { <i>ip-address</i> <i>server-name</i> } [<i>port</i>]	
Terminate the current FTP connection without exiting FTP client view	disconnect	
	close	
Terminate the current FTP connection and return to user view	quit	
	bye	
Display the online help about a specified command concerning FTP	remotehelp [<i>protocol-command</i>]	
Enable the verbose function	verbose	Optional Enabled by default.

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.

Follow these steps to specify the source interface and source IP address for an FTP client:

To do...	Use the command...	Remarks
Specify the source interface used for the current connection	ftp { cluster remote-server } source-interface <i>interface-type interface-number</i>	Optional
Specify the source IP address used for the current connection	ftp { cluster remote-server } source-ip ip-address	Optional
Enter system view	system-view	—
Specify an interface as the source interface the FTP client uses every time it connects to an FTP server	ftp source-interface <i>interface-type interface-number</i>	Use either command Not specified by default
Specify an IP address as the source IP address the FTP client uses every time it connects to an FTP server	ftp source-ip ip-address	
Display the source IP address used by an FTP client every time it connects to an FTP server	display ftp source-ip	Available in any view



Note

- The specified interface must be an existing one. Otherwise a prompt appears to show that the configuration fails.
- The value of the *ip-address* argument must be the IP address of the device where the configuration is performed. Otherwise a prompt appears to show that 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 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 valid at one time. If you execute both of them, the new setting will overwrite the original one.

Configuration Example: A Switch Operating as an FTP Server

Network requirements

A switch operates as an FTP server and a remote PC as an FTP client. The application **switch.bin** of the switch is stored on the PC. Upload the application to the remote switch through FTP and use the **boot boot-loader** command to specify **switch.bin** as the application for next startup. Reboot the switch

to upgrade the switch application and download the configuration file **config.cfg** from the switch, thus to back up the configuration file.

- Create a user account on the FTP server with the username **switch** and password **hello**.
- The IP addresses 1.1.1.1 for a VLAN interface on the switch and 2.2.2.2 for the PC have been configured. Ensure that a route exists between the switch and the PC.

Network diagram

Figure 1-4 Network diagram for FTP configurations: a switch operating as an FTP server



Configuration procedure

1) Configure Switch A (the FTP server)

Log in to the switch and enable the FTP server function on the switch. Configure the user name and password used to access FTP services, and specify the service type as FTP (You can log in to a switch through the Console port or by telnetting the switch. See the *Login* module for detailed information.)

Configure the FTP username as **switch**, the password as **hello**, and the service type as FTP.

```
<Sysname>
<Sysname> system-view
[Sysname] ftp server enable
[Sysname] local-user switch
[Sysname-luser-switch] password simple hello
[Sysname-luser-switch] service-type ftp
```

2) Configure the PC (FTP client)

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 username **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 file **switch.bin**.

```
ftp> put switch.bin
200 Port command okay.
150 Opening ASCII mode data connection for switch.bin.
226 Transfer complete.
ftp: 75980 bytes received in 5.55 seconds 13.70Kbytes/sec.
```

Download file **config.cfg**.

```
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 in to 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 not in use from the Flash memory to make room for the file, and then upload the file again. The files in use cannot be deleted. If you have to delete the files in use to make room for the file to be uploaded, you can only delete/download them through the Boot ROM menu.
- H3C series switch is not shipped with FTP client application software. You need to purchase and install it by yourself.

3) Configure Switch A (FTP server)

After uploading the application, 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.

```
<Sysname> boot boot-loader switch.bin
<Sysname> 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 part of this manual.

FTP Banner Display Configuration Example

Network requirements

Configure the Ethernet switch as an FTP server and the remote PC as an FTP client. After a connection between the FTP client and the FTP server is established and login succeeds, the banner is displayed

on the FTP client.

- An FTP user with username **switch** and the password **hello** has been configured on the FTP server.
- The IP addresses 1.1.1.1 for a VLAN interface on the switch and 2.2.2.2 for the PC have been configured. Ensure that a route exists between the switch and the PC.
- Configure the login banner of the switch as “login banner appears” and the shell banner as “shell banner appears”.

Network diagram

Figure 1-5 Network diagram for FTP banner display configuration



Configuration procedure

- 1) Configure the switch (FTP server)

Configure the login banner of the switch as “login banner appears” and the shell banner as “shell banner appears”. For detailed configuration of other network requirements, see section [Configuration Example: A Switch Operating as an FTP Server](#).

```
<Sysname> system-view
[Sysname] header login %login banner appears%
[Sysname] header shell %shell banner appears%
```

- 2) Configure the PC (FTP client)

Access the Ethernet switch through FTP. Enter the username **switch** and the password **hello** to log in to the switch, and then enter FTP view. Login banner appears after FTP connection is established. Shell banner appears after the user passes the authentication.

```
C:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220-login banner appears
220 FTP service ready.
User (1.1.1.1:(none)): switch
331 Password required for switch.
Password:
230-shell banner appears
230 User logged in.
ftp>
```

FTP Configuration: A Switch Operating as an FTP Client

Network requirements

A switch operates as an FTP client and a remote PC as an FTP server. The switch application named **switch.bin** is stored on the PC. Download it to the switch through FTP and use the **boot boot-loader** command to specify **switch.bin** as the application for next startup. Reboot the switch to upgrade the

switch application, and then upload the switch configuration file named **config.cfg** to directory **switch** of the PC to back up the configuration file.

- Create a user account on the FTP server with the username **switch** and password **hello**, and grant the user **switch** read and write permissions for the directory **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 a route exists between the switch and the PC.

Network diagram

Figure 1-6 Network diagram for FTP configurations: a switch operating as an FTP client



Configuration procedure

1) Configure the PC (FTP server)

Perform FTP server-related configurations on the PC, that is, create a user account on the FTP server with username **switch** and password **hello**. (For detailed configuration, refer to the configuration instruction relevant to the FTP server software.)

2) Configure the switch (FTP client)

Log in to the switch. (You can log in to a switch through the Console port or by telnetting the switch. See the *Login* module for detailed information.)

<Sysname>



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 not in use from the Flash memory to make room for the file, and then upload the file again. The files in use cannot be deleted. If you have to delete the files in use to make room for the file to be uploaded, you can only delete/download them through the Boot ROM menu.

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 to enter FTP view.

<Sysname> ftp 2.2.2.2

Trying ...

Press CTRL+K to abort

Connected.

220 FTP service ready.

User(none):admin

331 Password required for admin.

Password:

230 User logged in.

```

[ftp]

# Enter the authorized directory on the FTP server.

[ftp] cd switch

# Execute the put command to upload the configuration file named config.cfg to the FTP server.

[ftp] put config.cfg

# Execute the get command to download the file named switch.bin to the Flash memory of the switch.

[ftp] get switch.bin

# Execute the quit command to terminate the FTP connection and return to user view.

[ftp] quit
<Sysname>

# After downloading the file, use the boot boot-loader command to specify the downloaded file
(switch.bin) to be the application for next startup, and then restart the switch. Thus the switch
application is upgraded.

<Sysname> boot boot-loader switch.bin
<Sysname> 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.

SFTP Configuration

Complete the following tasks to configure SFTP:

Task		Remarks
SFTP Configuration: A Switch Operating as an SFTP Server	Enabling an SFTP server	Required
	Configuring connection idle time	Optional
	Supported SFTP client software	—
SFTP Configuration: A Switch Operating as an SFTP Client	Basic configurations on an SFTP client	—
	Specifying the source interface or source IP address for an SFTP client	Optional

SFTP Configuration: A Switch Operating as an SFTP Server

Enabling an SFTP server

Before enabling an SFTP server, you need to enable the SSH server function and specify the service type of the SSH user as **SFTP** or **all**. For details, see the SSH server configuration part of *SSH Operation Manual* of this manual.

Follow these steps to enable an SFTP server:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable an SFTP server	sftp server enable	Required Disabled by default.

Configuring connection idle time

After the idle time is configured, if the server does not receive service requests from a client within a specified time period, it terminates the connection with the client, thus preventing a user from occupying the connection for a long time without performing any operation.

Follow these steps to configure connection idle time:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the connection idle time for the SFTP server	ftp timeout <i>time-out-value</i>	Optional 10 minutes by default.

Supported SFTP client software

An H3C S3600 series Ethernet switch operating as an SFTP server can interoperate with SFTP client software, including SSH Tectia Client v4.2.0 (SFTP), v5.0, and WINSCP.

SFTP client software supports the following operations: logging in to a device; uploading a file; downloading a file; creating a directory; modify a file name or a directory name; browsing directory structure; and manually terminating a connection.

For configurations on client software, see the corresponding configuration manual.



Note

- Currently an H3C S3600 series Ethernet switch operating as an SFTP server supports the connection of only one SFTP user. When multiple users attempt to log in to the SFTP server or multiple connections are enabled on a client, only the first user can log in to the SFTP user. The subsequent connection will fail.
- When you upload a large file through WINSCP, if a file with the same name exists on the server, you are recommended to set the packet timeout time to over 600 seconds, thus to prevent the client from failing to respond to device packets due to timeout. Similarly, when you delete a large file from the server, you are recommended to set the client packet timeout time to over 600 seconds.

SFTP Configuration: A Switch Operating as an SFTP Client

Basic configurations on an SFTP client

By default a switch can operate as an SFTP client. In this case you can connect the switch to the SFTP server to perform SFTP-related operations (such as creating/removing a directory) by executing commands on the switch.

Follow these steps to perform basic configurations on an SFTP client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter SFTP client view	sftp { host-ip host-name } [port-num] [identity-key { dsa rsa } prefer_kex { dh_group1 dh_exchange_group } prefer_ctos_cipher { 3des des aes128 } prefer_stoc_cipher { 3des des aes128 } prefer_ctos_hmac { sha1 sha1_96 md5 md5_96 } prefer_stoc_hmac { sha1 sha1_96 md5 md5_96 } } *	Required
Change the working directory on the remote SFTP server	cd pathname	Optional
Change the working directory to be the parent directory	cdup	
Display the working directory on the SFTP server	pwd	
Create a directory on the remote SFTP server	mkdir pathname	
Remove a directory on the remote SFTP server	rmdir pathname	
Delete a specified file	delete remotefile	Optional
	remove remote-file	Both commands have the same effect.

To do...	Use the command...	Remarks
Query a specified file on the SFTP server	dir [-a -l] [<i>remote-path</i>]	Optional
	ls [-a -l] [<i>remote-path</i>]	If no file name is provided, all the files in the current directory are displayed. The difference between these two commands is that the dir command can display the file name, directory as well as file attributes; while the ls command can display only the file name and directory.
Download a remote file from the SFTP server	get <i>remotefile</i> [<i>localfile</i>]	Optional
Upload a local file to the remote SFTP server	put <i>localfile</i> [<i>remotefile</i>]	
Rename a file on the remote server	rename <i>remote-source</i> <i>remote-dest</i>	
Exit SFTP client view and return to system view	bye	The three commands have the same effect.
	exit	
	quit	
Display the online help about a specified command concerning SFTP	help [all <i>command-name</i>]	Optional



Note

If you specify to authenticate a client through public key on the server, the client needs to read the local private key when logging in to the SFTP server. Since both RSA and DSA are available for public key authentication, you need to use the **identity-key** key word to specify the algorithms to get correct local private key; otherwise you will fail to log in. For details, see *SSH Operation Manual*.

Specifying the source interface or source IP address for an SFTP client

You can specify the source interface or source IP address for a switch acting as an FTP client, so that it can connect to a remote SFTP server.

Follow these steps to specify the source interface or source IP address for an SFTP client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify an interface as the source interface of the specified SFTP client	sftp source-interface <i>interface-type interface-number</i>	Use either command Not specified by default.
Specify an IP address as the source IP address of the specified SFTP client	sftp source-ip <i>ip-address</i>	

To do...	Use the command...	Remarks
Display the source IP address used by the current SFTP client	display sftp source-ip	Optional Available in any view

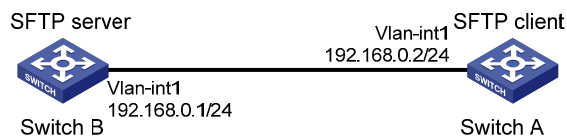
SFTP Configuration Example

Network requirements

As shown in [Figure 1-7](#), establish an SSH connection between the SFTP client (switch A) and the SFTP server (switch B). Log in to switch B through switch A to manage and transmit files. An SFTP user with the username **client001** and password **abc** exists on the SFTP server.

Network diagram

Figure 1-7 Network diagram for SFTP configuration



Configuration procedure

1) Configure the SFTP server (switch B)

Create key pairs.

```

<Sysname> system-view
[Sysname] public-key local create rsa
[Sysname] public-key local create dsa

```

Create a VLAN interface on the switch and assign to it an IP address, which is used as the destination address for the client to connect to the SFTP server.

```

[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[Sysname-Vlan-interface1] quit

```

Specify the SSH authentication mode as **AAA**.

```

[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode scheme

```

Configure the protocol through which the remote user logs in to the switch as SSH.

```

[Sysname-ui-vty0-4] protocol inbound ssh
[Sysname-ui-vty0-4] quit

```

Create a local user client001.

```

[Sysname] local-user client001
[Sysname-luser-client001] password simple abc
[Sysname-luser-client001] service-type ssh
[Sysname-luser-client001] quit

```

Configure the authentication mode as **password**. Authentication timeout time, retry number, and update time of the server key adopt the default values.

```
[Sysname] ssh user client001 authentication-type password
```

Specify the service type as SFTP.

```
[Sysname] ssh user client001 service-type sftp
```

Enable the SFTP server.

```
[Sysname] sftp server enable
```

2) Configure the SFTP client (switch A)

Configure the IP address of the VLAN interface on switch A. It must be in the same segment with the IP address of the VLAN interface on switch B. In this example, configure it as 192.168.0.2.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 1
```

```
[Sysname-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
```

```
[Sysname-Vlan-interface1] quit
```

Connect to the remote SFTP server. Enter the username **client001** and the password **abc**, and then enter SFTP client view.

```
[Sysname] 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 to 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 of the server. Delete the file **z** and verify the result.

```
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
```

```
Received status: End of file
```

```
Received status: Success
```

```
sftp-client> delete z
```

```
The following files will be deleted:
```

```
/z
```

```
Are you sure to delete it?(Y/N):y
```

```
This operation may take a long time.Please wait...
```

```
Received status: Success
```

```
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
Received status: End of file
Received status: Success
```

Add a directory **new1**, and then check whether the new directory is successfully created.

```
sftp-client> mkdir new1
Received status: Success
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
Received status: End of file
Received status: Success
```

Rename the directory **new1** as **new2**, and then verify the result.

```
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
Received status: End of file
Received status: Success
```

Download the file **pubkey2** from the server and rename it as **public**.

```
sftp-client> get pubkey2 public
This operation may take a long time, please wait...
.
Remote file:/pubkey2 ---> Local file: public..
Received status: End of file
Received status: Success
Downloading file successfully ended
```

Upload file **pu** to the server and rename it as **puk**, and then verify the result.

```
sftp-client> put pu puk
This operation may take a long time, please wait...
Local file: pu ---> Remote file: /puk
Received status: Success
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
```

Received status: End of file

Received status: Success

sftp-client>

Exit SFTP.

sftp-client> quit

Bye

[Sysname]

2 TFTP Configuration

When configuring TFTP, go to these sections for information you are interested in:

- [Introduction to TFTP](#)
- [TFTP Configuration](#)

Introduction to TFTP

Compared with FTP, Trivial File Transfer Protocol (TFTP) 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 RFC 1986.

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.

An H3C S3600 series Ethernet switch can act as a TFTP client only.

When an S3600 series Ethernet switch serving as a TFTP client downloads files from the TFTP server, the seven-segment digital LED on the front panel of the switch rotates clockwise, and it stops rotating when the file downloading is finished, as shown in [Figure 1-1](#).

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 file transfer.
- ASCII mode for text file transfer.



Note

Before performing TFTP-related configurations, you need to configure IP addresses for the TFTP client and the TFTP server, and make sure a route exists between the two.

TFTP Configuration

Complete the following tasks to configure TFTP:

Task		Remarks
TFTP Configuration: A Switch Operating as a TFTP Client	Basic configurations on a TFTP client	—
	Specifying the source interface or source IP address for an FTP client	Optional
TFTP server configuration	For details, see the corresponding manual	—

TFTP Configuration: A Switch Operating as a TFTP Client

Basic configurations on a TFTP client

By default a switch can operate as a TFTP client. In this case you can connect the switch to the TFTP server to perform TFTP-related operations (such as creating/removing a directory) by executing commands on the switch.

Follow these steps to perform basic configurations on a TFTP client:

To do...	Use the command...	Remarks
Download a file from a TFTP server	tftp tftp-server get source-file [dest-file]	Optional
Upload a file to a TFTP server	tftp tftp-server put source-file [dest-file]	Optional
Enter system view	system-view	—
Set the file transmission mode	tftp { ascii binary }	Optional Binary by default.
Specify an ACL rule used by the specified TFTP client to access a TFTP server	tftp-server acl acl-number	Optional Not specified by default.

Specifying the source interface or source IP address for an FTP 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.

Follow these steps to specify the source interface and source IP address for a TFTP client:

To do...	Use the command...	Remarks
Specify the source interface used for the current connection	tftp tftp-server source-interface <i>interface-type interface-number</i> { get source-file [dest-file] put source-file-url [dest-file] }	Optional Not specified by default.
Specify the source IP address used for the current connection	tftp tftp-server source-ip <i>ip-address</i> { get source-file [dest-file] put source-file-url [dest-file] }	Optional Not specified by default.

To do...	Use the command...	Remarks
Enter system view	system-view	—
Specify an interface as the source interface a TFTP client uses every time it connects to a TFTP server	tftp source-interface <i>interface-type interface-number</i>	Use either command Not specified by default.
Specify an IP address as the source IP address a TFTP client uses every time it connects to a TFTP server	tftp source-ip <i>ip-address</i>	
Display the source IP address used by a TFTP client every time it connects to a TFTP server	display tftp source-ip	Optional Available in any view



Note

- The specified interface must be an existing one; otherwise a prompt appears to show that the configuration fails.
- The value of the *ip-address* argument must be an IP address on the device where the configuration is performed, and otherwise a prompt appears to show that 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.

TFTP Configuration Example

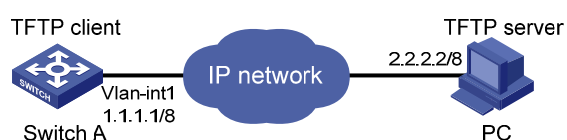
Network requirements

A switch operates as a TFTP client and a PC as the TFTP server. The application named **switch.bin** is stored on the PC. Download it (**switch.bin**) to the switch through TFTP, and use the **boot boot-loader** command to specify **switch.bin** as the application for next startup. Reboot the switch to upload the configuration file named **config.cfg** to the work directory on the PC to back up the configuration file.

- The TFTP working directory is configured on the TFTP server.
- Configure the IP addresses of a VLAN interface on the switch and the PC as 1.1.1.1 and 2.2.2.2 respectively. The port through which the switch connects with the PC belongs to the VLAN.

Network diagram

Figure 2-1 Network diagram for TFTP configurations



Configuration procedure

- 1) Configure the TFTP server (PC)

Start the TFTP server and configure the working directory on the PC.

- 2) Configure the TFTP client (switch).

Log in to the switch. (You can log in to a switch through the Console port or by telnetting the switch. See the *Login* module for detailed information.)

<Sysname>



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 not in use from the Flash memory to make room for the file, and then upload the file again. The files in use cannot be deleted. If you have to delete the files in use to make room for the file to be uploaded, you can only delete/download them through the Boot ROM menu.

Enter system view

```
<Sysname> system-view
```

```
[Sysname]
```

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.)

```
[Sysname] interface Vlan-interface 1
```

```
[Sysname-Vlan-interface1] ip address 1.1.1.1 255.255.255.0
```

```
[Sysname-Vlan-interface1] quit
```

Download the switch application named **switch.bin** from the TFTP server to the switch.

```
<Sysname> tftp 2.2.2.2 get switch.bin switch.bin
```

Upload the switch configuration file named **config.cfg** to the TFTP server.

```
<Sysname> tftp 2.2.2.2 put config.cfg config.cfg
```

After downloading the file, 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.

```
<Sysname> boot boot-loader switch.bin
```


<Sysname> 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

1 Information Center	1-1
Information Center Overview	1-1
Introduction to Information Center	1-1
System Information Format	1-4
Information Center Configuration	1-7
Information Center Configuration Task List	1-7
Configuring Synchronous Information Output	1-7
Configuring to Display the Time Stamp with the UTC Time Zone	1-8
Setting to Output System Information to the Console	1-8
Setting to Output System Information to a Monitor Terminal	1-10
Setting to Output System Information to a Log Host	1-11
Setting to Output System Information to the Trap Buffer	1-12
Setting to Output System Information to the Log Buffer	1-13
Setting to Output System Information to the SNMP NMS	1-13
Displaying and Maintaining Information Center	1-14
Information Center Configuration Examples	1-15
Log Output to a UNIX Log Host	1-15
Log Output to a Linux Log Host	1-16
Log Output to the Console	1-18
Configuration Example	1-19

1 Information Center

When configuring information center, go to these sections for information you are interested in:

- [Information Center Overview](#)
- [Information Center Configuration](#)
- [Displaying and Maintaining Information Center](#)
- [Information Center Configuration Examples](#)



Note

The information center now supports to add the UTC time zone in the time stamp of the output information. See [Timestamp](#) for details.

Information Center Overview

Introduction to Information Center

Acting as the system information hub, information center classifies and manages system information. Together with the debugging function (the **debugging** command), information center offers a powerful support for network administrators and developers in monitoring network performance and diagnosing network problems.

The information center of the system has the following features:

Classification of system information

The system is available with three types of information:

- Log information
- Trap information
- Debugging information

Eight levels of system information

The information is classified into eight levels by severity and can be filtered by level. More emergent information has a smaller severity level.

Table 1-1 Severity description

Severity	Severity value	Description
emergencies	1	The system is unavailable.
alerts	2	Information that demands prompt reaction
critical	3	Critical information
errors	4	Error information

Severity	Severity value	Description
warnings	5	Warnings
notifications	6	Normal information that needs to be noticed
informational	7	Informational information to be recorded
debugging	8	Information generated during debugging

Information filtering by severity works this way: information with the severity value greater than the configured threshold is not output during the filtering.

- If the threshold is set to 1, only information with the severity being emergencies will be output;
- If the threshold is set to 8, information of all severities will be output.

Ten channels and six output destinations of system information

The system supports six information output destinations, including the Console, Monitor terminal (monitor), logbuffer, loghost, trapbuffer and SNMP.

The system supports ten channels. The channels 0 through 5 have their default channel names and are associated with six output destinations by default. Both the channel names and the associations between the channels and output destinations can be changed through commands.

Table 1-2 Information channels and output destinations

Information channel number	Default channel name	Default output destination
0	console	Console (Receives log, trap and debugging information.)
1	monitor	Monitor terminal (Receives log, trap and debugging information, facilitating remote maintenance.)
2	loghost	Log host (Receives log, trap and debugging information and information will be stored in files for future retrieval.)
3	trapbuffer	Trap buffer (Receives trap information, a buffer inside the device for recording information.)
4	logbuffer	Log buffer (Receives log information, a buffer inside the device for recording information.)
5	snmpagent	SNMP NMS (Receives trap information.)
6	channel6	Not specified (Receives log, trap, and debugging information.)
7	channel7	Not specified (Receives log, trap, and debugging information.)
8	channel8	Not specified (Receives log, trap, and debugging information.)
9	channel9	Not specified (Receives log, trap, and debugging information.)



Note

Configurations for the six output destinations function independently and take effect only after the information center is enabled.

Outputting system information by source module

The system information can be classified by source module and then filtered. Some module names and description are shown in [Table 1-3](#).

Table 1-3 Source module name list

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
HTTPD	HTTP server module
IFNET	Interface management module
IGSP	IGMP snooping module
IP	Internet protocol module
LAGG	Link aggregation module
LINE	Terminal line module
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

Module name	Description
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	Virtual router redundancy protocol module
VTY	Virtual type terminal module
XM	XModem module
default	Default settings for all the modules

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

System Information Format

The format of system information varies with the output destinations.

- If the output destination is console, monitor terminal, logbuffer, trapbuffer, or SNMP, the system information is in the following format:

```
timestamp sysname module/level/digest: - unitid -content
```



Note

- The space, the forward slash /, and the colon are all required in the above format.
 - Before <timestamp> may have %, #, or * followed with a space, indicating log, alarm, or debugging information respectively.
-

Below is an example of the format of log information to be output to a monitor terminal:

%Dec 6 10:44:55:283 2006 Sysname NTP/5/NTP_LOG:- 1 - NTP service enable

("1-" indicates that the unit number of the device is 1.)

- If the output destination is loghost, the switch and the log host use the syslog protocol. The system information is in the following format according to RFC 3164 (The BSD Syslog Protocol):

<Int_16>timestamp sysname %nmodule/level/digest: source content



Note

- If the address of the log host is specified in the information center of the switch, when logs are generated, the switch sends the logs to the log host in the above format. For detailed information, refer to [Setting to Output System Information to a Log Host](#).
 - There is the syslog process on the Unix or Linux platform, you can start the process to receive the logs sent from the switch; in the Windows platform, you need to install the specific software, and it will operate as the syslog host.
 - Some log host software will resolve the received information as well as its format, so that the log format displayed on the log host is different from the one described in this manual.
-

What follows is a detailed explanation of the information fields involved:

Int_16 (Priority)

The priority is calculated using the following formula: facility*8+severity-1, in which

- facility (the device name) defaults to local7 with the value being 23 (the value of local6 is 22, that of local5 is 21, and so on).
- severity (the information level) ranges from 1 to 8. [Table 1-1](#) details the value and meaning associated with each severity.

Note that the priority field appears only when the information has been sent to the log host.

Timestamp

Timestamp records the time when system information is generated to allow users to check and identify system events.

Note that there is a space between the timestamp and sysname (host name) fields.

The time stamp has the following two formats.

- 1) Without the universal time coordinated (UTC) time zone, the time stamp is in the format of "Mmm dd hh:mm:ss:ms yyyy".
- 2) With the UTC time zone, the time stamp is in the format of "Mmm dd hh:mm:ss:ms yyyy [GMT +/-hh:mm:ss]".

Each field is described as follows:

- "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. (Note that: the time stamp of the system information sent from the information center to the log host is with a precision of seconds,

while that of the system information sent from the system center to the Console, monitor terminal, logbuffer, trapbuffer and the SNMP is with a precision of milliseconds.)

- “yyyy” is the year.
- “[GMT +/- hh:mm:ss]” is the UTC time zone, which represents the time difference with the Greenwich standard time.

Because switches in a network may distribute in different time zones, when the time displayed in the time stamps of output information is the local time on each switch, it is not so convenient for you to locate and solve problems globally. In this case, you can configure the information center to add UTC time zone to the time stamp of the output information, so that you can know the standard time when the information center processing each piece of information. That is, you can know the Greenwich standard time of each switch in the network based on the UTC record in the time stamp.

To add UTC time zone to the time stamp in the information center output information, you must:

- Set the local time zone
- Set the time stamp format in the output destination of the information center to **date**
- Configure to add UTC time zone to the output information

After the above configuration, the UTC time zone will be displayed in the output information, like the following:

```
%Dec 8 10:12:21:708 2006 [GMT+08:00:00] Sysname SHELL/5/LOGIN:- 1 - VTY(1.1.0.2) in unit1
login
```

Sysname

Sysname is the system name of the local switch and defaults to “H3C”.

You can use the **sysname** command to modify the system name. Refer to the System Maintenance and Debugging part of this manual for details)

Note that there is a space between the sysname and module fields.

%%

This field is a preamble used to identify a vendor. It is displayed only when the output destination is log host.

nn

This field is a version identifier of syslog. It is displayed only when the output destination is log host.

Module

The module field represents the name of the module that generates system information. You can enter the **info-center source ?** command in system view to view the module list. Refer to [Table 1-3](#) for module name and description.

Between “module” and “level” is a “/”.

Level (Severity)

System information can be divided into eight levels based on its severity, from 1 to 8. Refer to [Table 1-1](#) for definition and description of these severity levels. Note that there is a forward slash “/” between the level (severity) and digest fields.

Digest

The digest field is a string of up to 32 characters, outlining the system information.

Note that there is a colon between the digest and content fields.

For system information destined to the log host,

- If the character string ends with (l), it indicates the log information
- If the character string ends with (t), it indicates the trap information
- If the character string ends with (d), it indicates the debugging information

Source

This field indicates the source of the information, such as the source IP address of the log sender. This field is optional and is displayed only when the output destination is the log host.

Context

This field provides the content of the system information.

Information Center Configuration

Information Center Configuration Task List

Complete the following tasks to configure information center:

Task	Remarks
Configuring Synchronous Information Output	Optional
Configuring to Display the Time Stamp with the UTC Time Zone	Optional
Setting to Output System Information to the Console	Optional
Setting to Output System Information to a Monitor Terminal	Optional
Setting to Output System Information to a Log Host	Optional
Setting to Output System Information to the Trap Buffer	Optional
Setting to Output System Information to the Log Buffer	Optional
Setting to Output System Information to the SNMP NMS	Optional

Configuring Synchronous Information Output

Synchronous information output refers to the feature that if the system information such as log, trap, or debugging information is output when the user is inputting commands, the command line prompt (in command editing mode a prompt, or a [Y/N] string in interaction mode) and the input information are echoed after the output.

This feature is used in the case that your input is interrupted by a large amount of system output. With this feature enabled, the system echoes your previous input and you can continue your operations from where you were stopped.

Follow these steps to configure synchronous information output:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable synchronous information output	info-center synchronous	Required Disabled by default



Note

- If the system information is output before you input any information following the current command line prompt, the system does not echo any command line prompt after the system information output.
- In the interaction mode, you are prompted for some information input. If the input is interrupted by system output, no system prompt (except the Y/N string) will be echoed after the output, but your input will be displayed in a new line.

Configuring to Display the Time Stamp with the UTC Time Zone

To add UTC time zone to the time stamp in the information center output information, you must:

- Set the local time zone
- Set the time stamp format in the output destination of the information center to **date**
- Configure to add the UTC time zone to the output information

Follow these steps to configure to display time stamp with the UTC time zone:

To do...	Use the command...	Remarks
Set the time zone for the system	clock timezone <i>zone-name</i> { add minus } <i>time</i>	Required By default, UTC time zone is set for the system.
Enter system view	system-view	—
Set the time stamp format in the output destination of the information center to date	Log host direction info-center timestamp loghost date	Required Use either command
	Non log host direction info-center timestamp { log trap debugging } date	
Set to display the UTC time zone in the output information of the information center	info-center timestamp utc	Required By default, no UTC time zone is displayed in the output information

Setting to Output System Information to the Console

Setting to output system information to the console

Follow these steps to set to output system information to the console:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the information center	info-center enable	Optional Enabled by default.
Enable system information output to the console	info-center console channel { <i>channel-number</i> <i>channel-name</i> }	Optional By default, the switch uses information channel 0 to output log/debugging/trap information to the console.
Configure the output rules of system information	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug } { level <i>severity</i> state <i>state</i> }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	info-center timestamp { log trap debugging } { boot date none }	Optional By default, the time stamp format of the log and trap output information is date , and that of the debugging output information is boot .



Note

To view the debugging information of some modules on the switch, you need to set the type of the output information to **debug** when configuring the system information output rules, and use the **debugging** command to enable debugging for the corresponding modules.

Table 1-4 Default output rules for different output destinations

Output destination	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/disabled	Severity	Enabled/disabled	Severity	Enabled/disabled	Severity
Console	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging
Monitor terminal	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging
Log host	default (all modules)	Enabled	informational	Enabled	debugging	Disabled	debugging
Trap buffer	default (all modules)	Disabled	informational	Enabled	warnings	Disabled	debugging
Log buffer	default (all modules)	Enabled	warnings	Disabled	debugging	Disabled	debugging
SNMP NMS	default (all modules)	Disabled	debugging	Enabled	warnings	Disabled	debugging

Enabling system information display on the console

After setting to output system information to the console, you need to enable the associated display function to display the output information on the console.

Follow these steps to enable the system information display on the console:

To do...	Use the command...	Remarks
Enable the debugging/log/trap information terminal display function	terminal monitor	Optional Enabled by default.
Enable debugging information terminal display function	terminal debugging	Optional Disabled by default.
Enable log information terminal display function	terminal logging	Optional Enabled by default.
Enable trap information terminal display function	terminal trapping	Optional Enabled by default.



Note

Make sure that the debugging/log/trap information terminal display function is enabled (use the **terminal monitor** command) before you enable the corresponding terminal display function by using the **terminal debugging**, **terminal logging**, or **terminal trapping** command.

Setting to Output System Information to a Monitor Terminal

System information can also be output to a monitor terminal, which is a user terminal that has login connections through the AUX, or VTY user interface.

Setting to output system information to a monitor terminal

Follow these steps to set to output system information to a monitor terminal:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the information center	info-center enable	Optional Enabled by default.
Enable system information output to Telnet terminal or dumb terminal	info-center monitor channel { <i>channel-number</i> <i>channel-name</i> }	Optional By default, a switch outputs log/debugging/trap information to a user terminal through information channel 1.
Configure the output rules of system information	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug } { level severity state state }]*	Optional Refer to Table 1-4 for the default output rules of system information.

To do...	Use the command...	Remarks
Set the format of time stamp in the output information	info-center timestamp { log trap debugging } { boot date none }	Optional By default, the time stamp format of the log and trap output information is date , and that of the debugging output information is boot .



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 setting the system information output rules, and enable debugging for corresponding modules through the **debugging** command.

Enabling system information display on a monitor terminal

After setting to output system information to a monitor terminal, you need to enable the associated display function in order to display the output information on the monitor terminal.

Follow these steps to enable the display of system information on a monitor terminal:

To do...	Use the command...	Remarks
Enable the debugging/log/trap information terminal display function	terminal monitor	Optional Enabled by default
Enable debugging information terminal display function	terminal debugging	Optional Disabled by default
Enable log information terminal display function	terminal logging	Optional Enabled by default
Enable trap information terminal display function	terminal trapping	Optional Enabled by default



Note

Make sure that the debugging/log/trap information terminal display function is enabled (use the **terminal monitor** command) before you enable the corresponding terminal display function by using the **terminal debugging**, **terminal logging**, or **terminal trapping** command.

Setting to Output System Information to a Log Host

Follow these steps to set to output system information to a log host:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the information center	info-center enable	Optional Enabled by default.
Enable information output for a specified switch in a fabric	info-center switch-on { unit <i>unit-id</i> master all } [debugging logging trapping]*	Optional 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 system information output to a log host	info-center loghost <i>host-ip-addr</i> [channel { <i>channel-number</i> <i>channel-name</i> } facility <i>local-number</i>]*	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.
Configure the source interface through which log information is sent to the log host	info-center loghost source <i>interface-type</i> <i>interface-number</i>	Optional By default, no source interface is configured, and the system automatically selects an interface as the source interface.
Configure the output rules of system information	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug } { level <i>severity</i> state <i>state</i> }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of the time stamp to be sent to the log host	info-center timestamp loghost { date no-year-date none }	Optional By default, the time stamp format of the information output to the log host is date .



Note

- After the switches form a fabric, you can use the **info-center switch-on** command to enable the information output for the switches 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.
- Be sure to set the correct IP address when using the **info-center loghost** command. A loopback IP address will cause an error message prompting that this address is invalid.

Setting to Output System Information to the Trap Buffer

Follow these steps to set to output system information to the trap buffer:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the information center	info-center enable	Optional Enabled by default.
Enable system information output to the trap buffer	info-center trapbuffer [channel { <i>channel-number</i> <i>channel-name</i> } size <i>buffer-size</i>]*	Optional By default, the switch uses information channel 3 to output trap information to the trap buffer, which can hold up to 256 items by default.
Configure the output rules of system information	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug } { level <i>severity</i> state <i>state</i> }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	info-center timestamp { log trap debugging } { boot date none }	Optional By default, the time stamp format of the output trap information is date .

Setting to Output System Information to the Log Buffer

Follow these steps to set to output system information to the log buffer:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the information center	info-center enable	Optional Enabled by default.
Enable information output to the log buffer	info-center logbuffer [channel { <i>channel-number</i> <i>channel-name</i> } size <i>buffer-size</i>]*	Optional By default, the switch uses information channel 4 to output log information to the log buffer, which can hold up to 512 items by default.
Configure the output rules of system information	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug } { level <i>severity</i> state <i>state</i> }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	info-center timestamp { log trap debugging } { boot date none }	Optional By default, the time stamp format of the output log information is date .

Setting to Output System Information to the SNMP NMS

Follow these steps to set to output system information to the SNMP NMS:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the information center	info-center enable	Optional Enabled by default.
Enable information output to the SNMP NMS	info-center snmp channel { <i>channel-number</i> <i>channel-name</i> }	Optional By default, the switch outputs trap information to SNMP through channel 5.
Configure the output rules of system information	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug } { level severity state state }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	info-center timestamp { log trap debugging } { boot date none }	Optional By default, the time stamp format of the information output to the SNMP NMS is date .



Note

To send information to a remote SNMP NMS properly, related configurations are required on both the switch and the SNMP NMS. For the detailed configuration, refer to the *SNMP-RMON* part.

Displaying and Maintaining Information Center

To do...	Use the command...	Remarks
Display information on an information channel	display channel [<i>channel-number</i> <i>channel-name</i>]	Available 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 [<i>unit unit-id</i>]	
Display the status of log buffer and the information recorded in the log buffer	display logbuffer [<i>unit unit-id</i>] [level severity size buffersize]* [[begin exclude include] <i>regular-expression</i>]	
Display the summary information recorded in the log buffer	display logbuffer summary [level severity]	
Display the status of trap buffer and the information recorded in the trap buffer	display trapbuffer [<i>unit unit-id</i>] [size buffersize]	

To do...	Use the command...	Remarks
Clear information recorded in the log buffer	reset logbuffer [unit <i>unit-id</i>]	Available in user view
Clear information recorded in the trap buffer	reset trapbuffer [unit <i>unit-id</i>]	

Information Center Configuration Examples

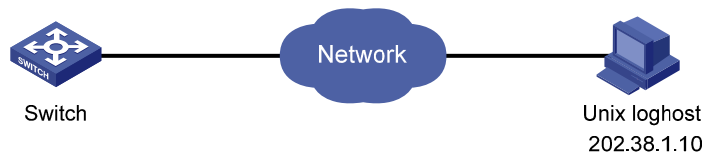
Log Output to a UNIX Log Host

Network requirements

The switch sends the following log information 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”.

Network diagram

Figure 1-1 Network diagram for log output to a Unix log host



Configuration procedure

1) Configure the switch:

Enable the information center.

```
<Switch> system-view
```

```
[Switch] info-center enable
```

Disable the function of outputting information to log host channels, because all modules output log information to the log host channels by default.

```
[Switch] undo info-center source default channel loghost
```

Configure the host whose IP address is 202.38.1.10 as the log host. Permit ARP and IP modules to output information with severity level higher than informational to the log host.

```
[Switch] info-center loghost 202.38.1.10 facility local4
```

```
[Switch] info-center source arp channel loghost log level informational debug state off trap state off
```

```
[Switch] 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/Switch
```

```
# touch /var/log/Switch/information
```

Step 2: Edit the file “/etc/syslog.conf” as the super user (root user) to add the following selector/action pairs.

```
# Switch configuration messages
local4.info    /var/log/Switch/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 device name (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 reread its 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.

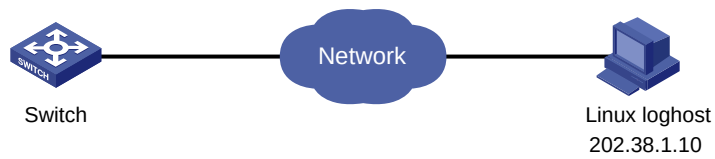
Log Output to a Linux Log Host

Network requirements

The switch sends the following log information to the Linux log host whose IP address is 202.38.1.10: All modules' log information, with severity higher than “errors”.

Network diagram

Figure 1-2 Network diagram for log output to a Linux log host



Configuration procedure

1) Configure the switch:

Enable the information center.

```
<Switch> system-view
```

```
[Switch] info-center enable
```

Configure the host whose IP address is 202.38.1.10 as the log host. Permit all modules to output log information with severity level higher than error to the log host.

```
[Switch] info-center loghost 202.38.1.10 facility local7
```

```
[Switch] 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/Switch
```

```
# touch /var/log/Switch/information
```

Step 2: Edit the file “/etc/syslog.conf” as the super user (root user) to add the following selector/action pairs.

```
# Switch configuration messages
```

```
local7.info    /var/log/Switch/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 device name (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 &
```

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.

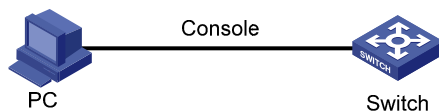
Log Output to the Console

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”.

Network diagram

Figure 1-3 Network diagram for log output to the console



Configuration procedure

Enable the information center.

```
<Switch> system-view
```

```
[Switch] info-center enable
```

Disable the function of outputting information to the console channels.

```
[Switch] undo info-center source default channel console
```

Enable log information output to the console. Permit ARP and IP modules to output log information with severity level higher than informational to the console.

```
[Switch] info-center console channel console
```

```
[Switch] info-center source arp channel console log level informational debug state off trap state off
```

```
[Switch] info-center source ip channel console log level informational debug state off trap state off
```

Enable terminal display.

```
<Switch> terminal monitor
```

```
<Switch> terminal logging
```

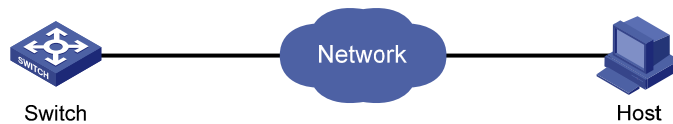
Configuration Example

Network requirements

- The switch is in the time zone of GMT+ 08:00:00.
- The time stamp format of output log information is date.
- UTC time zone will be added to the output information of the information center.

Network diagram

Figure 1-4 Network diagram



Configuration procedure

Name the local time zone z8 and configure it to be eight hours ahead of UTC time.

```
<Switch> clock timezone z8 add 08:00:00
```

Set the time stamp format of the log information to be output to the log host to date.

```
<Switch> system-view
```

System View: return to User View with Ctrl+Z.

```
[Switch] info-center timestamp loghost date
```

Configure to add UTC time to the output information of the information center.

```
[Switch] info-center timestamp utc
```

Table of Contents

1 Boot ROM and Host Software Loading	1-1
Introduction to Loading Approaches	1-1
Local Boot ROM and Software Loading.....	1-2
BOOT Menu	1-2
Loading by XModem through Console Port	1-3
Loading by TFTP through Ethernet Port	1-8
Loading by FTP through Ethernet Port.....	1-10
Remote Boot ROM and Software Loading	1-11
Remote Loading Using FTP	1-11
Remote Loading Using TFTP	1-16
2 Basic System Configuration and Debugging	2-1
Basic System Configuration	2-1
Displaying the System Status	2-2
Debugging the System.....	2-2
Enabling/Disabling System Debugging	2-2
Displaying Debugging Status	2-3
Displaying Operating Information about Modules in System	2-3
3 Network Connectivity Test	3-1
Network Connectivity Test	3-1
ping	3-1
tracert.....	3-1
4 Device Management	4-1
Introduction to Device Management	4-1
Device Management Configuration.....	4-1
Device Management Configuration Task list.....	4-1
Rebooting the Ethernet Switch	4-1
Scheduling a Reboot on the Switch	4-2
Configuring Real-time Monitoring of the Running Status of the System	4-2
Specifying the APP to be Used at Reboot.....	4-3
Upgrading the Boot ROM	4-3
Upgrading the Host Software in the Fabric	4-3
Enabling Auto Power Down on the Ethernet Electrical Port.....	4-3
Loading Hot Patch	4-4
Identifying and Diagnosing Pluggable Transceivers	4-6
Displaying the Device Management Configuration	4-7
Remote Switch APP Upgrade Configuration Example	4-8
5 Scheduled Task Configuration.....	5-1
What Is a Scheduled Task	5-1
Configuring a Scheduled Task	5-1
Configuration prerequisites	5-1
Configuring a scheduled task to be executed at a specified time	5-1
Configuring a scheduled task to be executed after a delay time	5-2

Scheduled Task Configuration Example	5-2
Network requirements	5-2
Configuration procedure	5-3

1 Boot ROM and Host Software Loading



Note

- The Enabling Auto Power Down on the Ethernet Electrical Port is added. For the detailed configuration, refer to [Enabling Auto Power Down on the Ethernet Electrical Port](#).
 - The Scheduled Task Configuration is added. For the detailed configuration, refer to [Scheduled Task Configuration](#).
-

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 the Boot ROM and host software to a switch locally and remotely. When configuring the Boot ROM and host software loading, go to these sections for information you are interested in:

- [Introduction to Loading Approaches](#)
- [Local Boot ROM and Software Loading](#)
- [Remote Boot ROM and Software Loading](#)

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 Boot ROM software version should be compatible with the host software version when you load the Boot ROM and host software.

Local Boot ROM and Software Loading

If your terminal is directly connected to the Console port of the switch, you can load the Boot ROM 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 Boot ROM software is the same as that of the host software, except that during the former process, you should press “6” or <Ctrl+U> and <Enter> after entering the BOOT menu and the system gives different prompts. The following text mainly describes the Boot ROM loading process.

BOOT Menu

Starting.....

```
*****
*
*          H3C S3600-52P-EI BOOTROM, Version 510
*
*****

Copyright(c) 2004-2007 Hangzhou H3C Technologies Co., Ltd.
Creation date   : May 29 2007, 19:39:48
CPU Clock Speed : 200MHz
BUS Clock Speed : 33MHz
Memory Size    : 64MB
Mac Address     : 000fe2123456
```

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 (full startup mode) or one second (fast startup mode) 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 Boot ROM password (no password is set 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):

Loading by XModem through Console Port

Introduction to XModem

XModem protocol is a file transfer protocol that is widely used due to its simplicity and high stability. 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.

Loading Boot ROM

Follow these steps to load the Boot ROM:

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 Boot ROM 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 Boot ROM 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 baudrate for downloading. For example, if you press 5, the baudrate 115200 bps is chosen and the system displays the following information:

Download baudrate is 115200 bit/s

Please change the terminal's baudrate to 115200 bit/s 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.

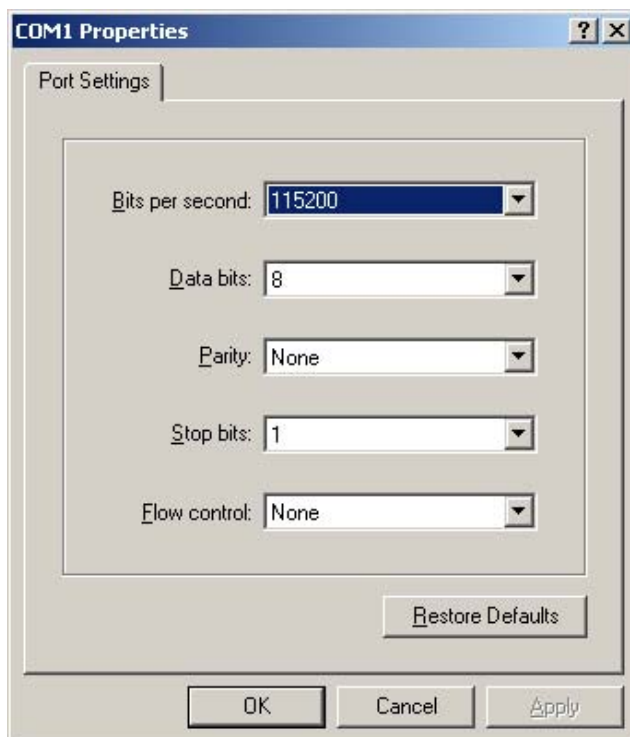
Following are configurations on PC. Take the HyperTerminal in Windows 2000 as an example.

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

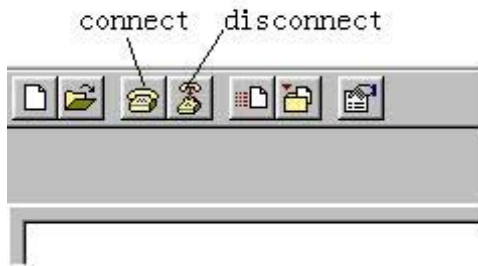


Figure 1-2 Console port configuration dialog box



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:

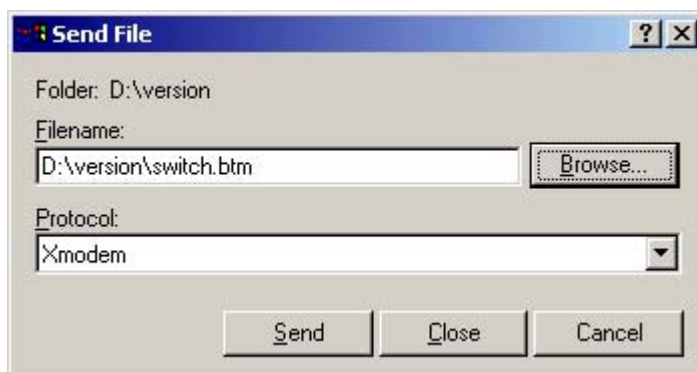
Now please start transfer file with XMODEM protocol.

If you want to exit, Press <Ctrl+X>.

Loading ...CCCCCCCCC

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

Xmodem file send for switch

Sending: D:\version\switch.btm

Packet: 12 Error checking: CRC

Retries: 0 Total retries: 0

Last error:

File: 1k of 291K

Elapsed: 00:00:01 Remaining: Throughput:

Cancel cps/bps

Step 9: After the sending process completes, the system displays the following information:

Loading ...CCCCCCCCC 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 the Boot ROM automatically and prompts "Bootrom updating now.....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):

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 Boot ROM, except that the system gives the prompt for host software loading instead of Boot ROM loading.



You can also use the **xmodem get** command to load host software through the Console port (of AUX type). The load procedures are as follows (assume that the PC is connected to the Console port of the switch, and logs onto the switch through the Console port):

Step 1: Execute the **xmodem get** command in user view. In this case, the switch is ready to receive files.

Step 2: Enable the HyperTerminal on the PC, and configure XModem as the transfer protocol, and configure communication parameters on the Hyper Terminal the same as that on the Console port.

Step 3: Choose the file to be loaded to the switch, and then start to transmit the file.

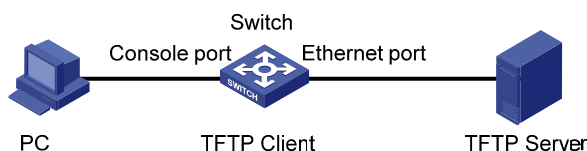
Loading by TFTP through Ethernet Port

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.

Loading the Boot ROM

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.



You can use one PC as both the configuration device and the TFTP server.

Step 2: 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 Boot ROM 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 Boot ROM using TFTP. Then set the following TFTP-related parameters as required:

```
Load File name           :Switch.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 Boot ROM update menu. If you enter Y, the system begins to download and update the Boot ROM. 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):

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 Boot ROM, except that the system gives the prompt for host software loading instead of Boot ROM loading.



Caution

When loading Boot ROM 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.

Loading by FTP through Ethernet Port

Introduction to FTP

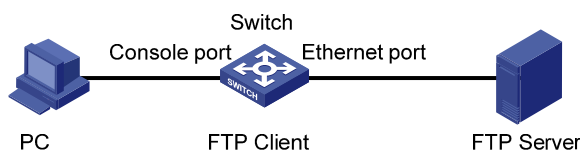
FTP is an application-layer protocol in the TCP/IP protocol suite. It is used for file transfer between server and client, and is widely used in IP networks.

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.

Loading Procedure Using FTP Client

- Loading Boot ROM

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 Boot ROM 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 Boot ROM using FTP. Then set the following FTP-related parameters as required:

```
Load File name           :switch.btm
Switch IP address        :10.1.1.2
Server IP address        :10.1.1.1
FTP User Name            :Switch
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 Boot ROM 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 Boot ROM, except for that the system gives the prompt for host software loading instead of Boot ROM loading.



Caution

When loading the Boot ROM 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.

Remote Boot ROM 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 the Boot ROM and host software remotely.

Remote Loading Using FTP

Loading Procedure Using FTP Client

- 1) Loading the Boot ROM

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 Boot ROM program switch.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.

```
<Sysname> 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 switch.btm
[ftp] bye
```



Note

When using different FTP server software on PC, different information will be output to the switch.

Step 2: Update the Boot ROM program on the switch.

```
<Sysname> boot bootrom switch.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.

```
<Sysname> 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 Boot ROM 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 Boot ROM and host software loading is completed.

Pay attention to the following:

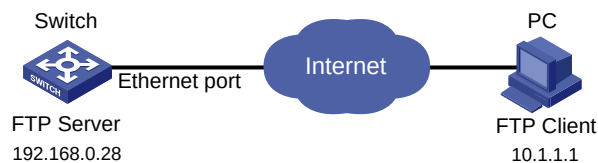
- The loading of Boot ROM and host software takes effect only after you restart the switch with the **reboot** command.
- If the space of the Flash memory is not enough, you can delete the unused files in the Flash memory before software downloading. For information about deleting files, refer to *File System Management* part of this manual.
- Ensure the power supply during software loading.

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 upload the Boot ROM switch.btm to the switch.

1) Loading the Boot ROM

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 192.168.0.28, 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.

```
<Sysname> system-view
```

```
System View: return to User View with Ctrl+Z.
```

```
[Sysname] interface Vlan-interface 1
```

```
[Sysname-Vlan-interface1] ip address 192.168.0.28 255.255.255.0
```

Step 3: Enable FTP service on the switch, and configure the FTP user name to test and password to pass.

```
[Sysname-Vlan-interface1] quit
```

```
[Sysname] ftp server enable
```

```
[Sysname] local-user test
```

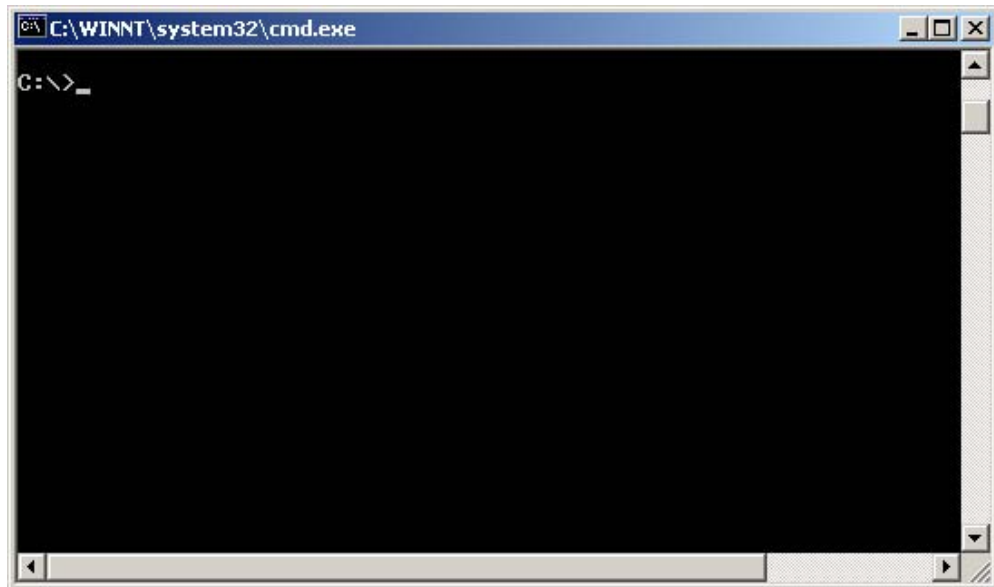
New local user added.

```
[Sysname-luser-test] password simple pass
```

```
[Sysname-luser-test] service-type ftp
```

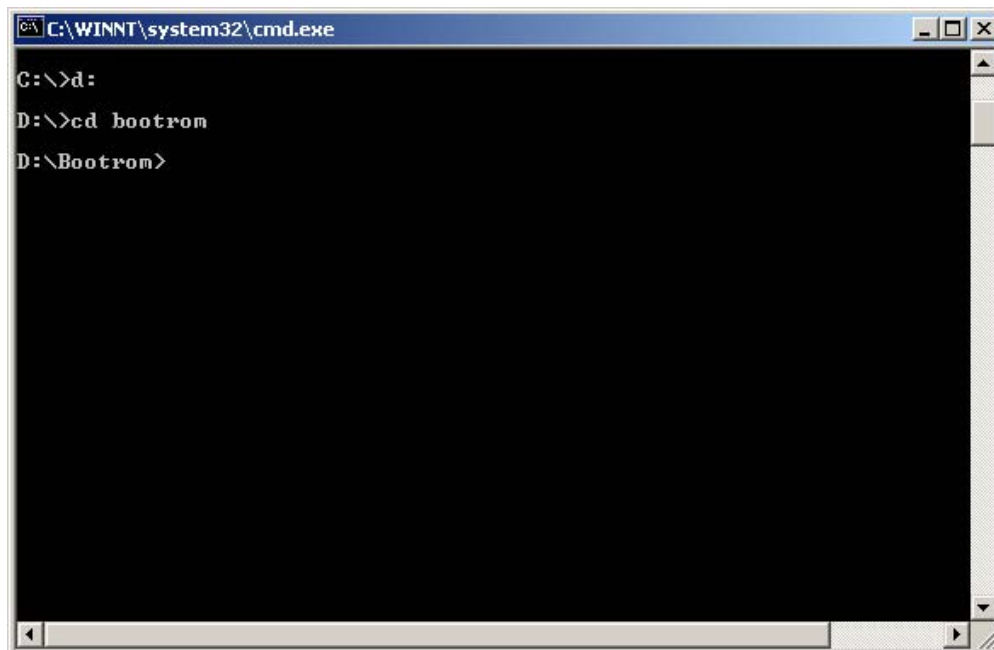
Step 4: Enable FTP client software on the PC. Refer to [Figure 1-10](#) for the command line interface in Windows operating system.

Figure 1-10 Command line interface



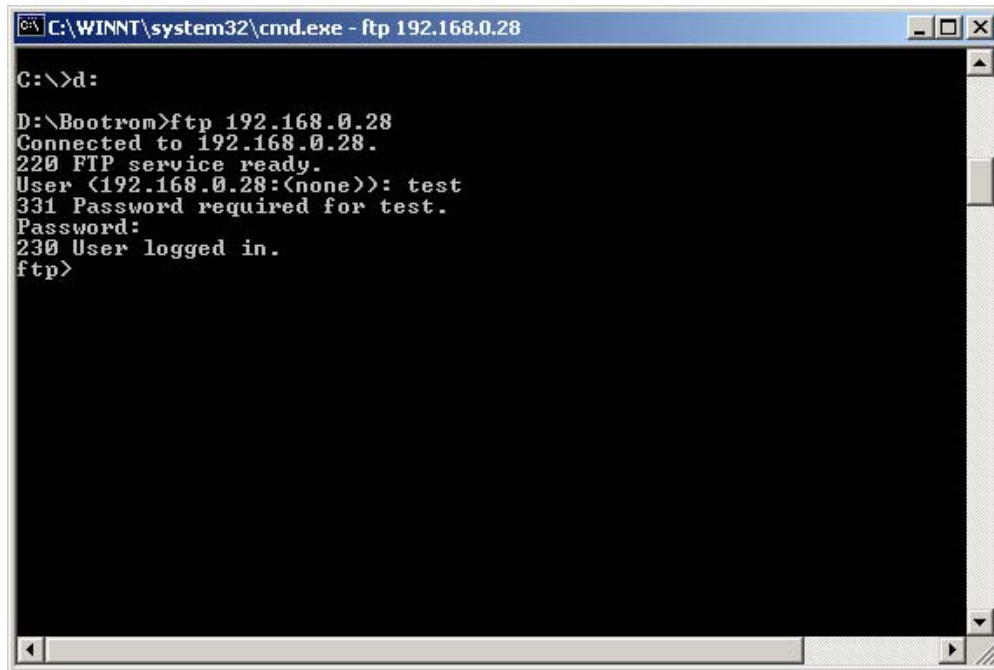
Step 5: Use the **cd** command on the interface to enter the path that the Boot ROM upgrade file is to be stored. Assume the name of the path is D:\Bootrom, as shown in [Figure 1-11](#).

Figure 1-11 Enter Boot ROM directory



Step 6: Enter **ftp 192.168.0.28** 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



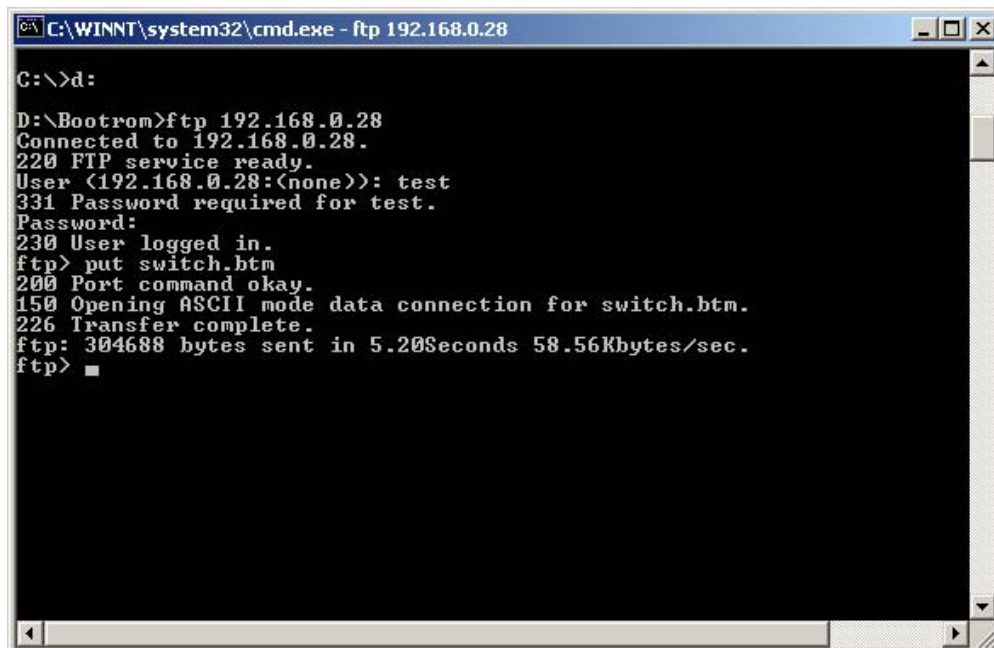
```
C:\WINNT\system32\cmd.exe - ftp 192.168.0.28

C:\>d:

D:\Bootrom>ftp 192.168.0.28
Connected to 192.168.0.28.
220 FTP service ready.
User (192.168.0.28:(none)): test
331 Password required for test.
Password:
230 User logged in.
ftp>
```

Step 7: Use the **put** command to upload the file switch.btm to the switch, as shown in [Figure 1-13](#).

Figure 1-13 Upload file switch.btm to the switch



```
C:\WINNT\system32\cmd.exe - ftp 192.168.0.28

C:\>d:

D:\Bootrom>ftp 192.168.0.28
Connected to 192.168.0.28.
220 FTP service ready.
User (192.168.0.28:(none)): test
331 Password required for test.
Password:
230 User logged in.
ftp> put switch.btm
200 Port command okay.
150 Opening ASCII mode data connection for switch.btm.
226 Transfer complete.
ftp: 304688 bytes sent in 5.20Seconds 58.56Kbytes/sec.
ftp> ■
```

Step 8: Configure switch.btm to be the Boot ROM at next startup, and then restart the switch.

```
<Sysname> boot bootrom switch.btm
This will update Bootrom on unit 1. Continue? [Y/N] y
Upgrading Bootrom, please wait...
Upgrade Bootrom succeeded!
<Sysname> reboot
```

After the switch restarts, the file switch.btm is used as the Boot ROM. It indicates that the Boot ROM loading is finished.

2) Loading host software

Loading the host software is the same as loading the Boot ROM 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 *FTP-SFTP-TFTP* part of this manual.
-

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.

2 Basic System Configuration and Debugging

When configuring basic system configuration and debugging, go to these sections for information you are interested in:

- [Basic System Configuration](#)
- [Displaying the System Status](#)
- [Debugging the System](#)

Basic System Configuration

Perform the following basic system configuration:

To do...	Use the command...	Remarks
Set the current date and time of the system	clock datetime <i>HH:MM:SS</i> { <i>YYYY/MM/DD</i> <i>MM/DD/YYYY</i> }	Required Execute this command in user view. The default value is 23:55:00 04/01/2000 when the system starts up.
Set the local time zone	clock timezone <i>zone-name</i> { add minus } <i>HH:MM:SS</i>	Optional Execute this command in user view. By default, it is the UTC time zone.
Set the name and time range of the summer time	clock summer-time <i>zone_name</i> { one-off repeating } <i>start-time</i> <i>start-date end-time</i> <i>end-date offset-time</i>	Optional Execute this command in user view. • 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.
Enter system view from user view	system-view	—
Set the system name of the switch	sysname <i>sysname</i>	Optional By default, the name is H3C.
Return from current view to lower level view	quit	Optional If the current view is user view, you will quit the current user interface.
Return from current view to user view	return	Optional The composite key <Ctrl+Z> has the same effect with the return command.

Displaying the System Status

To do...	Use the command...	Remarks
Display the current date and time of the system	display clock	Available in any view
Display the version of the system	display version	
Display the information about users logging onto the switch	display users [all]	

Debugging the System

Enabling/Disabling System Debugging

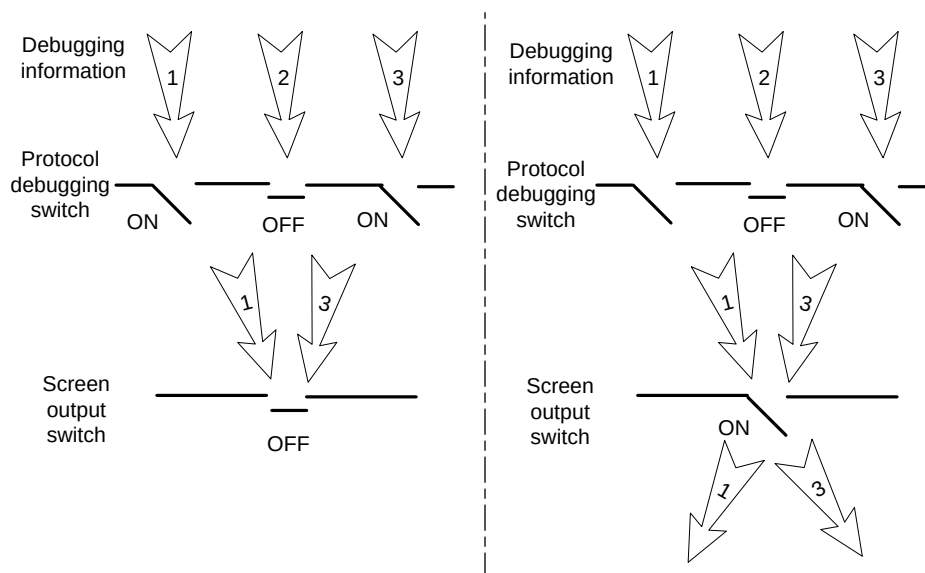
The device provides various debugging functions. For the majority of protocols and features supported, the system provides corresponding debugging information to help users diagnose errors.

The following two switches control the display of debugging information:

- Protocol debugging switch, which controls protocol-specific debugging information
- Screen output switch, which controls whether to display the debugging information on a certain screen.

[Figure 2-1](#) illustrates the relationship between the protocol debugging switch and the screen output switch. Assume that the device can output debugging information to module 1, 2 and 3. Only when both are turned on can debugging information be output on a terminal.

Figure 2-1 The relationship between the protocol and screen debugging switch



Note

Displaying debugging information on the terminal is the most commonly used way to output debugging information. You can also output debugging information to other directions. For details, refer to *Information Center Operation*.

You can use the following commands to enable the two switches.

Follow these steps to enable debugging and terminal display for a specific module:

To do...	Use the command...	Remarks
Enable system debugging for specific module	debugging <i>module-name</i> [<i>debugging-option</i>]	Required Disabled for all modules by default.
Enable terminal display for debugging	terminal debugging	Required Disabled by default.



Caution

The output of debugging information affects the system operation. Disable all debugging after you finish the system debugging.

Displaying Debugging Status

To do...	Use the command...	Remarks
Display all enabled debugging on the specified device	display debugging [fabric unit <i>unit-id</i>] [interface <i>interface-type interface-number</i>] [<i>module-name</i>]	Available in any view.
Display all enabled debugging in the Fabric by module	display debugging fabric by-module	

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.

To do...	Use the command...	Remarks
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.

3 Network Connectivity Test

When configuring network connectivity test, go to these sections for information you are interested in:

- [ping](#)
- [tracert](#)

Network Connectivity Test

ping

You can use the **ping** command to check the network connectivity and the reachability of a host.

To do...	Use the command...	Remarks
Check the IP network connectivity and the reachability of a host	ping [-a <i>ip-address</i>] [-c <i>count</i>] [-d] [-f] [-h <i>ttl</i>] [-i <i>interface-type interface-number</i>] [ip] [-n] [-p <i>pattern</i>] [-q] [-s <i>packetsize</i>] [-t <i>timeout</i>] [-tos <i>tos</i>] [-v] <i>host</i>	You can execute 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, time to live (TTL) 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.

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 also be used to help locate the network faults.

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.

To do...	Use the command...	Remarks
View the gateways that a packet passes from the source host to the destination	tracert [-a <i>source-ip</i>] [-f <i>first-ttl</i>] [-m <i>max-ttl</i>] [-p <i>port</i>] [-q <i>num-packet</i>] [-w <i>timeout</i>] <i>string</i>	You can execute the tracert command in any view.

4 Device Management

When configuring device management, go to these sections for information you are interested in:

- [Introduction to Device Management](#)
- [Device Management Configuration](#)
- [Displaying the Device Management Configuration](#)
- [Remote Switch APP Upgrade Configuration Example](#)

Introduction to Device Management

Device Management includes the following:

- Reboot the Ethernet switch
- Configure real-time monitoring of the running status of the system
- Specify the APP to be used at the next reboot
- Update the Boot ROM
- Update the host software of the switches in the Fabric
- Load Hot Patch
- Identifying and Diagnosing Pluggable Transceivers

Device Management Configuration

Device Management Configuration Task list

Complete the following tasks to configure device management:

Task	Remarks
Rebooting the Ethernet Switch	Optional
Scheduling a Reboot on the Switch	Optional
Configuring Real-time Monitoring of the Running Status of the System	Optional
Specifying the APP to be Used at Reboot	Optional
Upgrading the Boot ROM	Optional
Upgrading the Host Software in the Fabric	Optional
Loading Hot Patch	Optional
Identifying and Diagnosing Pluggable Transceivers	Optional

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

Use the following command to reboot the Ethernet switch:

To do...	Use the command...	Remarks
Reboot the Ethernet switch	reboot [unit <i>unit-id</i>]	Available in user view

Scheduling a Reboot on the Switch

After you schedule a reboot on the switch, the switch will reboot at the specified time.

Follow these steps to schedule a reboot on the switch:

To do...	Use the command...	Remarks
Schedule a reboot on the switch, and set the reboot date and time	schedule reboot at <i>hh:mm</i> [<i>mm/dd/yyyy</i> <i>yyyy/mm/dd</i>]	Optional
Schedule a reboot on the switch, and set the delay time for reboot	schedule reboot delay { <i>hh:mm</i> <i>mm</i> }	Optional
Enter system view	system-view	—
Schedule a reboot on the switch, and set the reboot period	schedule reboot regularity at <i>hh:mm period</i>	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.

Configuring Real-time Monitoring of the Running Status of the System

This function enables you to dynamically record the system running status, such as CPU, thus facilitating analysis and solution of the problems of the device.

Follow these steps to configure real-time monitoring of the running status of the system:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable real-time monitoring of the running status of the system	system-monitor enable	Optional Enabled by default.



Caution

Enabling of this function consumes some amounts of CPU resources. Therefore, if your network has a high CPU usage requirement, you can disable this function to release your CPU resources.

Specifying the APP to be Used 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 used when the switch reboots.

Use the following command to specify the APP to be used at reboot:

To do...	Use the command...	Remarks
Specify the APP to be used at reboot	boot boot-loader [backup-attribute] { <i>file-url</i> [fabric] <i>device-name</i> }	Required

Upgrading the Boot ROM

You can use the Boot ROM program saved in the Flash memory of the switch to upgrade the running Boot ROM. With this command, a remote user can conveniently upgrade the Boot ROM by uploading the Boot ROM to the switch through FTP and running this command. The Boot ROM can be used when the switch restarts.

Use the following command to upgrade the Boot ROM:

To do...	Use the command...	Remarks
Upgrade the Boot ROM	boot bootrom { <i>file-url</i> <i>device-name</i> }	Required

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.

To do...	Use the command...	Remarks
Upgrade the host software on the devices in the Fabric	update fabric { <i>file-url</i> <i>device-name</i> }	Required

Enabling Auto Power Down on the Ethernet Electrical Port

When auto power down is enabled on a Ethernet electrical port, if the port is not connected to another port, or if the peer port is shut down, the Ethernet electrical port automatically enters the power save state, so as to lower the power consumption of the switch.

Table 4-1 Follow these steps to enable auto power down on the Ethernet electrical port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable auto power down on the Ethernet electrical port	port auto-power-down	Required Disabled by default.



Note

Currently, the Ethernet switches only support configuring auto power down on Ethernet electrical ports.

Loading Hot Patch

A patch is a standalone software unit that is released to fix errors found in a system.

A hot patch can fix system errors without rebooting the device or interrupting network operation. That is, it can upgrade the system dynamically.

Patches can be added to a patch file incrementally. That is, any subsequent patch file contains all the patches for fixing errors in the previous patch file besides the patches for fixing the current errors. In this way, all the system errors found can be fixed once and for all by loading the latest patch file.

In the device, a patch can be in one of the following four states:

- IDLE: The patch is initialized but not loaded.
- DEACTIVE: The patch is loaded but not activated.
- ACTIVE: The patch is active but not running.
- RUNNING: The patch is running.

The difference between active patches and running patches:

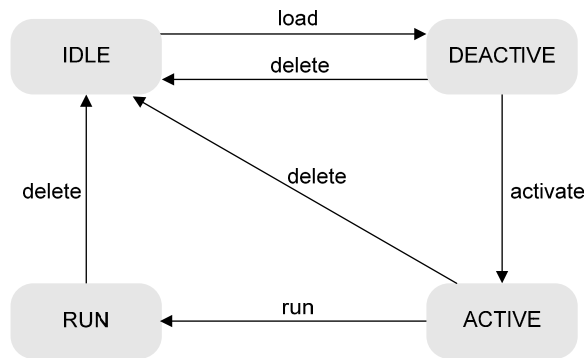
- After system reboot, an ACTIVE patch becomes DEACTIVE and stops working;
- After system reboot, a running patch remains running.

The active state provides a buffer to help prevent the system from running with errors introduced by the by the patches.

Any state of the four cannot be switched to another without user intervention on the command line.

[Figure 4-1](#) illustrates how patch states change with commands:

Figure 4-1 Relationship between patch state transition and commands



Note

To dynamically upgrade a fabric constituted by several switches, you can activate, run, and delete the patches on the fabric, which can be regarded as an independent device, instead of performing upgrades on each device. However, for each unit device, patch files need to be uploaded separately through FTP or TFTP to the flash memory and loaded into the memory with the **patch load** command.

Follow these steps to perform hot patch configuration:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Load a patch file	patch load <i>filename</i>	Required
Activate patches	patch activate	Required
Run patches	patch run	Optional
Delete patches	patch delete	Optional

Note the following:

- 2) Make sure that you set the file transfer mode to binary before you upload a patch file through FTP or TFTP to the flash memory of the device; otherwise, patch file loading will fail.
- 3) Before loading a patch file, verify that the baseline version number of the patch file and the current software version number are consistent, and the extension name of a patch file must be .pat by using the **display version** command. For the baseline version number of the patch file, see the patch file name. Patch files are named in the format of [product name]-[baseline version number]-[patch version number].pat.
- 4) The **patch delete** command deletes all the patches in the device. To prevent the solved system errors from occurring again, you need to reload and activate the related patches.
- 5) Patch state information is stored in a file named **patchstate** in the flash memory. You are not encouraged to perform any operation on this file.

Identifying and Diagnosing Pluggable Transceivers

Introduction to pluggable transceivers

At present, four types of pluggable transceivers are commonly used, and they can be divided into optical transceivers and electrical transceivers based on transmission media as shown in [Table 4-2](#).

Table 4-2 Commonly used pluggable transceivers

Transceiver type	Applied environment	Whether can be an optical transceiver	Whether can be an electrical transceiver
SFP (Small Form-factor Pluggable)	Generally used for 100M/1000M Ethernet interfaces or POS 155M/622M/2.5G interfaces	Yes	Yes
GBIC (GigaBit Interface Converter)	Generally used for 1000M Ethernet interfaces	Yes	Yes
XFP (10-Gigabit small Form-factor Pluggable)	Generally used for 10G Ethernet interfaces	Yes	No
XENPAK (10 Gigabit EtherNet Transceiver Package)	Generally used for 10G Ethernet interfaces	Yes	Yes



Note

For pluggable transceivers supported by S3600 series Ethernet switches, refer to *H3C S3600 Series Ethernet Switches Installation Manual*.

Identifying pluggable transceivers

As pluggable transceivers are of various types and from different vendors, you can perform the following configurations to identify main parameters of the pluggable transceivers, including transceiver type, connector type, central wavelength of the laser sent, transfer distance and vendor name or vendor name specified.

Follow these steps to identify pluggable transceivers:

To do...	Use the command...	Remarks
Display main parameters of the pluggable transceiver(s)	display transceiver interface [<i>interface-type</i> <i>interface-number</i>]	Available for all pluggable transceivers
Display part of the electrical label information of the anti-spoofing transceiver(s) customized by H3C	display transceiver manuinfo interface [<i>interface-type</i> <i>interface-number</i>]	Available for anti-spoofing pluggable transceiver(s) customized by H3C only

- You can use the **Vendor Name** field in the prompt information of the **display transceiver interface** command to identify an anti-spoofing pluggable transceiver customized by H3C. If the field is **H3C**, it is considered an H3C-customized pluggable transceiver.
- Electrical label information is also called permanent configuration data or archive information, which is written to the storage device of a card during device debugging or test. The information includes name of the card, device serial number, and vendor name or vendor name specified.

Diagnosing pluggable transceivers

The system outputs alarm information for you to diagnose and troubleshoot faults of pluggable transceivers. Optical transceivers customized by H3C also support the digital diagnosis function, which enables a transceiver to monitor the main parameters such as temperature, voltage, laser bias current, TX power, and RX power. When these parameters are abnormal, you can take corresponding measures to prevent transceiver faults.

Follow these steps to display pluggable transceiver information:

To do...	Use the command...	Remarks
Display the current alarm information of the pluggable transceiver(s)	display transceiver alarm interface [<i>interface-type interface-number</i>]	Available for all pluggable transceivers
Display the currently measured value of the digital diagnosis parameters of the anti-spoofing optical transceiver(s) customized by H3C	display transceiver diagnosis interface [<i>interface-type interface-number</i>]	Available for anti-spoofing pluggable optical transceiver(s) customized by H3C only

Displaying the Device Management Configuration

To do...	Use the command...	Remarks
Display the APP to be adopted at next startup	display boot-loader [<i>unit unit-id</i>]	Available in any view.
Display the module type and operating status of each board	display device [<i>manuinfo</i> [<i>unit unit-id</i>] <i>unit unit-id</i>]	
Display CPU usage of a switch	display cpu [<i>unit unit-id</i>]	
Display the operating status of the fan	display fan [<i>unit unit-id</i> [<i>fan-id</i>]]	
Display memory usage of a switch	display memory [<i>unit unit-id</i> <i>limit</i>]	
Display the operating status of the power supply	display power [<i>unit unit-id</i> [<i>power-id</i>]]	
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 { <i>fabric</i> <i>unit unit-id</i> } [<i>interface interface-type interface-number</i>] [<i>module-name</i>]	
Display enabled debugging on all switches in the fabric by modules	display debugging fabric by-module	

To do...	Use the command...	Remarks
Display patch state information	display patch-information	

Remote Switch APP Upgrade Configuration Example

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 Boot ROM 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.

Network diagram

Figure 4-2 Network diagram for FTP configuration



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 *Login Operation* part of this manual 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:
<Sysname>



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.

```
<Sysname> 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
```

```
<Sysname>
```

- 8) Upgrade the Boot ROM.

```
<Sysname> 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.

```
<Sysname> boot boot-loader switch.bin
```

```
The specified file will be booted next time on unit 1!
```

```
<Sysname> display boot-loader
```

```
Unit 1:
```

```
The current boot app is: switch.bin
```

```
The main boot app is: switch.bin
```

```
The backup boot app is:
```

- # Reboot the switch to upgrade the Boot ROM and host software of the switch.

```
<Sysname> reboot
```

```
Start to check configuration with next startup configuration file,  
please wait.....
```

This command will reboot the device. Current configuration may be lost in next startup if you continue. Continue? [Y/N] y
This will reboot device. Continue? [Y/N] y

5 Scheduled Task Configuration

What Is a Scheduled Task

A scheduled task defines a command or a group of commands and when such commands will be executed. It allows a device to execute specified command(s) at a time when no person is available to maintain the device.

With a scheduled task configured, the device checks the configured task list every minute; if the device finds that the time to execute a command is reached, it automatically executes the command.

Configuring a Scheduled Task

Configuration prerequisites

Note the following when configuring a scheduled task:

- The commands in a scheduled task must be in the same view.
- You can specify up to ten commands in one scheduled task. To execute more than ten commands, you can specify multiple scheduled tasks.

Configuring a scheduled task to be executed at a specified time

Follow these steps to configure a scheduled task that will be executed at a specified time

To do...		Use the command...	Description
Enter system view		system-view	—
Create a scheduled task, and enter scheduled task view		job <i>job-name</i>	Required
Configure the view where the specified commands are to be executed		view <i>view</i>	Required You can specify only one view for each scheduled task
Configure a scheduled task	Execute the task repeatedly within a specified time period	time <i>time-id</i> { one-off repeating } at <i>time</i> [week-day <i>week-daylist</i> month-date <i>month-day</i>] command <i>command</i>	Use either command.
	Execute the task at the specified time	time <i>time-id</i> at <i>time date</i> command <i>command</i>	
Display configuration of a specified scheduled task		display job [<i>job-name</i>]	Available in any view



Note

Modification of the system time will affect the execution of a scheduled task.

Configuring a scheduled task to be executed after a delay time

Follow these steps to configure a scheduled task that will be executed after a delay time

To do...	Use the command...	Description
Enter system view	system-view	—
Create a scheduled task, and enter scheduled task view	job <i>job-name</i>	Required
Configure the view where the specified commands are to be executed	view <i>view</i>	Required You can specify only one view for each scheduled task
Configure a scheduled task to be executed after a delay time	time <i>time-id</i> { one-off repeating } delay <i>time</i> command <i>command</i>	Required
Display configuration of a specified scheduled task	display job [<i>job-name</i>]	Available in any view



Note

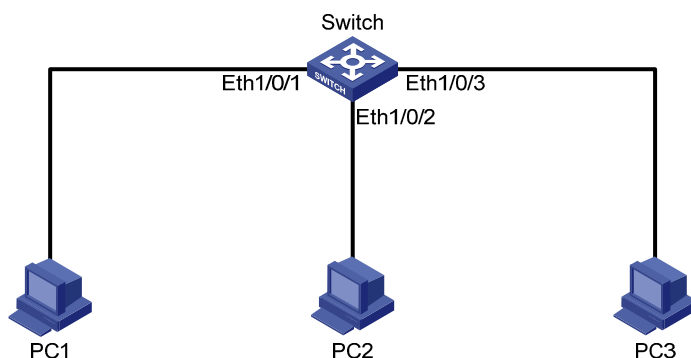
A scheduled task with a delay time configured will still be executed after the specified delay time even if the system time is modified.

Scheduled Task Configuration Example

Network requirements

Configure Switch so that the PC connected to the port of Switch is available from eight AM to six PM from Monday to Friday.

Figure 5-1 Network diagram for scheduled task configuration



Configuration procedure

```
<Switch> system-view
```

Create scheduled task pc1, and enter scheduled task view.

```
[Switch] job pc1
```

Configure the view where the specified command to be executed as Ethernet interface view.

```
[Switch-job-pc1] view Ethernet1/0/1
```

Configure the scheduled task so that the Ethernet port can be enabled on Switch at eight AM from Monday to Friday.

```
[Switch-job-pc1] time 1 repeating at 8:00 week-day Mon Tue Wed Thu Fri command undo shutdown
```

Configure the scheduled task so that the Ethernet port can be disabled on Switch at six PM from Monday to Friday.

```
[Switch-job-pc1] time 2 repeating at 18:00 week-day Mon Tue Wed Thu Fri command shutdown
```

```
[Switch-job-pc1] quit
```

Create scheduled task phone2, phone3, and Configure the scheduled task so that the Ethernet port can be enabled on Switch at eight AM from Monday to Friday.

```
[Switch] job pc2
```

```
[Switch-job-pc2] view Ethernet1/0/2
```

```
[Switch-job-pc2] time 1 repeating at 8:00 week-day Mon Tue Wed Thu Fri command undo shutdown
```

```
[Switch-job-pc2] time 2 repeating at 18:00 week-day Mon Tue Wed Thu Fri command shutdown
```

```
[Switch-job-pc2] quit
```

```
[Switch] job pc3
```

```
[Switch-job-pc3] view Ethernet1/0/3
```

```
[Switch-job-pc3] time 1 repeating at 8:00 week-day Mon Tue Wed Thu Fri command undo shutdown
```

```
[Switch-job-pc3] time 2 repeating at 18:00 week-day Mon Tue Wed Thu Fri command shutdown
```

```
[Switch-job-pc3] quit
```

Display the information about the scheduled task.

```
[Switch] display job
```

Job name: pc1

Specified view: Ethernet1/0/1

Time 1: Execute command undo shutdown at 08:00 Mondays Tuesdays Wednesdays Thursdays Fridays

Time 2: Execute command shutdown at 18:00 Mondays Tuesdays Wednesdays Thursdays Fridays

Job name: pc2

Specified view: Ethernet1/0/2

Time 1: Execute command undo shutdown at 08:00 Mondays Tuesdays Wednesdays Thursdays Fridays

Time 2: Execute command shutdown at 18:00 Mondays Tuesdays Wednesdays Thursdays Fridays

Job name: pc3

Specified view: Ethernet1/0/3

Time 1: Execute command undo shutdown at 08:00 Mondays Tuesdays Wednesdays Thursdays Fridays

Time 2: Execute command shutdown at 18:00 Mondays Tuesdays Wednesdays Thursdays Fridays

Table of Contents

1 VLAN-VPN Configuration	1-1
VLAN-VPN Overview	1-1
Introduction to VLAN-VPN	1-1
Implementation of VLAN-VPN	1-2
Configuring the TPID for VLAN-VPN Packets	1-2
Inner-to-Outer Tag Priority Replicating and Mapping	1-3
Transparent IGMP Message Transmission on a VLAN-VPN Port	1-3
VLAN-VPN Configuration	1-3
VLAN-VPN Configuration Task List	1-3
Enabling the VLAN-VPN Feature for a Port	1-4
Configuring the TPID Value for VLAN-VPN Packets on a Port	1-4
Configuring the Inner-to-Outer Tag Priority Replicating and Mapping Feature	1-5
Enabling Transparent IGMP Message Transmission on a VLAN-VPN Port	1-5
Displaying and Maintaining VLAN-VPN Configuration	1-6
VLAN-VPN Configuration Example	1-6
Transmitting User Packets through a Tunnel in the Public Network by Using VLAN-VPN	1-6
2 Selective QinQ Configuration	2-1
Selective QinQ Overview	2-1
Selective QinQ Overview	2-1
MAC Address Replicating	2-2
Selective QinQ Configuration	2-3
Selective QinQ Configuration Task List	2-3
Enabling the Selective QinQ Feature for a Port	2-3
Enabling the Inter-VLAN MAC Address Replicating Feature	2-4
Selective QinQ Configuration Example	2-4
Processing Private Network Packets by Their Types	2-4
3 BPDU Tunnel Configuration	3-1
BPDU Tunnel Overview	3-1
Introduction to the BPDU Tunnel Feature	3-1
BPDU Tunnel Fundamental	3-1
BPDU Tunnel Configuration	3-3
Configuration Prerequisites	3-3
Configuring a BPDU Tunnel	3-3
Displaying and Maintaining BPDU Tunnel Configuration	3-4
BPDU Tunnel Configuration Example	3-4
Transmitting STP Packets Through a Tunnel	3-4

1 VLAN-VPN Configuration

When configuring VLAN-VPN, go to these sections for information you are interested in:

- [VLAN-VPN Overview](#)
- [VLAN-VPN Configuration](#)
- [Displaying and Maintaining VLAN-VPN Configuration](#)
- [VLAN-VPN Configuration Example](#)

The function of transparent IGMP message transmission on a VLAN-VPN port is added. For more information, refer to [Enabling Transparent IGMP Message Transmission on a VLAN-VPN Port](#).

VLAN-VPN Overview

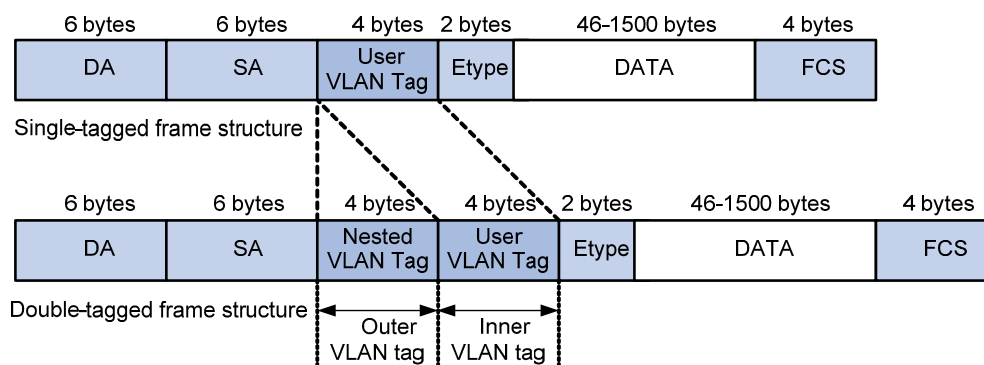
Introduction to VLAN-VPN

Virtual private network (VPN) is a new technology that emerges with the expansion of the Internet. It can be used for establishing private networks over the public network. With VPN, you can specify to process packets on the client or the access end of the service provider in specific ways, establish dedicated tunnels for user traffic on public network devices, and thus improve data security.

VLAN-VPN feature is a simple yet flexible Layer 2 tunneling technology. It tags private network packets with outer VLAN tags, thus enabling the packets to be transmitted through the service providers' backbone networks with both inner and outer VLAN tags. In public networks, packets of this type are transmitted by their outer VLAN tags (that is, the VLAN tags of public networks), and the inner VLAN tags are treated as part of the payload.

[Figure 1-1](#) shows the structure of single-tagged and double-tagged Ethernet frames.

Figure 1-1 Single-tagged frame structure vs. double-tagged Ethernet frame structure



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 through manual configuration. That is, signaling protocol-related configuration is not needed.

The VLAN-VPN feature 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.
- Provides simple Layer 2 VPN solutions for small-sized MANs or intranets.

Implementation of VLAN-VPN

With the VLAN-VPN feature enabled, no matter whether or not a received packet already carries a VLAN tag, the switch will tag the received packet with the default VLAN tag of the receiving port and add the source MAC address to the MAC address table of the default VLAN. When a packet reaches a VLAN-VPN-enabled port:

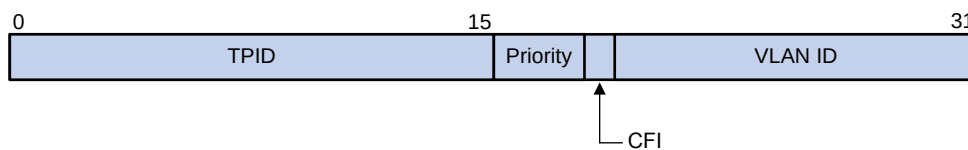
- If the packet already carries a VLAN tag, the packet becomes a dual-tagged packet.
- Otherwise, the packet becomes a packet carrying the default VLAN tag of the port.

Configuring the TPID for VLAN-VPN Packets

A VLAN tag uses the tag protocol identifier (TPID) field to identify the protocol type of the tag. The value of this field is 0x8100 for IEEE 802.1Q.

[Figure 1-2](#) illustrates the structure of the IEEE 802.1Q VLAN tag in an Ethernet frame.

Figure 1-2 The structure of the VLAN tag in an Ethernet frame



An S3600 switch determines whether a received frame is VLAN tagged by comparing its own TPID with the TPID field in the received frame. If they match, the frame is considered as a VLAN tagged frame. If not, the switch tags the frame with the default VLAN tag of the receiving port.

By default, S3600 series switches adopt the IEEE 802.1Q TPID value 0x8100. Some vendors, however, use other TPID values such as 0x9100. For compatibility with these systems, the S3600 series switches allow you to change the TPID that a port uses when tagging a received VLAN-VPN frame as needed. When doing that, you should set the same TPID on both the customer-side port and the service provider-side port.

The TPID in an Ethernet frame has the same position with the protocol type field in a frame without a VLAN tag. To avoid problems in packet forwarding and handling, you cannot set the TPID value to any of the values in the table below.

Table 1-1 Commonly used protocol type values in Ethernet frames

Protocol type	Value
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848

Protocol type	Value
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1x	0x888E

Inner-to-Outer Tag Priority Replicating and Mapping

As shown in [Figure 1-2](#), the user priority field is the 802.1p priority of the tag. The value of this 3-bit field is in the range 0 to 7. By configuring inner-to-outer tag priority replicating or mapping for a VLAN-VPN-enabled port, you can replicate the inner tag priority to the outer tag or assign outer tags of different priorities to packets according to their inner tag priorities.

Refer to *QoS-QoS Profile* part for information about priority.

Transparent IGMP Message Transmission on a VLAN-VPN Port



Note

For detailed information about IGMP messages and how a switch processes IGMP messages of different types, refer to the *Multicast* module in this manual.

For a VLAN-VPN-disabled port, the switch transparently transmits an IGMP message received on the port within the VLAN that the IGMP message belongs to. For the switch to transparently transmit an IGMP message received on a VLAN-VPN port in the outer VLAN, you must enable transparent IGMP message transmission on the port.

VLAN-VPN Configuration

VLAN-VPN Configuration Task List

Complete the following tasks to configure VLAN-VPN:

Task	Remarks
Enabling the VLAN-VPN Feature for a Port	Required
Configuring the TPID Value for VLAN-VPN Packets on a Port	Optional
Configuring the Inner-to-Outer Tag Priority Replicating and Mapping Feature	Optional
Enabling Transparent IGMP Message Transmission on a VLAN-VPN Port	Optional



Caution

As IRF fabric is mutually exclusive with VLAN-VPN, make sure that IRF fabric is disabled on the switch before performing any of the configurations listed in the above table. For information about IRF fabric, refer to *IRF Fabric Configuration* in this manual.

Enabling the VLAN-VPN Feature for a Port

Follow these steps to enable the VLAN-VPN feature for a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the VLAN-VPN feature on the port	vlan-vpn enable	Required By default, the VLAN-VPN feature is disabled on a port.

Configuring the TPID Value for VLAN-VPN Packets on a Port

For your device to correctly identify the VLAN tagged frames from the public network, make sure that the TPID you will use is the same as that used on the peer device in the public network.

Follow these steps to configure the TPID for VLAN-VPN packets on a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Set the TPID value on the port	vlan-vpn tpid <i>value</i>	Required Do not set the TPID value to any of the protocol type values listed in Table 1-1 . For H3C series switches, the TPID defaults to 0x8100.



Note

- Besides the default TPID 0x8100, you can configure only one TPID value on an S3600 switch.
- For the S3600 series to exchange packets with the public network device properly, you should configure the TPID value used by the public network device on both the customer-side port and the service provider-side port.

Configuring the Inner-to-Outer Tag Priority Replicating and Mapping Feature

Make sure that the VLAN-VPN feature is enabled on a port before configuring the inner-to-outer tag priority replicating and mapping feature.

Follow these steps to configure the inner-to-outer tag priority replicating and mapping feature:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable the inner-to-outer tag priority replicating feature	vlan-vpn inner-cos-trust enable	Either of the two configurations is required.
Enable the inner-to-outer tag priority mapping feature and create a priority mapping	vlan-vpn priority <i>old-priority</i> remark <i>new-priority</i>	By default, neither the inner-to-outer tag priority replicating feature nor the inner-to-outer tag priority mapping feature is enabled.



Caution

- If you have configured the port priority (refer to *QoS-QoS Profile Configuration* part in this manual), you will be prompted that the port priority configured for the current port gets invalid after you enable the inner-to-outer tag priority replicating feature.
- The inner-to-outer tag priority replicating feature is mutually exclusive with the inner-to-outer tag priority mapping feature.

Enabling Transparent IGMP Message Transmission on a VLAN-VPN Port

Follow these steps to enable transparent IGMP message transmission on a VLAN-VPN port:

To do...	Use the command...	Description
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable transparent IGMP message transmission on the VLAN-VPN port	igmp transparent enable	Required By default, transparent IGMP message transmission is disabled on a VLAN-VPN port.



Caution

- If your switch is required to process the IGMP messages received on a VLAN-VPN port (for example, because IGMP or IGMP snooping is enabled on the port), you must disable transparent IGMP message transmission on the port so that the switch can process the IGMP messages normally.
 - Do not enable transparent IGMP message transmission on a port without VLAN-VPN enabled.
-

Displaying and Maintaining VLAN-VPN Configuration

To do...	Use the command...	Remarks
Display the VLAN-VPN configurations of all the ports	display port vlan-vpn	Available in any view

VLAN-VPN Configuration Example

Transmitting User Packets through a Tunnel in the Public Network by Using VLAN-VPN

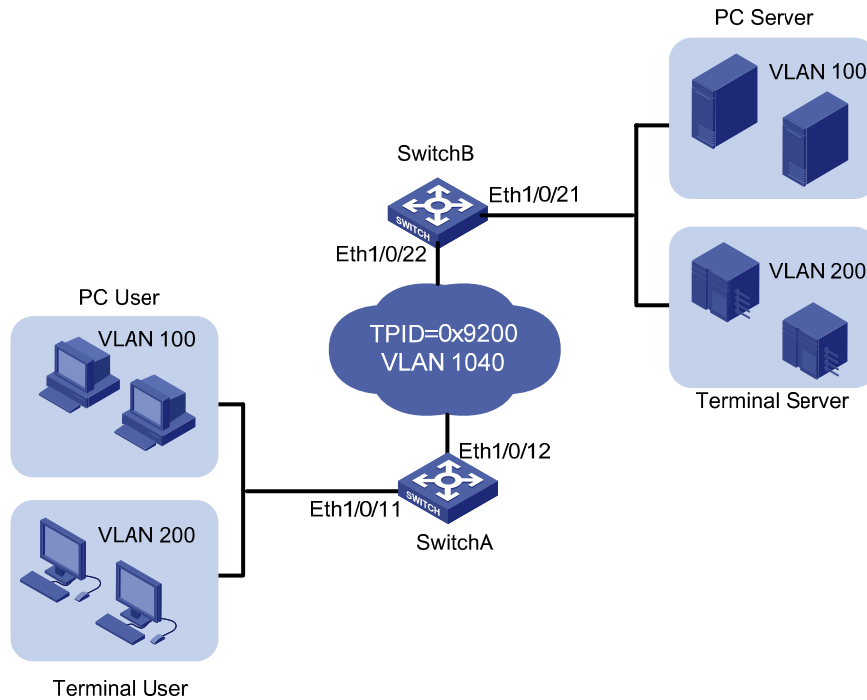
Network requirements

As shown in [Figure 1-3](#), Switch A and Switch B are both S3600 series switches. They connect the users to the servers through the public network.

- PC users and PC servers are in VLAN 100 created in the private network, while terminal users and terminal servers are in VLAN 200, which is also created in the private network. The VLAN VPN connection is established in VLAN 1040 of the public network.
- Switches of other vendors' are used in the public network. They use the TPID value 0x9200.
- Employ VLAN-VPN on Switch A and Switch B to enable the PC users and PC servers to communicate with each other through a VPN, and employ VLAN-VPN on Switch A and Switch B to enable the Terminal users and Terminal servers to communicate with each other through a VPN.

Network diagram

Figure 1-3 Network diagram for VLAN-VPN configuration



Configuration procedure

- Configure Switch A.

Enable the VLAN-VPN feature on Ethernet 1/0/11 of Switch A and tag the packets received on this port with the tag of VLAN 1040 as the outer VLAN tag.

```
<SwitchA> system-view
[SwitchA] vlan 1040
[SwitchA-vlan1040] port Ethernet 1/0/11
[SwitchA-vlan1040] quit
[SwitchA] interface Ethernet 1/0/11
[SwitchA-Ethernet1/0/11] vlan-vpn enable
[SwitchA-Ethernet1/0/11] quit
```

Set the TPID value of Ethernet 1/0/12 to 0x9200 (for intercommunication with the devices in the public network) and configure the port as a trunk port permitting packets of VLAN 1040.

```
[SwitchA] interface Ethernet 1/0/12
[SwitchA-Ethernet1/0/12] vlan-vpn tpid 9200
[SwitchA-Ethernet1/0/12] port link-type trunk
[SwitchA-Ethernet1/0/12] port trunk permit vlan 1040
```

- Configure Switch B.

Enable the VLAN-VPN feature on Ethernet 1/0/21 of Switch B and tag the packets received on this port with the tag of VLAN 1040 as the outer VLAN tag.

```
<SwitchB> system-view
[SwitchB] vlan 1040
[SwitchB-vlan1040] port Ethernet 1/0/21
[SwitchB-vlan1040] quit
```



```
[SwitchB] interface Ethernet 1/0/21
[SwitchB-Ethernet1/0/21] vlan-vpn enable
```

Set the TPID value of Ethernet1/0/22 to 0x9200 (for intercommunication with the devices in the public network) and set the port as a trunk port permitting packets of VLAN 1040.

```
[SwitchB-Ethernet1/0/22] vlan-vpn tpid 9200
[SwitchB-Ethernet1/0/22] quit
[SwitchB] interface Ethernet 1/0/21
[SwitchB-Ethernet1/0/22] port link-type trunk
[SwitchB-Ethernet1/0/22] port trunk permit vlan 1040
```



Note

- Do not configure VLAN 1040 as the default VLAN of Ethernet 1/0/12 of Switch A and Ethernet 1/0/22 of Switch B. Otherwise, the outer VLAN tag of a packet will be removed during transmission.
- In this example, both Ethernet1/0/11 of Switch A and Ethernet1/0/21 of Switch B are access ports. In cases where the ports are trunk ports or hybrid ports, you need to configure the two ports to remove the outer VLAN tags before transmitting packets of VLAN 1040. Refer to *VLAN* in this manual for detailed configuration.

-
- Configure the devices in the public network

As the devices in the public network are from other vendors, only the basic principles are introduced here. That is, you need to configure the devices connecting to Ethernet 1/0/12 of Switch A and Ethernet 1/0/22 of Switch B to permit the corresponding ports to transmit tagged packets of VLAN 1040.

Data transfer process

The following describes how a packet is forwarded from Switch A to Switch B in this example.

- 1) As Ethernet 1/0/11 of Switch A is a VLAN-VPN port, when a packet from the customer's network side reaches this port, it is tagged with the default VLAN tag of the port (VLAN 1040).
- 2) The TPID value of the outer VLAN tag is set to 0x9200 before the packet is forwarded to the public network through Ethernet1/0/12 of Switch A.
- 3) The outer VLAN tag of the packet remains unchanged while the packet travels in the public network, till it reaches Ethernet1/0/22 of Switch B.
- 4) After the packet reaches Switch B, it is forwarded through Ethernet1/0/21 of Switch B. As the port belongs to VLAN 1040 and is an access port, the outer VLAN tag (the tag of VLAN 1040) of the packet is removed before the packet is forwarded, which restores the packet to a packet tagged with only the private VLAN tag and enables it to be forwarded to its destination networks.
- 5) It is the same case when a packet travels from Switch B to Switch A.

2 Selective QinQ Configuration

When configuring selective QinQ, go to these sections for information you are interested in:

- [Selective QinQ Overview](#)
- [Selective QinQ Configuration](#)
- [Selective QinQ Configuration Example](#)

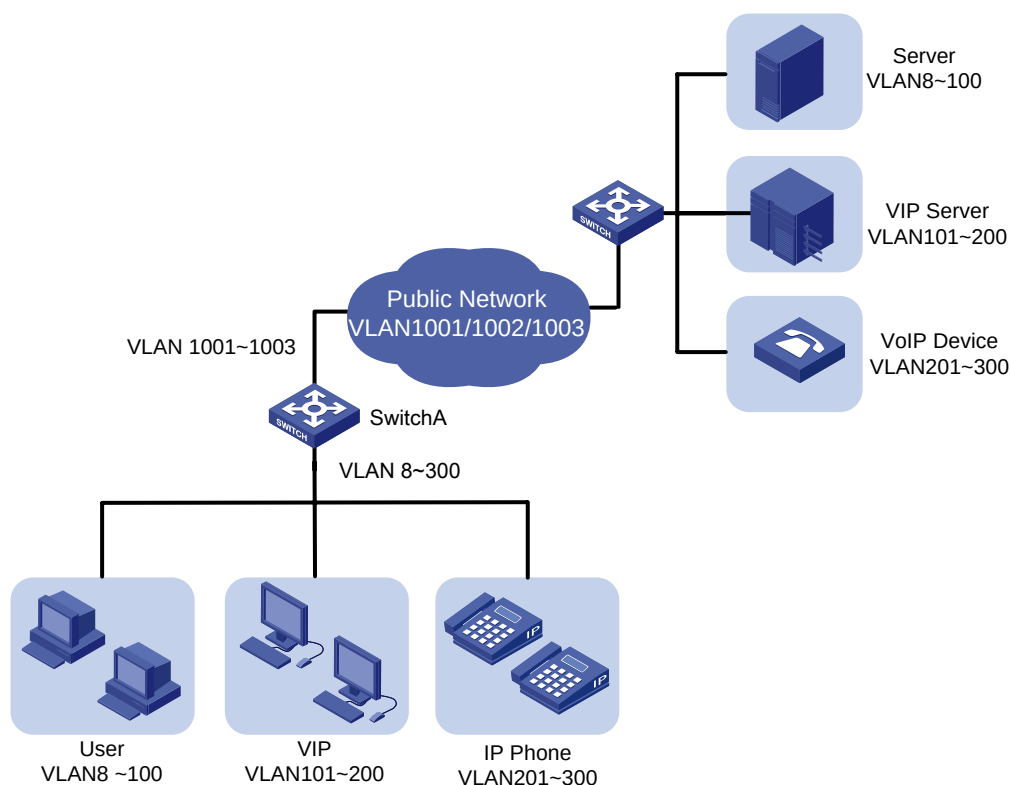
Selective QinQ Overview

Selective QinQ Overview

Selective QinQ is an enhanced application of the VLAN-VPN feature. With the selective QinQ feature, you can configure inner-to-outer VLAN tag mapping, according to which you can add different outer VLAN tags to the packets with different inner VLAN tags.

The selective QinQ feature makes the service provider network structure more flexible. You can classify the terminal users on the port connecting to the access layer device according to their VLAN tags, and add different outer VLAN tags to these users. In the public network, you can configure QoS policies based on outer VLAN tags to assign different priorities to different packets, thus providing differentiated services. See [Figure 2-1](#) for details.

Figure 2-1 Diagram for a selective QinQ implementation



In this implementation, Switch A is an access device of the service provider. The users connecting to it include common customers (in VLAN 8 to VLAN 100), VIPs (in VLAN 101 to VLAN 200), and IP

telephone users (in VLAN 201 to VLAN 300). Packets of all these users are forwarded by Switch A to the public network.

After the selective QinQ feature and the inner-to-outer tag mapping feature are enabled on the port connecting Switch A to these users, the port will add different outer VLAN tags to the packets according to their inner VLAN tags. For example, you can configure to add the tag of VLAN 1002 to the packets of IP telephone users in VLAN 201 to VLAN 300 and forward the packets to the VoIP device, which is responsible for processing IP telephone services.

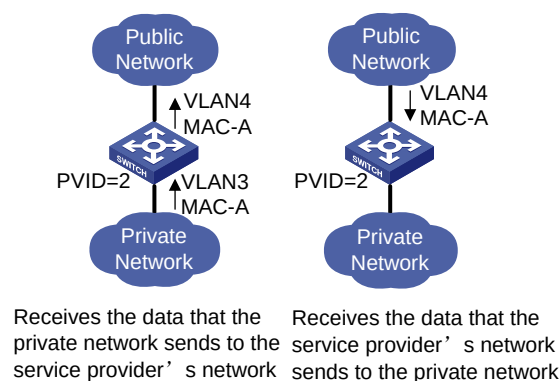
To guarantee the quality of voice packet transmission, you can configure QoS policies in the public network to reserve bandwidth for packets of VLAN 1002 and forward them preferentially.

In this way, you can configure different forwarding policies for data of different type of users, thus improving the flexibility of network management. On the other hand, network resources are well utilized, and users of the same type are also isolated by their inner VLAN tags. This helps to improve network security.

MAC Address Replicating

Like the VLAN-VPN feature, a port with the selective QinQ enabled adds the source MAC addresses of user packets to the MAC address table of the default VLAN on the port. However, the port with selective QinQ enabled can insert an outer VLAN tag other than that of the default VLAN to the packets. Thus, when packets are forwarded from the service provider to users, they may be broadcast if their destination MAC addresses cannot be found in the MAC address table of the outer VLANs.

Figure 2-2 Learn MAC addresses of selective QinQ packets



As shown in [Figure 2-2](#), the default VLAN of the port used to receive packets is VLAN 2. The port is configured to receive packets of VLAN 3, tag the received packets with the outer tag of VLAN 4, and add the source MAC addresses (MAC-A) of the packets to the MAC address table of its default VLAN (VLAN 2).

When a response packet is returned to the device from VLAN 4 of the service provider network, the device searches the outbound port for MAC-A in the MAC address table of VLAN 4. However, because the corresponding entry is not added to the MAC address table of VLAN 4, this packet is considered to be a unicast packet with unknown destination MAC address. As a result, this packet will be broadcast to all the ports in VLAN 4, which wastes the network resources and incurs potential security risks.

The S3600 series Ethernet switches provide the inter-VLAN MAC address replicating feature, which can replicate the entries in the MAC address table of the default VLAN to that of the VLAN corresponding to the outer tag. With the inter-VLAN MAC address replicating feature enabled, when a device receives a packet from the service provider network, this device will find the path for the packet

by searching the MAC address table of the VLAN corresponding to the outer tag and unicast the packet. Thus, packet broadcast is reduced in selective QinQ applications.

Likewise, the entries in the MAC address table of the outer VLAN can also be replicated to that of the default VLAN on a port, through which the outbound port to the service provider network can be determined through the MAC address table of the default VLAN and user packets destined for the service provider can be unicast.

Selective QinQ Configuration

Selective QinQ Configuration Task List

Complete the following tasks to configure selective QinQ:

Task	Remarks
Enabling the Selective QinQ Feature for a Port	Required
Enabling the Inter-VLAN MAC Address Replicating Feature	Optional



Caution

If IRF Fabric has been enabled on a device, you cannot enable the VLAN-VPN feature and the selective QinQ feature on any port of the device.

Enabling the Selective QinQ Feature for a Port

The following configurations are required for the selective QinQ feature:

- Enabling the VLAN-VPN feature on the current port
- Configuring the current port to permit packets of specific VLANs (the VLANs whose tags are to be used as the outer VLAN tags are required)

Follow these steps to enable the selective QinQ feature:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the outer VLAN tag and enter QinQ view	vlan-vpn vid <i>vlan-id</i>	Required
Configure to add outer VLAN tags to the packets with the specific inner VLAN tags	raw-vlan-id inbound <i>vlan-id-list</i>	Required By default, the feature of adding an outer VLAN tag to the packets with the specific inner VLAN tags is disabled.



Note

Do not enable both the selective QinQ function and the DHCP snooping function on a switch. Otherwise, the DHCP snooping function may operate improperly.

Enabling the Inter-VLAN MAC Address Replicating Feature

Follow these steps to enable the inter-VLAN MAC address replicating feature:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the inter-VLAN MAC address replicating feature	mac-address-mapping <i>index</i> source-vlan <i>source-vlan-id-list</i> destination-vlan <i>dest-vlan-id</i>	Required By default, the inter-VLAN MAC address replicating feature is disabled.



Caution

- On a port, the inter-VLAN MAC address replicating feature can be configured only once for a destination VLAN. If the configuration needs to be modified, you need to remove the existing configuration first.
- With the inter-VLAN MAC address replicating feature disabled, all the MAC address entries that the destination VLAN learns from the other VLANs through this function are removed.
- MAC address entries obtained through the inter-VLAN MAC address replicating feature cannot be removed manually. To remove a MAC address entry of this kind, you need to disable the inter-VLAN MAC address replicating feature first.
- VLAN 4093 is a special VLAN reserved for the IRF fabric feature. It can not serve as the destination VLAN of the inter-VLAN MAC address replicating feature to receive MAC address entries from the other VLANs.

Selective QinQ Configuration Example

Processing Private Network Packets by Their Types

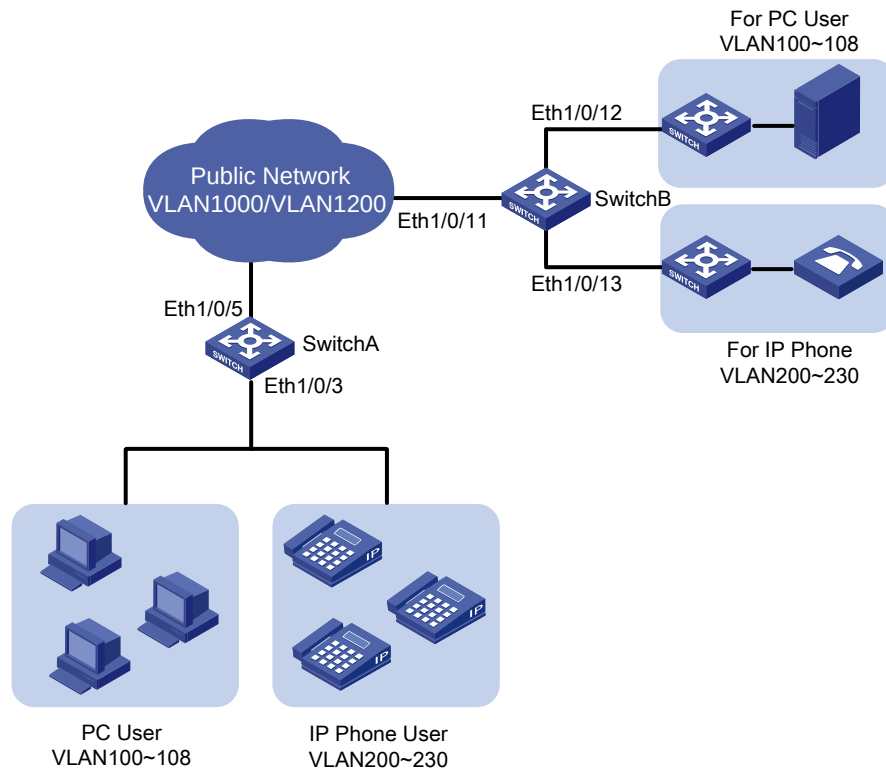
Network requirements

- Ethernet 1/0/3 of Switch A provides public network access for PC users and IP phone users. PC users belong to VLAN 100 through VLAN 108, and IP phone users belong to VLAN 200 through VLAN 230. Ethernet 1/0/5 of Switch A is connected to the public network. The peer end of Switch A is Switch B.
- Ethernet 1/0/11 of Switch B is connected to the public network. Ethernet 1/0/12 and Ethernet1/0/13 of Switch B provide network access for PC servers belonging to VLAN 100 through VLAN 108 and voice gateways (for IP phone users) belonging to VLAN 200 through VLAN 230 respectively.

- The public network permits packets of VLAN 1000 and VLAN 1200. Apply QoS policies for these packets to reserve bandwidth for packets of VLAN 1200. That is, packets of VLAN 1200 have higher transmission priority over packets of VLAN 1000.
- Employ the selective QinQ feature on Switch A and Switch B to differentiate traffic of PC users from that of IP phone users, for the purpose of using QoS policies to guarantee higher priority for voice traffic.
- To reduce broadcast packets in the network, enable the inter-VLAN MAC address replicating feature for selective QinQ.

Network diagram

Figure 2-3 Network diagram for selective QinQ configuration



Configuration procedure

- Configure Switch A.

Create VLAN 1000, VLAN 1200 and VLAN 5 (the default VLAN of Ethernet 1/0/3) on SwitchA.

```
<SwitchA> system-view
[SwitchA] vlan 1000
[SwitchA-vlan1000] quit
[SwitchA] vlan 1200
[SwitchA-vlan1200] quit
[SwitchA] vlan 5
[SwitchA-vlan5] quit
```

Configure Ethernet 1/0/5 as a hybrid port and configure it not to remove VLAN tags when forwarding packets of VLAN 5, VLAN 1000, and VLAN 1200.

```
[SwitchA] interface Ethernet 1/0/5
[SwitchA-Ethernet1/0/5] port link-type hybrid
```

```
[SwitchA-Ethernet1/0/5] port hybrid vlan 5 1000 1200 tagged
```

```
[SwitchA-Ethernet1/0/5] quit
```

Configure Ethernet 1/0/3 as a hybrid port and configure VLAN 5 as its default VLAN. Configure Ethernet 1/0/3 to remove VLAN tags when forwarding packets of VLAN 5, VLAN 1000, and VLAN 1200.

```
[SwitchA] interface Ethernet 1/0/3
```

```
[SwitchA-Ethernet1/0/3] port link-type hybrid
```

```
[SwitchA-Ethernet1/0/3] port hybrid pvid vlan 5
```

```
[SwitchA-Ethernet1/0/3] port hybrid vlan 5 1000 1200 untagged
```

Enable the VLAN-VPN feature on Ethernet 1/0/3.

```
[SwitchA-Ethernet1/0/3] vlan-vpn enable
```

Enable the selective QinQ feature on Ethernet 1/0/3 to tag packets of VLAN 100 through VLAN 108 with the tag of VLAN 1000 as the outer VLAN tag, and tag packets of VLAN 200 through VLAN 230 with the tag of VLAN 1200 as the outer VLAN tag.

```
[SwitchA-Ethernet1/0/3] vlan-vpn vid 1000
```

```
[SwitchA-Ethernet1/0/3-vid-1000] raw-vlan-id inbound 100 to 108
```

```
[SwitchA-Ethernet1/0/3-vid-1000] quit
```

```
[SwitchA-Ethernet1/0/3] vlan-vpn vid 1200
```

```
[SwitchA-Ethernet1/0/3-vid-1200] raw-vlan-id inbound 200 to 230
```

Enable the inter-VLAN MAC address replicating feature to replicate the MAC address entries of the MAC address tables of the outer VLANs to the MAC address table of the default VLAN, and replicate the MAC address entries of the MAC address table of the default VLAN to the MAC address tables of the outer VLANs.

```
[SwitchA-Ethernet1/0/3-vid-1200] quit
```

```
[SwitchA-Ethernet1/0/3] mac-address mapping 0 source-vlan 5 destination-vlan 1000
```

```
[SwitchA-Ethernet1/0/3] mac-address mapping 1 source-vlan 5 destination-vlan 1200
```

```
[SwitchA-Ethernet1/0/3] quit
```

```
[SwitchA] interface Ethernet 1/0/5
```

```
[SwitchA-Ethernet1/0/5] mac-address mapping 0 source-vlan 1000 1200 destination-vlan 5
```

After the above configuration, packets of VLAN 100 through VLAN 108 (that is, packets of PC users) are tagged with the tag of VLAN 1000 as the outer VLAN tag when they are forwarded to the public network by Switch A; and packets of VLAN 200 through VLAN 230 (that is, packets of IP phone users) are tagged with the tag of VLAN 1200 as the outer VLAN tag when they are forwarded to the public network.

- Configure Switch B.

Create VLAN 1000, VLAN 1200, VLAN 12 (the default VLAN of Ethernet1/0/12) and VLAN 13 (the default VLAN of Ethernet1/0/13) on Switch B.

```
<SwitchB> system-view
```

```
[SwitchB] vlan 1000
```

```
[SwitchB-vlan1000] quit
```

```
[SwitchB] vlan 1200
```

```
[SwitchB-vlan1200] quit
```

```
[SwitchB] vlan 12 to 13
```

Configure Ethernet 1/0/11 as a hybrid port, and configure Ethernet 1/0/11 not to remove VLAN tags when forwarding packets of VLAN 12, VLAN 13, VLAN 1000, and VLAN 1200.

```
<SwitchB> system-view
```

```
[SwitchB] interface Ethernet 1/0/11
[SwitchB-Ethernet1/0/11] port link-type hybrid
[SwitchB-Ethernet1/0/11] port hybrid vlan 12 13 1000 1200 tagged
```

Configure Ethernet1/0/12 as a hybrid port and configure VLAN 12 as its default VLAN . Configure Ethernet 1/0/12 to remove VLAN tags when forwarding packets of VLAN 12 and VLAN 1000.

```
[SwitchB] interface Ethernet 1/0/12
[SwitchB-Ethernet1/0/12] port link-type hybrid
[SwitchB-Ethernet1/0/12] port hybrid pvid vlan 12
[SwitchB-Ethernet1/0/12] port hybrid vlan 12 1000 untagged
[SwitchB-Ethernet1/0/12] quit
```

Configure Ethernet 1/0/13 as a hybrid port and configure VLAN 13 as its default VLAN . Configure Ethernet 1/0/13 to remove VLAN tags when forwarding packets of VLAN 13 and VLAN 1200.

```
[SwitchB] interface Ethernet 1/0/13
[SwitchB-Ethernet1/0/13] port link-type hybrid
[SwitchB-Ethernet1/0/13] port hybrid pvid vlan 13
[SwitchB-Ethernet1/0/13] port hybrid vlan 13 1200 untagged
```

After the above configuration, Switch B can forward packets of VLAN 1000 and VLAN 1200 to the corresponding servers through Ethernet 1/0/12 and Ethernet 1/0/13 respectively.

To make the packets from the servers be transmitted to the clients in the same way, you need to configure the selective QinQ feature and the inter-VLAN MAC address replicating feature on Ethernet 1/0/12 and Ethernet 1/0/13. The configuration on Switch B is similar to that on Switch A and is thus omitted.



Note

- The port configuration on Switch B is only an example for a specific network requirement. The key to this example is to enable the ports to receive and forward packets of specific VLANs. So you can also configure the ports as trunk ports. Refer to *VLAN Configuration* for details.
 - A selective QinQ-enabled device tags a user packet with an outer VLAN tag regardless of the VLAN tag of the user packet, so there is no need to configure user VLANs on the device.
 - Make sure the packets of the default VLAN of a selective QinQ-enabled port are permitted on both the local port and the port connecting to the public network.
-

3 BPDU Tunnel Configuration

When configuring BPDU tunnel, go to these sections for information you are interested in:

- [BPDU Tunnel Overview](#)
- [BPDU Tunnel Configuration](#)
- [Displaying and Maintaining BPDU Tunnel Configuration](#)
- [BPDU Tunnel Configuration Example](#)

BPDU Tunnel Overview

Introduction to the BPDU Tunnel Feature

Normally, Layer 2 protocols are needed in a LAN for network topology maintenance and management. For example, spanning tree protocol (STP) is used for maintaining spanning trees and preventing loops. Huawei group management protocol (HGMP) is used for managing network topology and devices in a network.

When multiple branch networks of an organization are connected together through a public network, you can combine the corresponding network nodes into one so as to maintain the branch networks as a whole. This requires the packets of some of the user's Layer 2 protocol packets be transmitted across the provider's network without getting involved in the computation of the public network.

The BPDU Tunnel feature is designed to address the above requirements. It enables some Layer 2 protocol packets of private networks to be transmitted along tunnels established in the public network.

BPDU Tunnel Fundamental

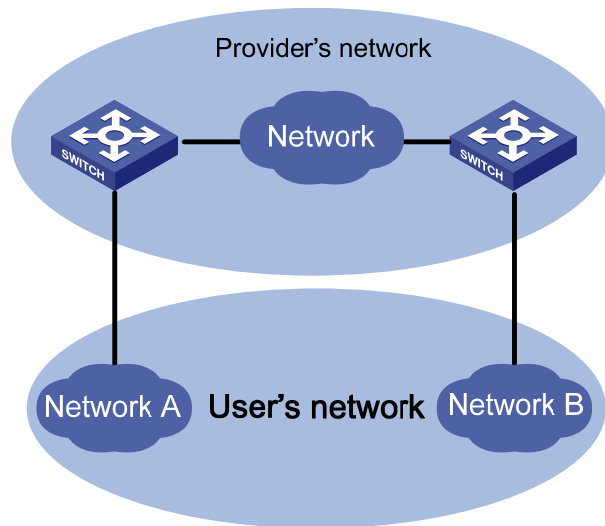
Layer 2 protocol packet identification

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 to IEEE standards carries a special destination MAC address (for example, the destination MAC address of an STP protocol packet is 0180-c200-0000) 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.

Transmitting BPDU packets transparently

As shown in [Figure 3-1](#), the network on the top is the service provider network, and the one on the bottom is a customer network. The service provider network contains edge devices connecting the customer network to the service provider network. The customer network contains Network A and Network B. You can make the BPDU packets of the customer network to be transmitted in the service provider network transparently by enabling the BPDU tunnel feature on the edge devices at both ends of the service provider network.

Figure 3-1 BPDU Tunnel network hierarchy



- When a BPDU packet coming from a customer network reaches an edge device in the service provider network, the edge device changes the destination MAC address carried in the packet from a protocol-specific MAC address to a private multicast MAC address, which can be defined using a command. A packet with this multicast address as its destination address is called a tunnel packet. In the service provider network, the tunnel packet can be forwarded as a normal data packet.
- Before the device in the service provider network forwards the packet to the destination customer network, the edge device will identify the tunnel packet, determine the packet type based on the type field in the packet, restore its destination MAC address to the original protocol-specific MAC address and then forward the packet to the access device on the user side. This ensures the packet to be forwarded is consistent with the packet before entering the tunnel. So, a tunnel here acts as a local link for user devices. It enables Layer 2 protocols to run on a virtual local network.

[Figure 3-2](#) and [Figure 3-3](#) show the structure of a BPDU packet before and after it enters a BPDU tunnel.

Figure 3-2 The structure of a BPDU packet before it enters a BPDU tunnel

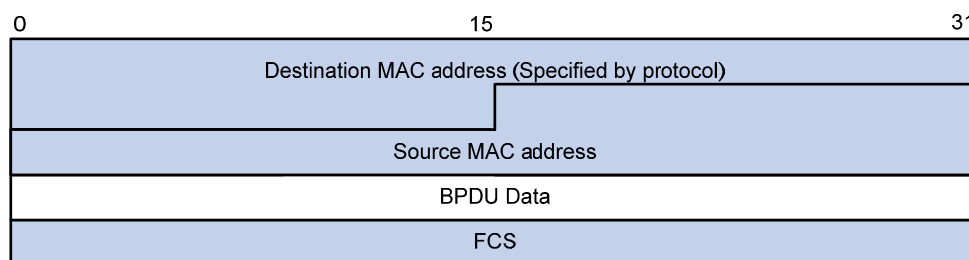
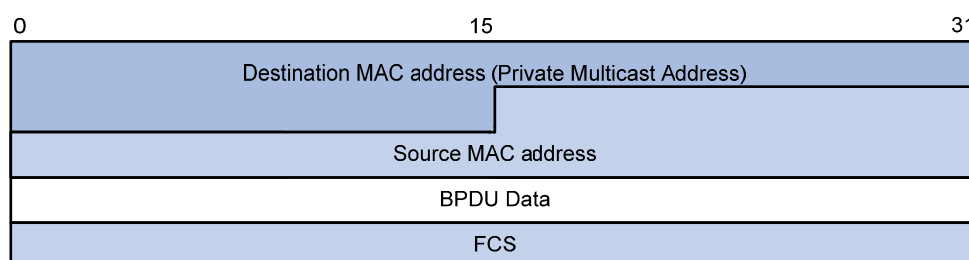


Figure 3-3 The structure of a BPDU packet after it enters a BPDU tunnel





Caution

To prevent the devices in the service provider network from processing the tunnel packets as other protocol packets, the MAC address of a tunnel packet must be a multicast address uniquely assigned to the BPDU tunnel in the service provider network.

BPDU Tunnel Configuration

You can establish BPDU tunnels between S3600 series Ethernet switches for the packets of the following protocols:

- LACP (link aggregation control protocol)
- STP (spanning tree protocol)
- HGMP-related protocols, including: NDP (neighbor discovery protocol), NTDP (neighbor topology discovery protocol), cluster MRC (cluster member remote control), and HABP (Huawei authentication bypass protocol)
- Proprietary protocols of other vendors, including CDP (CISCO discovery protocol), PAGP (port aggregation protocol), PVST (per-VLAN spanning tree), VTP (VLAN trunk protocol), and UDLD (uni-directional link discovery)

Configuration Prerequisites

The edge devices can communicate with the user devices properly.

Configuring a BPDU Tunnel

Follow these steps to configure a BPDU tunnel:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a private multicast MAC address for packets transmitted along the tunnel	bpdu-tunnel tunnel-dmac <i>mac-address</i>	Optional By default, the destination MAC address for packets transmitted along a BPDU tunnel is 010f-e200-0003.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Enable BPDU tunnel for packets of a specific protocol	bpdu-tunnel <i>protocol-type</i>	Required By default, BPDU tunnel is disabled for packets of any protocol.



Note

- The BPDU Tunnel is unavailable to all the ports of a device if the device has the fabric feature enabled on one of its ports.
- If BPDU tunnel transparent transmission is enabled for packets of a protocol, the protocol cannot be enabled on the port. For example, if you execute the **bpdu-tunnel lacp** command, the **lacp enable** command cannot be executed on the port.
- The **bpdu-tunnel stp** command is mutually exclusive with the **vlan-vpn tunnel** command. Refer to *MSTP* part of this manual for details.
- To enable BPDU tunnel transmission for PAGP packets, LACP packets and UDLD packets, make sure that the links the service provider provides are point-to-point links. Otherwise, these protocols cannot operate properly.
- Because the NDP configuration and NTDP configuration cannot be synchronized to ports in an aggregation group, make sure that NDP and NTDP are not enabled on any port in an aggregation group before enabling the service provider network to use aggregation group to transmit HGMP packets through BPDU tunnels.
- The **bpdu-tunnel cdp** command is mutually exclusive with the **voice vlan legacy** command. Refer to *Voice VLAN* part of this manual for details.
- If a BPDU-tunnel-enabled port receives a tunnel packet from the customer's network, errors occur in the network and the tunnel packet will be dropped directly.

Displaying and Maintaining BPDU Tunnel Configuration

To do...	Use the command...	Remarks
Display the private multicast MAC address used by the tunnel packets	display bpdu-tunnel	Available in any view

BPDU Tunnel Configuration Example

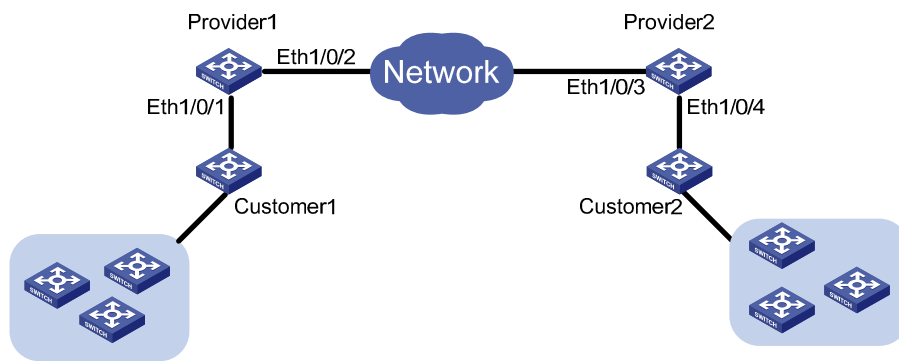
Transmitting STP Packets Through a Tunnel

Network requirements

- Customer1 and Customer2 are devices operating in a customer network; Provider1 and Provider2 are edge devices operating in the service provider network. The two devices receive data from the customer network by using Ethernet1/0/1 and Ethernet1/0/2 respectively.
- Provider1 and Provider2 are connected through trunk links, which permit packets of all VLANs.
- Enable the service provider network to transmit STP packets of the customer network through BPDU tunnel. The destination MAC address for tunnel packets is 010f-e233-8b22.
- Enable the VLAN-VPN feature for the service provider network, and enable the service provider network to use VLAN 100 to transmit data packets of the customer network.

Network diagram

Figure 3-4 Network diagram for BPDU Tunnel configuration



Configuration procedure

1) Configure Provider1.

Disable STP on Ethernet1/0/1.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp disable
```

Enable the BPDU tunnel feature for STP BPDUs on Ethernet1/0/1.

```
[Sysname-Ethernet1/0/1] bpdu-tunnel stp
```

Enable the VLAN-VPN feature on Ethernet1/0/1 and use VLAN 100 to transmit user data packets through BPDU tunnels.

```
[Sysname-Ethernet1/0/1] port access vlan 100
[Sysname-Ethernet1/0/1] vlan-vpn enable
```

Configure the destination MAC address for protocol packets transmitted through the BPDU tunnel.

```
[Sysname-Ethernet1/0/1] quit
[Sysname] bpdu-tunnel tunnel-dmac 010f-e233-8b22
```

Configure Ethernet1/0/2 as a trunk port that permits packets of all VLANs.

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

2) Configure Provider2.

Disable STP on Ethernet1/0/4.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/4
[Sysname-Ethernet1/0/4] stp disable
```

Enable BPDU tunnel for STP packets.

```
[Sysname-Ethernet1/0/4] bpdu-tunnel stp
```

Enable VLAN-VPN and use VLAN 100 to transmit user data packets through BPDU tunnels.

```
[Sysname-Ethernet1/0/4] port access vlan 100
[Sysname-Ethernet1/0/4] vlan-vpn enable
```

Configure the destination MAC address for the packets transmitted in the tunnel.

```
[Sysname-Ethernet1/0/4] quit
```

```
[Sysname] bpdu-tunnel tunnel-dmac 010f-e233-8b22
```

Configure Ethernet1/0/3 as a trunk port that permits packets of all VLANs.

```
[Sysname] interface Ethernet 1/0/3
```

```
[Sysname-Ethernet1/0/3] port link-type trunk
```

```
[Sysname-Ethernet1/0/3] port trunk permit vlan all
```

Table of Contents

1 HWPing Configuration	1-1
HWPing Overview	1-1
Introduction to HWPing	1-1
Test Types Supported by HWPing	1-2
HWPing Test Parameters	1-2
HWPing Configuration	1-4
HWPing Server Configuration	1-4
HWPing Client Configuration	1-5
Displaying HWPing Configuration	1-22
HWPing Configuration Examples	1-22
ICMP Test	1-22
DHCP Test	1-24
FTP Test	1-26
HTTP Test	1-28
Jitter Test	1-30
SNMP Test	1-32
TCP Test (Tcprivate Test) on the Specified Ports	1-33
UDP Test (Udprivate Test) on the Specified Ports	1-35
DNS Test	1-37

1 HWPing Configuration



Note

New HWPing commands are added including datafill, description, display hwping statistics, filesize, history keep-time, history-record enable, hwping-agent clear, hwping-agent max-requests, sendpacket passroute, ttl, statistics, statistics keep-time, test-time begin, and adv-factor. For description about the commands, refer to the HWPing Configuration.

When configuring HWPing, go to these sections for information you are interested in:

- [HWPing Overview](#)
- [HWPing Configuration](#)
- [HWPing Configuration Examples](#)

HWPing Overview

Introduction to HWPing

HWPing (pronounced Hua'Wei Ping) is a network diagnostic tool. It is used to test the performance of various protocols running in networks. HWPing provides more functions than the **ping** command.

- The **ping** command can only use the ICMP protocol to test the round trip time (RTT) between this end and a specified destination end for the user to judge whether the destination end is reachable.
- Besides the above function of the **ping** command, HWPing can also provide other functions, such as testing the status (open/close) of a DHCP/FTP/HTTP/SNMP server and the response time of various services.

You need to configure HWPing client and sometimes the corresponding HWPing servers as well to perform various HWPing tests.

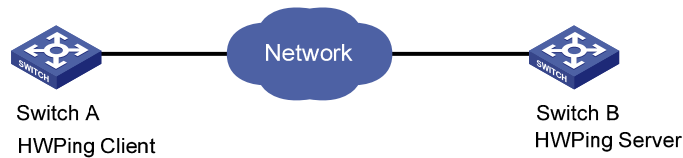
All HWPing tests are initiated by an HWPing client and you can view the test results on the HWPing client only.

When performing an HWPing test, you need to configure an HWPing test group on the HWPing client. An 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 and a test tag.

After creating an HWPing test group and configuring the test parameters, you can then perform an HWPing test by the **test-enable** command.

- Being different from the **ping** command, HWPing does not display the RTT or timeout status of each packet on the Console terminal in real time. To view the statistic results of your HWPing test operation, you need to execute the **display hwping** command.
- HWPing also allows you to set parameters for HWPing test groups, start HWPing tests and view statistical test results through a network management device.

Figure 1-1 HWPing illustration



Test Types Supported by HWPing

Among the test types supported by HWPing, only the ICMP test can be performed when IRF fabric is enabled; all other test types cannot be performed when IRF fabric is enabled.

Table 1-1 Test types supported by HWPing

Supported test types		Description
ICMP test		For these types of tests, you need to configure the HWPing client and corresponding servers.
DHCP test		
FTP test		
HTTP test		
DNS test		
SNMP test		
Jitter test		• These types of tests need the cooperation of the HWPing client and HWPing server. • Do not perform a TCP, UDP or jitter test on a well-known port (ports with a number ranging from 1 to 1023). Otherwise, your HWPing test may fail or the service corresponding to the well-known port may become unavailable.
TCP test	Tcppublic test	
	Tcprivate test	
UDP test	Udppublic test	
	Udprivate test	

HWPing Test Parameters

You need to configure corresponding test parameters for each type of HWPing test. HWPing test parameters can be configured on HWPing client only. For the configurations on the HWPing client, refer to section [HWPing Client Configuration](#).

Table 1-2 HWPing test parameters

Test parameter	Description
Destination address (destination-ip)	For a TCP/UDP/jitter test, you must specify a destination IP address, and the destination address must be the IP address of a TCP/UDP/UDP listening service configured on the HWPing server.
Destination port (destination-port)	For a tcprivate/udprivate/jitter test, you must specify a destination port number, and the destination port number must be the port number of a TCP or UDP listening service configured on the HWPing server.

Test parameter	Description
Source interface (source-interface)	- For a DHCP test, you must specify a source interface, which will be used by the HWPing client to send DHCP requests. If no source interface is specified for the DHCP test, the test will not succeed. - After a source interface is specified, the HWPing client uses this source interface to send DHCP requests during the DHCP test. - The IP address of the specified source interface will be used as the source IP address of DHCP requests.
Source address (source-ip)	For HWPing tests other than DHCP tests, you can specify a source IP address for test packets, which will be used by the server as the destination address of response packets.
Source port (source-port)	For HWPing tests other than ICMP, DHCP and DNS, you can specify a source port number for test packets, which will be used by the server as the destination port number of response packets.
Test type (test-type)	- You can use HWPing to test a variety of protocols, see Table 1-1 for details. - To perform a type of test, you must first create a test group of this type. One test group can be of only one HWPing test type. - If you modify the test type of a test group using the test-type command, the parameter settings, test results, and history records of the original test type will be all cleared.
Number of probes per test (count)	For tests except jitter test, only one test packet is sent in a probe. In a jitter test, you can use the jitter-packetnum command to set the number of packets to be sent in a probe.
Packet size (datasize)	- For ICMP/UDP/jitter test, you can configure the size of test packets. - For ICMP test, the ICMP packet size refers to the length of ECHO-REQUEST packets (excluding IP and ICMP headers)
Padding string for the test packet (datafill)	In ICMP, UDP and jitter tests, the system should stuff the data field of each transmitted ICMP message. The stuffing character string ranges from 1 to 230 characters, including spaces. If the size of a test datagram is smaller than that of the configured stuffing character string, only a portion of the string will be used for stuffing. If the size of the test datagram is larger, the string will be used cyclically for stuffing. Suppose a stuffing string, "abcde", is configured. If the test datagram size is 3, only "abc" will be used for stuffing; if it is 8, the string "abcdeabc" will be used.
Routing table bypass(sendpacket passroute)	With routing table bypass, a remote host can bypass the normal routing tables and send ICMP packets directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. You can use this function when pinging a local host on a VLAN interface that has no route defined.
TTL of HWPing test packets (tll)	It is equal to the argument " -h " in a ping command.
Maximum number of history records that can be saved (history-records)	This parameter is used to specify the maximum number of history records that can be saved in a test group. When the number of saved history records exceeds the maximum number, HWPing discards some earliest records.
Automatic test interval (frequency)	This parameter is used to set the interval at which the HWPing client periodically performs the same test automatically.
Probe timeout time (timeout)	- The probe timeout timer is started after the HWPing client sends out a test packet. - This parameter is in seconds.
Type of service (tos)	Type of service is the value of the ToS field in IP header in the test packets.

Test parameter	Description
dns	This parameter is used to specify a DNS domain name in an HWPing DNS test group.
dns-server	This parameter is used to set the DNS server IP address in an HWPing DNS test group.
HTTP operation type (http-operation)	This parameter is used to set the type of HTTP interaction operation between HWPing client and HTTP server.
FTP operation type (ftp-operation)	This parameter is used to set the type of FTP interaction operation between HWPing client and FTP server.
FTP login username and password (username and password)	The two parameters are used to set the username and password to be used for FTP operation.
File name for FTP operation (filename)	Name of a file to be transferred between HWPing client and FTP server
Size of a file to be uploaded in an FTP test(filesize)	Size of a file to be uploaded in an FTP test
Number of jitter test packets to be sent per probe (jitter-packetnum)	- Jitter test is used to collect statistics about delay jitter in UDP packet transmission - In a jitter probe, the HWPing client sends a series of packets to the HWPing server at regular intervals (you can set the interval). Once receiving such a packet, the HWPing server marks it with a timestamp, and then sends it back to the HWPing client. Upon receiving a packet returned, the HWPing client computes the delay jitter time. The HWPing client collects delay jitter statistics on all the packets returned in the test. So, the more packets a jitter probe sends, the more accurate the jitter statistics is, but the longer time the jitter test costs.
Interval to send jitter test packets (jitter-interval)	Each jitter probe will send multiple UDP test packets at regular intervals (you can set the interval). The smaller the interval is, the faster the test is. But a too small interval may somewhat impact your network.
Enable the HWPing client to send Trap messages (send-trap)	- An HWPing test will generate a Trap message no matter whether the test successes or not. You can use the Trap switch to enable or disable the output of trap messages. - You can set the number of consecutive failed HWPing tests before Trap output. You can also set the number of consecutive failed HWPing probes before Trap output.

HWPing Configuration

The TCP/UDP/jitter tests need the cooperation of HWPing client and HWPing server. Other types of tests need to configure HWPing client and corresponding different servers.

You can enable both the HWPing client and HWPing server functions on the switch, that is, the switch can serve as an HWPing client and server simultaneously.

HWPing Server Configuration

The following table describes the configuration on HWPing server, which is the same for HWPing test types that need to configure HWPing server.

Follow these steps to perform HWPing server configurations:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the HWPing server function	hwping-server enable	Required Disabled by default.
Configure a UDP listening service	hwping-server udpecho <i>ip-address port-num</i>	Required for UDP and jitter tests By default, no UDP listening service is configured.
Configure a TCP listening service	hwping-server tcpconnect <i>ip-address port-num</i>	Required for TCP tests By default, no TCP listening service is configured.

Note that:

- The HWPing server function is needed only for jitter, TCP, and UDP tests.
- You can configure multiple TCP/UDP listening services on one HWPing server, with each listening service corresponding to a specific destination IP address and port number.

HWPing Client Configuration

HWPing client configuration

After HWPing client is enabled, you can create multiple test groups for different tests, without the need to enable HWPing client repeatedly for each test group.

Different types of HWPing tests are somewhat different in parameters and parameter ranges. The following text describes the configuration on HWPing client for different test types.



Note

Among the test types supported by HWPing, only the ICMP test can be performed when IRF fabric is enabled; all other test types cannot be performed when IRF fabric is enabled. With IRF fabric enabled, you are allowed to configure HWPing tests and use the **display** commands to check your configurations, but for non ICMP tests, the HWPing tests you configured cannot be executed until fabric is disabled.

1) Configuring ICMP test on HWPing client

Follow these steps to configure ICMP test on HWPing client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the HWPing client function	hwping-agent enable	Required By default, the HWPing client function is disabled.
Create an HWPing test group and enter its view	hwping <i>administrator-name</i> <i>operation-tag</i>	Required By default, no test group is configured.

To do...	Use the command...	Remarks
Configure the test type	test-type icmp	Optional By default, the test type is ICMP.
Configure the destination IP address	destination-ip <i>ip-address</i>	Required By default, no destination address is configured.
Configure the source IP address	source-ip <i>ip-address</i>	Optional By default, no source IP address is configured.
Configure the number of probes per test	count <i>times</i>	Optional By default, each test makes one probe.
Configure the packet size	datasize <i>size</i>	Optional By default, the packet size is 56 bytes.
Configure a stuffing character string	datafill <i>string</i>	Optional By default, the numbers between 0 and 255 are stuffed into datagrams in a cyclically way.
Configure a test description	description <i>string</i>	Optional By default, no description information is configured.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Optional By default, the maximum number is 50.
Enable history record	history-record enable	Optional By default, history record is not enabled.
Configure the retaining time of history record	history keep-time <i>keep-time</i>	Optional By default, the retaining time of history record is 120 minutes.
Configure statistics interval and the maximum number of retained statistics information	statistics { interval <i>interval</i> max-group <i>number</i> }	Optional By default, statistics interval is 120 minutes and up to two pieces of statistics information can be retained.
Configure the retaining time of statistics information	statistics keep-time <i>keep-time</i>	Optional By default, the retaining time of statistics information is 120 minutes.
Configure test start time and lifetime	test-time begin { <i>hh:mm:ss</i> [<i>yyyy/mm/dd</i>] now } lifetime <i>lifetime</i>	Optional By default, no test start time and lifetime is configured.
Enable routing table bypass	sendpacket passroute	Optional By default, routing table bypass is disabled.

To do...	Use the command...	Remarks
Configure the TTL	tll <i>number</i>	Optional By default, TTL is 20. The sendpacket passroute command voids the tll command.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the type of service (ToS)	tos <i>value</i>	Optional By default, the service type is zero.
Start the test	test-enable	Required
Display test results	display hwping results [<i>admin-name operation-tag</i>]	Required Available in any view.



Note

- For an HWPing ICMP test, if no IP address is configured for the source interface configured through the **source-interface** command, the test cannot be performed; if a source IP address has already been configured through the **source-ip** command, the **source-interface** command does not take effect.
- In an ICMP test, after you specify a source interface by the **source-interface** *interface-type interface-number* command, the TTL value turns to 1 automatically to test the directly connected devices.

2) Configuring DHCP test on HWPing client

Follow these steps to configure DHCP test on HWPing client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the HWPing client function	hwping-agent enable	Required By default, the HWPing client function is disabled.
Create an HWPing test group and enter its view	hwping <i>administrator-name operation-tag</i>	Required By default, no test group is configured.
Configure the test type	test-type dhcp	Required By default, the test type is ICMP.

To do...	Use the command...	Remarks
Configure the source interface	source-interface <i>interface-type</i> <i>interface-number</i>	Required You can only configure a VLAN interface as the source interface. By default, no source interface is configured.
Configure the number of probes per test	count <i>times</i>	Optional By default, each test makes one probe.
Configure a test description	description <i>string</i>	Optional By default, no description information is configured.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Optional By default, the maximum number is 50.
Enable history record	history-record enable	Optional By default, history record is not enabled.
Configure the retaining time of history record	history keep-time <i>keep-time</i>	Optional By default, the retaining time of history record is 120 minutes.
Configure statistics interval and the maximum number of retained statistics information	statistics { interval <i>interval</i> max-group <i>number</i> }	Optional By default, statistics interval is 120 minutes and up to two pieces of statistics information can be retained.
Configure the retaining time of statistics information	statistics keep-time <i>keep-time</i>	Optional By default, the retaining time of statistics information is 120 minutes.
Configure test start time and lifetime	test-time begin { <i>hh:mm:ss</i> [<i>yyyy/mm/dd</i>] now } lifetime <i>lifetime</i>	Optional By default, no test start time and lifetime is configured.
Enable routing table bypass	sendpacket passroute	Optional By default, routing table bypass is disabled.
Set the maximum number of concurrent tests	hwping-agent max-requests <i>number</i>	Optional By default, five concurrent tests are allowed.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Start the test	test-enable	Required
Display test results	display hwping results [<i>admin-name operation-tag</i>]	Required You can execute the command in any view.

3) Configuring FTP test on HWPing client

Follow these steps to configure FTP test on HWPing client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the HWPing client function	hwping-agent enable	Required By default, the HWPing client function is disabled.
Create an HWPing test group and enter its view	hwping <i>administrator-name operation-tag</i>	Required By default, no test group is configured.
Configure the test type	test-type ftp	Required By default, the test type is ICMP.
Configure the destination IP address	destination-ip <i>ip-address</i>	Required By default, no destination address is configured.
Configure the source IP address	source-ip <i>ip-address</i>	Required By default, no source IP address is configured.
Configure the source port	source-port <i>port-number</i>	Optional By default, no source port is configured.
Configure the number of probes per test	count <i>times</i>	Optional By default, each test makes one probe.
Configure a test description	description <i>string</i>	Optional By default, no description information is configured.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Optional By default, the maximum number is 50.
Enable history record	history-record enable	Optional By default, history record is not enabled.
Configure the retaining time of history record	history keep-time <i>keep-time</i>	Optional By default, the retaining time of history record is 120 minutes.
Configure statistics interval and the maximum number of retained statistics information	statistics { interval <i>interval</i> max-group <i>number</i> }	Optional By default, statistics interval is 120 minutes and up to two pieces of statistics information can be retained.
Configure the retaining time of statistics information	statistics keep-time <i>keep-time</i>	Optional By default, the retaining time of statistics information is 120 minutes.
Configure test start time and lifetime	test-time begin { <i>hh:mm:ss</i> [<i>yyyy/mm/dd</i>] now } lifetime <i>lifetime</i>	Optional By default, no test start time and lifetime is configured.
Enable routing table bypass	sendpacket passroute	Optional By default, routing table bypass is disabled.

To do...	Use the command...	Remarks
Configure the TTL	ttl <i>number</i>	Optional By default, TTL is 20. The sendpacket passroute command voids the ttl command.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the type of service	tos <i>value</i>	Optional By default, the service type is zero.
Configure the type of FTP operation	ftp-operation { get put }	Optional By default, the type of FTP operation is get , that is, the FTP operation will get a file from the FTP server.
Configure an FTP login username	username <i>name</i>	Required By default, neither username nor password is configured.
Configure an FTP login password	password <i>password</i>	
Configure a file name for the FTP operation	filename <i>file-name</i>	Required By default, no file name is configured for the FTP operation
Configure size of a file to be uploaded in an FTP test	filesize <i>file-size</i>	Required By default, the file is 1 MB.
Start the test	test-enable	Required
Display test results	display hwping results [<i>admin-name operation-tag</i>]	Required You can execute the command in any view.

4) Configuring HTTP test on HWPing client

Follow these steps to configure HTTP test on HWPing client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the HWPing client function	hwping-agent enable	Required By default, the HWPing client function is disabled.
Create an HWPing test group and enter its view	hwping <i>administrator-name operation-tag</i>	Required By default, no test group is configured.
Configure the test type	test-type http	Required By default, the test type is ICMP.

To do...	Use the command...	Remarks
Configure the destination IP address	destination-ip <i>ip-address</i>	Required You can configure an IP address or a host name. By default, no destination address is configured.
Configure dns-server	dns-server <i>ip-address</i>	Required when you use the destination-ip command to configure the destination address as the host name. By default, no IP address of the DNS server is configured.
Configure the source IP address	source-ip <i>ip-address</i>	Optional By default, no source IP address is configured.
Configure the source port	source-port <i>port-number</i>	Optional By default, no source port is configured.
Configure the number of probes per test	count <i>times</i>	Optional By default, each test makes one probe.
Configure a test description	description <i>string</i>	Optional By default, no description information is configured.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Optional By default, the maximum number is 50.
Enable history record	history-record enable	Optional By default, history record is not enabled.
Configure the retaining time of history record	history keep-time <i>keep-time</i>	Optional By default, the retaining time of history record is 120 minutes.
Configure statistics interval and the maximum number of retained statistics information	statistics { interval <i>interval</i> max-group <i>number</i> }	Optional By default, statistics interval is 120 minutes and up to two pieces of statistics information can be retained.
Configure the retaining time of statistics information	statistics keep-time <i>keep-time</i>	Optional By default, the retaining time of statistics information is 120 minutes.
Configure test start time and lifetime	test-time begin { hh:mm:ss [yyyy/mm/dd] now } lifetime <i>lifetime</i>	Optional By default, no test start time and lifetime is configured.
Enable routing table bypass	sendpacket passroute	Optional By default, routing table bypass is disabled.

To do...	Use the command...	Remarks
Configure the TTL	tll <i>number</i>	Optional By default, TTL is 20. The sendpacket passroute command voids the tll command.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the type of service	tos <i>value</i>	Optional By default, the service type is zero.
Configure the type of HTTP operation	http-operation { get post }	Optional By default, the type of HTTP operation is get , that is, the HTTP operation will get data from the HTTP server.
Configure the HTTP operation string and HTTP version	http-string <i>string version</i>	Optional By default, no HTTP operation string and HTTP version are configured.
Start the test	test-enable	Required
Display test results	display hwping results [<i>admin-name operation-tag</i>]	Required You can execute the command in any view.

5) Configuring jitter test on HWPing client

Follow these steps to configure jitter test on HWPing client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the HWPing client function	hwping-agent enable	Required By default, the HWPing client function is disabled.
Create an HWPing test group and enter its view	hwping <i>administrator-name operation-tag</i>	Required By default, no test group is configured.
Configure the test type	test-type jitter [codec <i>codec-value</i>]	Required By default, the test type is ICMP.

To do...	Use the command...	Remarks
Configure the destination IP address	destination-ip <i>ip-address</i>	Required The destination address must be the IP address of a UDP listening service on the HWPing server. By default, no destination address is configured.
Configure the destination port	destination-port <i>Port-number</i>	Required The destination port must be the port of a UDP listening service on the HWPing server. By default, no destination port is configured.
Configure the source IP address	source-ip <i>ip-address</i>	Optional By default, no source IP address is configured.
Configure the source port	source-port <i>port-number</i>	Optional By default, no source port is configured.
Configure the number of probes per test	count <i>times</i>	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Optional By default, the maximum number is 50.
Configure the packet size	datasize <i>size</i>	Optional By default, the packet size is 68 bytes.
Configure a stuffing character string	datafill <i>string</i>	Optional By default, the numbers between 0 and 255 are stuffed into datagrams in a cyclically way.
Configure a test description	description <i>string</i>	Optional By default, no description information is configured.
Enable history record	history-record enable	Optional By default, history record is not enabled.
Configure the retaining time of history record	history keep-time <i>keep-time</i>	Optional By default, the retaining time of history record is 120 minutes.
Configure statistics interval and the maximum number of retained statistics information	statistics { interval <i>interval</i> max-group <i>number</i> }	Optional By default, statistics interval is 120 minutes and up to two pieces of statistics information can be retained.

To do...	Use the command...	Remarks
Configure the retaining time of statistics information	statistics keep-time <i>keep-time</i>	Optional By default, the retaining time of statistics information is 120 minutes.
Configure test start time and lifetime	test-time begin { <i>hh:mm:ss</i> [<i>yyyy/mm/dd</i>] now } lifetime <i>lifetime</i>	Optional By default, no test start time and lifetime is configured.
Enable routing table bypass	sendpacket passroute	Optional By default, routing table bypass is disabled.
Configure the TTL	ttl <i>number</i>	Optional By default, TTL is 20. The sendpacket passroute command voids the ttl command.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the type of service	tos <i>value</i>	Optional By default, the service type is zero.
Configure the number of test packets that will be sent in each jitter probe	jitter-packetnum <i>number</i>	Optional By default, each jitter probe will send 10 packets.
Configure the interval to send test packets in the jitter test	jitter-interval <i>interval</i>	Optional By default, the interval is 20 milliseconds.
Configure advantage factor for a jitter voice test	adv-factor <i>adv-number</i>	By default, the advantage factor is zero.
Start the test	test-enable	Required
Display test results	display hwping results [<i>admin-name operation-tag</i>]	Required You can execute the command in any view.

6) Configuring SNMP test on HWPing client

Follow these steps to configure SNMP test on HWPing client:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
Enable the HWPing client function	hwping-agent enable	Required By default, the HWPing client function is disabled.
Create an HWPing test group and enter its view	hwping <i>administrator-name operation-tag</i>	Required By default, no test group is configured.
Configure the test type	test-type snmpquery	Required By default, the test type is ICMP.
Configure the destination IP address	destination-ip <i>ip-address</i>	Required By default, no destination address is configured.
Configure the source IP address	source-ip <i>ip-address</i>	Optional By default, no source IP address is configured.
Configure the source port	source-port <i>port-number</i>	Optional By default, no source port is configured.
Configure the number of probes per test	count <i>times</i>	Optional By default, each test makes one probe.
Configure a test description	description <i>string</i>	Optional By default, no description information is configured.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Optional By default, the maximum number is 50.
Enable history record	history-record enable	Optional By default, history record is not enabled.
Configure the retaining time of history record	history keep-time <i>keep-time</i>	Optional By default, the retaining time of history record is 120 minutes.
Configure statistics interval and the maximum number of retained statistics information	statistics { interval <i>interval</i> max-group <i>number</i> }	Optional By default, statistics interval is 120 minutes and up to two pieces of statistics information can be retained.
Configure the retaining time of statistics information	statistics keep-time <i>keep-time</i>	Optional By default, the retaining time of statistics information is 120 minutes.
Configure test start time and lifetime	test-time begin { <i>hh:mm:ss [yyyy/mm/dd]</i> now } lifetime <i>lifetime</i>	Optional By default, no test start time and lifetime is configured.

To do...	Use the command...	Remarks
Enable routing table bypass	sendpacket passroute	Optional By default, routing table bypass is disabled.
Configure the TTL	tll <i>number</i>	Optional By default, TTL is 20. The sendpacket passroute command voids the tll command.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the type of service	tos <i>value</i>	Optional By default, the service type is zero.
Start the test	test-enable	Required
Display test results	display hwping results [<i>admin-name operation-tag</i>]	Required You can execute the command in any view.

7) Configuring TCP test on HWPing client

Follow these steps to configure TCP test on HWPing client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the HWPing client function	hwping-agent enable	Required By default, the HWPing client function is disabled.
Create an HWPing test group and enter its view	hwping <i>administrator-name operation-tag</i>	Required By default, no test group is configured.
Configure the test type	test-type { tcpprivate tcppublic }	Required By default, the test type is ICMP.
Configure the destination address	destination-ip <i>ip-address</i>	Required This IP address and the one configured on the HWPing server for listening services must be the same. By default, no destination address is configured.

To do...	Use the command...	Remarks
Configure the destination port	destination-port <i>port-number</i>	Required in a Tcpprivate test A Tcppublic test is a TCP connection test on port 7. Use the hwping-server tcpconnect ip-address 7 command on the server to configure the listening service port; otherwise the test will fail. No port number needs to be configured on the client; any destination port number configured on the client will not take effect. By default, no destination port number is configured.
Configure the source IP address	source-ip <i>ip-address</i>	Optional By default, the source IP address is not specified.
Configure the source port	source-port <i>port-number</i>	Optional By default, no source port is specified.
Configure the number of probes per test	count <i>times</i>	Optional By default, one probe is made per time.
Configure a test description	description <i>string</i>	Optional By default, no description information is configured.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Enable history record	history-record <i>enable</i>	Optional By default, history record is not enabled.
Configure the retaining time of history record	history keep-time <i>keep-time</i>	Optional By default, the retaining time of history record is 120 minutes.
Configure statistics interval and the maximum number of retained statistics information	statistics { interval interval max-group number }	Optional By default, statistics interval is 120 minutes and up to two pieces of statistics information can be retained.
Configure the retaining time of statistics information	statistics keep-time <i>keep-time</i>	Optional By default, the retaining time of statistics information is 120 minutes.
Configure test start time and lifetime	test-time begin { hh:mm:ss [yyyy/mm/dd] now } lifetime <i>lifetime</i>	Optional By default, no test start time and lifetime is configured.
Enable routing table bypass	sendpacket passroute	Optional By default, routing table bypass is disabled.
Configure the TTL	ttl <i>number</i>	Optional By default, TTL is 20. The sendpacket passroute command voids the ttl command.

To do...	Use the command...	Remarks
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Optional By default, the maximum number is 50.
Configure the type of service	tos <i>value</i>	Optional By default, the service type is zero.
Start the test	test-enable	Required
Display test results	display hwping results [<i>admin-name operation-tag</i>]	Required The display command can be executed in any view.

8) Configuring UDP test on HWPing client

Follow these steps to configure UDP test on HWPing client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the HWPing client function	hwping-agent enable	Required By default, the HWPing client function is disabled.
Create an HWPing test group and enter its view	hwping <i>administrator-name operation-tag</i>	Required By default, no test group is configured.
Configure the test type	test-type { udpprivate udppublic }	Required By default, the test type is ICMP.
Configure the destination address	destination-ip <i>ip-address</i>	Required This IP address and the one configured on the HWPing server for listening service must be the same. By default, no destination address is configured.
Configure the destination port	destination-port <i>port-number</i>	- Required in a Udpprivate test - A Udppublic test is a UDP connection test on port 7. Use the <code>hwping-server udpecho ip-address 7</code> command on the server to configure the listening service port; otherwise the test will fail. No port number needs to be configured on the client; any destination port number configured on the client will not take effect. - By default, no destination port number is configured.
Configure the source IP address	source-ip <i>ip-address</i>	Optional By default, no source IP address is configured.
Configure the source port	source-port <i>port-number</i>	Optional By default, no source port is specified.

To do...	Use the command...	Remarks
Configure the number of probes per test	count <i>times</i>	Optional By default, one probe is made per test.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Optional By default, the maximum number is 50.
Configure the data packet size	datasize <i>size</i>	Optional By default, the data packet size is 100 bytes.
Configure a stuffing character string	datafill <i>string</i>	Optional By default, the numbers between 0 and 255 are stuffed into datagrams in a cyclically way.
Configure a test description	description <i>string</i>	Optional By default, no description information is configured.
Enable history record	history-record enable	Optional By default, history record is not enabled.
Configure the retaining time of history record	history keep-time <i>keep-time</i>	Optional By default, the retaining time of history record is 120 minutes.
Configure statistics interval and the maximum number of retained statistics information	statistics { interval <i>interval</i> max-group <i>number</i> }	Optional By default, statistics interval is 120 minutes and up to two pieces of statistics information can be retained.
Configure the retaining time of statistics information	statistics keep-time <i>keep-time</i>	Optional By default, the retaining time of statistics information is 120 minutes.
Configure test start time and lifetime	test-time begin { <i>hh:mm:ss</i> [<i>yyyy/mm/dd</i>] now } lifetime <i>lifetime</i>	Optional By default, no test start time and lifetime is configured.
Enable routing table bypass	sendpacket passroute	Optional By default, routing table bypass is disabled.
Configure the TTL	ttl <i>number</i>	Optional By default, TTL is 20. The sendpacket passroute command voids the ttl command.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the service type	tos <i>value</i>	Optional By default, the service type is zero.
Start the test	test-enable	Required

To do...	Use the command...	Remarks
Display test results	display hwping results [<i>admin-name operation-tag</i>]	Required The display command can be executed in any view.

9) Configuring DNS test on HWPing client

Follow these steps to configure DNS test on HWPing client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the HWPing client function	hwping-agent enable	Required By default, the HWPing client function is disabled.
Create an HWPing test group and enter its view	hwping <i>administrator-name operation-tag</i>	Required By default, no test group is configured.
Configure the test type	test-type dns	Required By default, the test type is ICMP.
Configure the source IP address	source-ip <i>ip-address</i>	Optional By default, no source IP address is specified.
Configure the number of probes per test	count <i>times</i>	Optional By default, one probe is made per test.
Configure a test description	description <i>string</i>	Optional By default, no description information is configured.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Optional By default, the maximum number is 50.
Enable history record	history-record enable	Optional By default, history record is not enabled.
Configure the retaining time of history record	history keep-time <i>keep-time</i>	Optional By default, the retaining time of history record is 120 minutes.
Configure statistics interval and the maximum number of retained statistics information	statistics { interval interval max-group number }	Optional By default, statistics interval is 120 minutes and up to two pieces of statistics information can be retained.
Configure the retaining time of statistics information	statistics keep-time <i>keep-time</i>	Optional By default, the retaining time of statistics information is 120 minutes.

To do...	Use the command...	Remarks
Configure test start time and lifetime	test-time begin { <i>hh:mm:ss</i> [<i>yyyy/mm/dd</i>] now } lifetime <i>lifetime</i>	Optional By default, no test start time and lifetime is configured.
Enable routing table bypass	sendpacket passroute	Optional By default, routing table bypass is disabled.
Configure the TTL	tll <i>number</i>	Optional By default, TTL is 20. The sendpacket passroute command voids the tll command.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the type of service	tos <i>value</i>	Optional By default, the service type is zero.
Configure the domain name to be resolved	dns resolve-targetdomai <i>domainname</i>	Required By default, the domain name to be resolved by DNS is not specified.
Configure the IP address of the DNS server	dns-server <i>ip-address</i>	Required By default, no DNS server address is configured.
Start the test	test-enable	Required
Display test results	display hwping results [<i>admin-name operation-tag</i>]	Required The display command can be executed in any view.

10) Clear all agents on the HWPing client

Follow these steps to clear all agents on the HWPing client:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Clear all agents on the HWPing client	hwping-agent clear	Required



Note

- This command clears all the configured agents, including the test configuration, test result, and history information.
- The result cannot be restored after the execution of the command.
- The command does not disable HWPing-agent.

Configuring HWPing client to send Trap messages

Trap messages are generated regardless of whether the HWPing test succeeds or fails. You can specify whether to output Trap messages by enabling/disabling Trap sending.

Follow these steps to configure the HWPing client to send Trap messages:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the HWPing client function	hwping-agent enable	Required By default, the HWPing client function is disabled.
Create an HWPing test group and enter its view	hwping <i>administrator-name operation-tag</i>	Required By default, no test group is configured.
Enable the HWPing client to send Trap messages	send-trap { all { probefailure testcomplete testfailure }* }	Required By default, Trap sending is disabled.
Configure the number of consecutive unsuccessful HWPing tests before Trap output	test-failtimes <i>times</i>	Optional By default, Trap messages are sent each time a test fails.
Configure the number of consecutive unsuccessful HWPing probes before Trap output	probe-failtimes <i>times</i>	Optional By default, Trap messages are sent each time a probe fails.

Displaying HWPing Configuration

To do...	Use the command...	Remarks
Display the results of the test	display hwping { results history jitter } [<i>administrator-name operation-tag</i>]	Available in any view
Display test statistics	display hwping statistics [<i>administrator-name operation-tag</i>]	

HWPing Configuration Examples

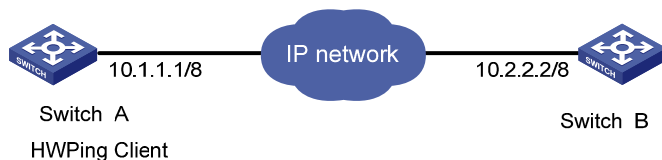
ICMP Test

Network requirements

An H3C S3600 series Ethernet switch serves as the HWPing client. An HWPing ICMP test between the switch and another switch uses ICMP to test the round trip time (RTT) for packets generated by the HWPing client to travel to and back from the destination switch.

Network diagram

Figure 1-2 Network diagram for the ICMP test



Configuration procedure

- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<Sysname> system-view
```

```
[Sysname] hwping-agent enable
```

Create an HWPing test group, setting the administrator name to **administrator** and test tag to **ICMP**.

```
[Sysname] hwping administrator icmp
```

Configure the test type as **icmp**.

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

Configure the destination IP address as 10.2.2.2.

```
[Sysname-hwping-administrator-icmp] destination-ip 10.2.2.2
```

Configure to make 10 probes per test.

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

Set the probe timeout time to 5 seconds.

```
[Sysname-hwping-administrator-icmp] timeout 5
```

Set the maximum number of history records that can be saved to 5.

```
[Sysname-hwping-administrator-icmp] history-records 5
```

Start the test.

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

Display test results.

```
[Sysname-hwping-administrator-icmp] display hwping results administrator icmp
```

HWPing entry(admin administrator, tag icmp) test result:

Destination ip address:10.2.2.2

Send operation times: 10

Receive response times: 10

Min/Max/Average Round Trip Time: 3/6/3

Square-Sum of Round Trip Time: 145

Last succeeded test time: 2000-4-2 20:55:12.3

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

[Sysname-hwping-administrator-icmp] display hwping history administrator icmp
HWPing entry(admin administrator, tag icmp) history record:

```

Index	Response	Status	LastRC	Time
1	3	1	0	2000-04-02 20:55:12.3
2	4	1	0	2000-04-02 20:55:12.3
3	4	1	0	2000-04-02 20:55:12.2
4	3	1	0	2000-04-02 20:55:12.2
5	3	1	0	2000-04-02 20:55:12.2

For detailed output description, see the corresponding command manual.

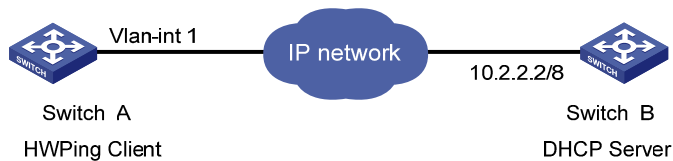
DHCP Test

Network requirements

Both the HWPing client and the DHCP server are H3C S3600 series Ethernet switches. Perform a HWPing DHCP test between the two switches to test the time required for the HWPing client to obtain an IP address from the DHCP server.

Network diagram

Figure 1-3 Network diagram for the DHCP test



Configuration procedure

- Configure DHCP Server(Switch B):

Configure DHCP server on Switch B. For specific configuration of DHCP server, refer to the *DHCP* part of the manual.

- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<Sysname> system-view
```

```
[Sysname] hwping-agent enable
```

Create an HWPing test group, setting the administrator name to **administrator** and test tag to **DHCP**.

```
[Sysname] hwping administrator dhcp
```

Configure the test type as **dhcp**.

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

Configure the source interface, which must be a VLAN interface. Make sure the DHCP server resides on the network connected to this interface.

```
[Sysname-hwping-administrator-dhcp] source-interface Vlan-interface 1
```

```
# Configure to make 10 probes per test.
[Sysname-hwping-administrator-dhcp] count 10

# Set the probe timeout time to 5 seconds.
[Sysname-hwping-administrator-dhcp] timeout 5

# Start the test.
[Sysname-hwping-administrator-dhcp] test-enable

# Display test results
[Sysname-hwping-administrator-dhcp] display hwping results administrator dhcp
HWPing entry(admin administrator, tag dhcp) test result:
    Send operation times: 10                Receive response times: 10
    Min/Max/Average Round Trip Time: 1018/1037/1023
    Square-Sum of Round Trip Time: 10465630
    Last complete test time: 2000-4-3 9:51:30.9
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
[Sysname-hwping-administrator-dhcp] display hwping history administrator dhcp
HWPing entry(admin administrator, tag dhcp) history record:
    Index      Response      Status      LastRC      Time
    1          1018          1           0           2000-04-03 09:51:30.9
    2          1037          1           0           2000-04-03 09:51:22.9
    3          1024          1           0           2000-04-03 09:51:18.9
    4          1027          1           0           2000-04-03 09:51:06.8
    5          1018          1           0           2000-04-03 09:51:00.8
    6          1020          1           0           2000-04-03 09:50:52.8
    7          1018          1           0           2000-04-03 09:50:48.8
    8          1020          1           0           2000-04-03 09:50:36.8
    9          1020          1           0           2000-04-03 09:50:30.8
    10         1028          1           0           2000-04-03 09:50:22.8
```

For detailed output description, see the corresponding command manual.

Note

You can perform an HWPing DHCP test only when no DHCP client is enabled on any interface. Otherwise, the DHCP Server sends the response to an interface enabled with the DHCP Client rather than to the source interface, thus resulting in HWPing DHCP test failure.

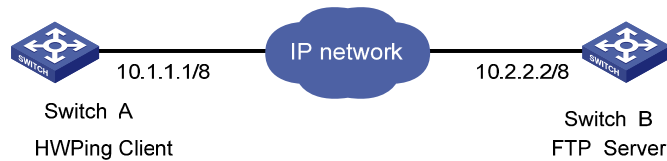
FTP Test

Network requirements

Both the HWPing client and the FTP server are H3C S3600 series Ethernet switches. Perform an HWPing FTP test between the two switches to test the connectivity to the specified FTP server and the time required to upload a file to the server after the connection is established. Both the username and password used to log in to the FTP server are **admin**. The file to be uploaded to the server is cmdtree.txt.

Network diagram

Figure 1-4 Network diagram for the FTP test



Configuration procedure

- Configure FTP Server (Switch B):

Configure FTP server on Switch B. For specific configuration of FTP server, refer to the FTP-SFTP-TFTP part of the manual.

- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<Sysname> system-view
```

```
[Sysname] hwping-agent enable
```

Create an HWPing test group, setting the administrator name to **administrator** and test tag to **FTP**.

```
[Sysname] hwping administrator ftp
```

Configure the test type as **ftp**.

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

Configure the IP address of the FTP server as 10.2.2.2.

```
[Sysname-hwping-administrator-ftp] destination-ip 10.2.2.2
```

Configure the FTP login username.

```
[Sysname-hwping-administrator-ftp] username admin
```

Configure the FTP login password.

```
[Sysname-hwping-administrator-ftp] password admin
```

Configure the type of FTP operation.

```
[Sysname-hwping-administrator-ftp] ftp-operation put
```

Configure a file name for the FTP operation.

```
[Sysname-hwping-administrator-ftp] filename cmdtree.txt
```

Configure to make 10 probes per test.

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

Set the probe timeout time to 30 seconds.

```

[Sysname-hwping-administrator-ftp] timeout 30

# Configure the source IP address

[Sysname-hwping-administrator-ftp] source-ip 10.1.1.1

# Start the test.

[Sysname-hwping-administrator-ftp] test-enable

# Display test results

[Sysname-hwping-administrator-ftp] display hwping results administrator ftp
HWPing entry(admin administrator, tag ftp) test result:
    Destination ip address:10.2.2.2
    Send operation times: 10                Receive response times: 10
    Min/Max/Average Round Trip Time: 3245/15891/12157
    Square-Sum of Round Trip Time: 1644458573
    Last complete test time: 2000-4-3 4:0:34.6
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
[Sysname-hwping-administrator-ftp] display hwping history administrator ftp
HWPing entry(admin administrator, tag ftp) history record:
    Index      Response      Status      LastRC      Time
    1          15822          1           0           2000-04-03 04:00:34.6
    2          15772          1           0           2000-04-03 04:00:18.8
    3           9945          1           0           2000-04-03 04:00:02.9
    4          15891          1           0           2000-04-03 03:59:52.9
    5          15772          1           0           2000-04-03 03:59:37.0
    6          15653          1           0           2000-04-03 03:59:21.2
    7           9792          1           0           2000-04-03 03:59:05.5
    8           9794          1           0           2000-04-03 03:58:55.6
    9           9891          1           0           2000-04-03 03:58:45.8
    10         3245          1           0           2000-04-03 03:58:35.9

```

For detailed output description, see the corresponding command manual.



Note

If you are downloading a file from the server, you do not need to specify an FTP operation type. For details, see section [Configuring FTP test on HWPing client](#).

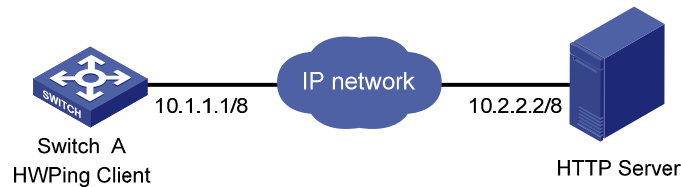
HTTP Test

Network requirements

An H3C S3600 series Ethernet switch serves as the HWPing client, and a PC serves as the HTTP server. Perform an HWPing HTTP test between the switch and the HTTP server to test the connectivity and the time required to download a file from the HTTP server after the connection to the server is established.

Network diagram

Figure 1-5 Network diagram for the HTTP test



Configuration procedure

- Configure HTTP Server:

Use Windows 2003 Server as the HTTP server. For HTTP server configuration, refer to the related instruction on Windows 2003 Server configuration.

- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<Sysname> system-view
```

```
[Sysname] hwping-agent enable
```

Create an HWPing test group, setting the administrator name to **administrator** and test tag to **HTTP**.

```
[Sysname] hwping administrator http
```

Configure the test type as **http**.

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

Configure the IP address of the HTTP server as 10.2.2.2.

```
[Sysname-hwping-administrator-http] destination-ip 10.2.2.2
```

Configure to make 10 probes per test.

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

Set the probe timeout time to 30 seconds.

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

Start the test.

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

Display test results

```
[Sysname-hwping-administrator-http] display hwping results administrator http
```

```
HWPing entry(admin administrator, tag http) test result:
```

```
Destination ip address:10.2.2.2
```

```
Send operation times: 10
```

```
Receive response times: 10
```

Min/Max/Average Round Trip Time: 47/87/74
Square-Sum of Round Trip Time: 57044
Last succeeded test time: 2000-4-2 20:41:50.4

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	

Http result:

DNS Resolve Time: 0	HTTP Operation Time: 675
DNS Resolve Min Time: 0	HTTP Test Total Time: 748
DNS Resolve Max Time: 0	HTTP Transmission Successful Times: 10
DNS Resolve Failed Times: 0	HTTP Transmission Failed Times: 0
DNS Resolve Timeout Times: 0	HTTP Transmission Timeout Times: 0
TCP Connect Time: 73	HTTP Operation Min Time: 27
TCP Connect Min Time: 5	HTTP Operation Max Time: 80
TCP Connect Max Time: 20	
TCP Connect Timeout Times: 0	

[Sysname-hwping-administrator-http] display hwping history administrator http
HWPing entry(admin administrator, tag http) history record:

Index	Response	Status	LastRC	Time
1	13	1	0	2000-04-02 15:15:52.5
2	9	1	0	2000-04-02 15:15:52.5
3	3	1	0	2000-04-02 15:15:52.5
4	3	1	0	2000-04-02 15:15:52.5
5	3	1	0	2000-04-02 15:15:52.5
6	2	1	0	2000-04-02 15:15:52.4
7	3	1	0	2000-04-02 15:15:52.4
8	3	1	0	2000-04-02 15:15:52.4
9	2	1	0	2000-04-02 15:15:52.4
10	2	1	0	2000-04-02 15:15:52.4

For detailed output description, see the corresponding command manual.



Note

For an HTTP test, if configuring the destination address as the host name, you must configure the IP address of the DNS server to resolve the host name into an IP address, which is the destination IP address of this HTTP test.

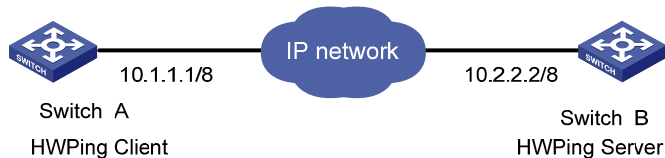
Jitter Test

Network requirements

Both the HWPing client and the HWPing server are H3C S3600 series Ethernet switches. Perform an HWPing jitter test between the two switches to test the delay jitter of the UDP packets exchanged between this end (HWPing client) and the specified destination end (HWPing server), with the port number set to 9000.

Network diagram

Figure 1-6 Network diagram for the Jitter test



Configuration procedure

- Configure HWPing Server (Switch B):

Enable the HWPing server and configure the IP address and port to listen on.

```
<Sysname> system-view
[Sysname] hwping-server enable
[Sysname] hwping-server udpecho 10.2.2.2 9000
```

- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<Sysname> system-view
[Sysname] hwping-agent enable
```

Create an HWPing test group, setting the administrator name to **administrator** and test tag to **Jitter**.

```
[Sysname] hwping administrator Jitter
```

Configure the test type as **jitter**

```
[Sysname-hwping-administrator-Jitter] test-type Jitter
```

Configure the IP address of the HWPing server as 10.2.2.2.

```
[Sysname-hwping-administrator-Jitter] destination-ip 10.2.2.2
```

Configure the destination port on the HWPing server.

```
[Sysname-hwping-administrator-Jitter] destination-port 9000
```

Configure to make 10 probes per test.

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

Set the probe timeout time to 30 seconds.

```
[Sysname-hwping-administrator-Jitter] timeout 30
```

Start the test.

```
[Sysname-hwping-administrator-Jitter] test-enable
```

Display test results

```
[Sysname-hwping-administrator-Jitter] display hwping results administrator Jitter
```

HWPing entry(admin administrator, tag Jitter) test result:

Destination ip address:10.2.2.2

Send operation times: 100

Receive response times: 100

Min/Max/Average Round Trip Time: 9/21/13

Square-Sum of Round Trip Time: 18623

Last complete test time: 2000-4-2 8:14:58.2

Extend result:

SD Maximal delay: 10

DS Maximal delay: 10

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

Jitter result:

RTT Number:100

Min Positive SD:1

Min Positive DS:1

Max Positive SD:6

Max Positive DS:8

Positive SD Number:38

Positive DS Number:25

Positive SD Sum:85

Positive DS Sum:42

Positive SD average:2

Positive DS average:1

Positive SD Square Sum:267

Positive DS Square Sum:162

Min Negative SD:1

Min Negative DS:1

Max Negative SD:6

Max Negative DS:8

Negative SD Number:30

Negative DS Number:24

Negative SD Sum:64

Negative DS Sum: 41

Negative SD average:2

Negative DS average:1

Negative SD Square Sum:200

Negative DS Square Sum:161

SD lost packets number:0

DS lost packet number:0

Unknown result lost packet number:0

[Sysname-hwping-administrator-Jitter] display hwping history administrator Jitter

HWPing entry(admin administrator, tag Jitter) history record:

Index	Response	Status	LastRC	Time
1	274	1	0	2000-04-02 08:14:58.2
2	278	1	0	2000-04-02 08:14:57.9
3	280	1	0	2000-04-02 08:14:57.6
4	279	1	0	2000-04-02 08:14:57.3
5	280	1	0	2000-04-02 08:14:57.1
6	270	1	0	2000-04-02 08:14:56.8
7	275	1	0	2000-04-02 08:14:56.5
8	263	1	0	2000-04-02 08:14:56.2
9	270	1	0	2000-04-02 08:14:56.0
10	275	1	0	2000-04-02 08:14:55.7

For detailed output description, see the corresponding command manual.

SNMP Test

Network requirements

Both the HWPing client and the SNMP Agent are H3C S3600 series Ethernet switches. Perform HWPing SNMP tests between the two switches to test the time required from Switch A sends an SNMP query message to Switch B (SNMP Agent) to it receives a response from Switch B.

Network diagram

Figure 1-7 Network diagram for the SNMP test



Configuration procedure

- Configure SNMP Agent (Switch B):

Start SNMP agent and set SNMP version to V2C, read-only community name to **public**, and read-write community name to **private**.

```
<Sysname> system-view
[Sysname] snmp-agent
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
```



Note

- The SNMP network management function must be enabled on SNMP agent before it can receive response packets.
- The SNMPv2c version is used as reference in this example. This configuration may differ if the system uses any other version of SNMP. For details, see *SNMP – RMON Operation Manual*.

-
- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<Sysname> system-view
[Sysname] hwping-agent enable
```

Create an HWPing test group, setting the administrator name to **administrator** and test tag to **snmp**.

```
[Sysname] hwping administrator snmp
```

Configure the test type as **snmp**.

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

Configure the destination IP address as 10.2.2.2.

```
[Sysname-hwping-administrator-snmp] destination-ip 10.2.2.2
```

```

# Configure to make 10 probes per test.
[Sysname-hwping-administrator-snmp] count 10

# Set the probe timeout time to 30 seconds.
[Sysname-hwping-administrator-snmp] timeout 30

# Start the test.
[Sysname-hwping-administrator-snmp] test-enable

# Display test results
[Sysname-hwping-administrator-snmp] display hwping results administrator snmp
HWPing entry(admin administrator, tag snmp) test result:
    Destination ip address:10.2.2.2
    Send operation times: 10                Receive response times: 10
    Min/Max/Average Round Trip Time: 9/11/10
    Square-Sum of Round Trip Time: 983
    Last complete test time: 2000-4-3 8:57:20.0
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
[Sysname-hwping-administrator-snmp] display hwping history administrator snmp
HWPing entry(admin administrator, tag snmp) history record:

```

Index	Response	Status	LastRC	Time
1	10	1	0	2000-04-03 08:57:20.0
2	10	1	0	2000-04-03 08:57:20.0
3	10	1	0	2000-04-03 08:57:20.0
4	10	1	0	2000-04-03 08:57:19.9
5	9	1	0	2000-04-03 08:57:19.9
6	11	1	0	2000-04-03 08:57:19.9
7	10	1	0	2000-04-03 08:57:19.9
8	10	1	0	2000-04-03 08:57:19.9
9	10	1	0	2000-04-03 08:57:19.8
10	10	1	0	2000-04-03 08:57:19.8

For detailed output description, see the corresponding command manual.

TCP Test (Tcprivate Test) on the Specified Ports

Network requirements

Both the HWPing client and the HWPing server are H3C S3600 series Ethernet switches. Perform an HWPing Tcprivate test to test time required to establish a TCP connection between this end (Switch A) and the specified destination end (Switch B), with the port number set to 8000.

Network diagram

Figure 1-8 Network diagram for the Tcpprivate test



Configuration procedure

- Configure HWPing Server (Switch B):

Enable the HWPing server and configure the IP address and port to listen on.

```
<Sysname> system-view
```

```
[Sysname] hwping-server enable
```

```
[Sysname] hwping-server tcpconnect 10.2.2.2 8000
```

- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<Sysname> system-view
```

```
[Sysname] hwping-agent enable
```

Create an HWPing test group, setting the administrator name to **administrator** and test tag to **tcpprivate**.

```
[Sysname] hwping administrator tcpprivate
```

Configure the test type as **tcpprivate**.

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

Configure the IP address of the HWPing server as 10.2.2.2.

```
[Sysname-hwping-administrator-tcpprivate] destination-ip 10.2.2.2
```

Configure the destination port on the HWPing server.

```
[Sysname-hwping-administrator-tcpprivate] destination-port 8000
```

Configure to make 10 probes per test.

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

Set the probe timeout time to 5 seconds.

```
[Sysname-hwping-administrator-tcpprivate] timeout 5
```

Start the test.

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

Display test results.

```
[Sysname-hwping-administrator-tcpprivate] display hwping results administrator tcpprivate
```

HWPing entry(admin administrator, tag tcpprivate) test result:

Destination ip address:10.2.2.2

Send operation times: 10

Receive response times: 10

Min/Max/Average Round Trip Time: 4/7/5

Square-Sum of Round Trip Time: 282

Last complete test time: 2000-4-2 8:26:2.9

Extend result:

```

SD Maximal delay: 0
Packet lost in test: 0%
Disconnect operation number: 0
System busy operation number: 0
Operation sequence errors: 0
Other operation errors: 0
DS Maximal delay: 0
Operation timeout number: 0
Connection fail number: 0
Drop operation number: 0

```

[Sysname-hwping-administrator-tcprivate] display hwping history administrator tcprivate
HWPing entry(admin administrator, tag tcprivate) history record:

Index	Response	Status	LastRC	Time
1	4	1	0	2000-04-02 08:26:02.9
2	5	1	0	2000-04-02 08:26:02.8
3	4	1	0	2000-04-02 08:26:02.8
4	5	1	0	2000-04-02 08:26:02.7
5	4	1	0	2000-04-02 08:26:02.7
6	5	1	0	2000-04-02 08:26:02.6
7	6	1	0	2000-04-02 08:26:02.6
8	7	1	0	2000-04-02 08:26:02.5
9	5	1	0	2000-04-02 08:26:02.5
10	7	1	0	2000-04-02 08:26:02.4

For detailed output description, see the corresponding command manual.

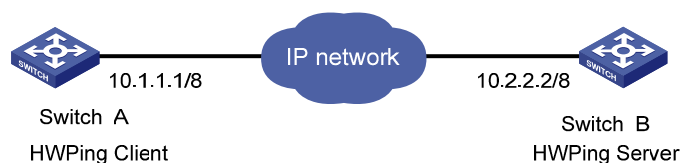
UDP Test (Udpprivate Test) on the Specified Ports

Network requirements

Both the HWPing client and the HWPing server are H3C S3600 series Ethernet switches. Perform an HWPing Udpprivate test on the specified ports between the two switches to test the RTT of UDP packets between this end (HWPing client) and the specified destination end (HWPing server), with the port number set to 8000.

Network diagram

Figure 1-9 Network diagram for the Udpprivate test



Configuration procedure

- Configure HWPing Server (Switch B):

Enable the HWPing server and configure the IP address and port to listen on.

```
<Sysname> system-view
```

```
[Sysname] hwping-server enable
```

```
[Sysname] hwping-server udpecho 10.2.2.2 8000
```

- Configure HWPing Client (Switch A):

Enable the HWPing client.

```
<Sysname> system-view
```

```

[Sysname] hwping-agent enable

# Create an HWPing test group, setting the administrator name to administrator and test tag to udpprivate.
[Sysname] hwping administrator udpprivate

# Configure the test type as udpprivate.
[Sysname-hwping-administrator-udpprivate] test-type udpprivate

# Configure the IP address of the HWPing server as 10.2.2.2.
[Sysname-hwping-administrator-udpprivate] destination-ip 10.2.2.2

# Configure the destination port on the HWPing server.
[Sysname-hwping-administrator-udpprivate] destination-port 8000

# Configure to make 10 probes per test.
[Sysname-hwping-administrator-udpprivate] count 10

# Set the probe timeout time to 5 seconds.
[Sysname-hwping-administrator-udpprivate] timeout 5

# Start the test.
[Sysname-hwping-administrator-udpprivate] test-enable

# Display test results.
[Sysname-hwping-administrator-udpprivate] display hwping results administrator udpprivate
HWPing entry(admin administrator, tag udpprivate) test result:
    Destination ip address:10.2.2.2
    Send operation times: 10                Receive response times: 10
    Min/Max/Average Round Trip Time: 10/12/10
    Square-Sum of Round Trip Time: 1170
    Last complete test time: 2000-4-2 8:29:45.5
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

[Sysname-hwping-administrator-udpprivate] display hwping history administrator udpprivate
HWPing entry(admin administrator, tag udpprivate) history record:

```

Index	Response	Status	LastRC	Time
1	11	1	0	2000-04-02 08:29:45.5
2	12	1	0	2000-04-02 08:29:45.4
3	11	1	0	2000-04-02 08:29:45.4
4	11	1	0	2000-04-02 08:29:45.4
5	11	1	0	2000-04-02 08:29:45.4
6	11	1	0	2000-04-02 08:29:45.4
7	10	1	0	2000-04-02 08:29:45.3
8	10	1	0	2000-04-02 08:29:45.3
9	10	1	0	2000-04-02 08:29:45.3
10	11	1	0	2000-04-02 08:29:45.3

For detailed output description, see the corresponding command manual.

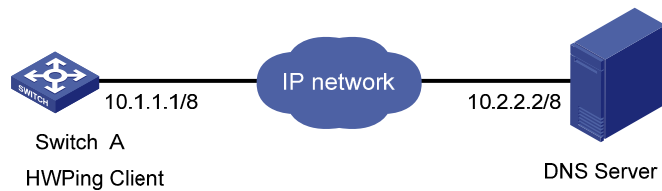
DNS Test

Network requirements

An H3C S3600 series Ethernet switch serves as the HWPing client, and a PC serves as the DNS server. Perform an HWPing DNS test between the switch and the DNS server to test the time required from the client sends a DNS request to it receives a resolution result from the DNS server.

Network diagram

Figure 1-10 Network diagram for the DNS test



Configuration procedure

- Configure DNS Server:

Use Windows 2003 Server as the DNS server. For DNS server configuration, refer to the related instruction on Windows 2003 Server configuration.

- Configure HWPing Client (Switch A)

Enable the HWPing client.

```
<Sysname> system-view
```

```
[Sysname] hwping-agent enable
```

Create an HWPing test group, setting the administrator name to **administrator** and test tag to **dns**.

```
[Sysname] hwping administrator dns
```

Configure the test type as **dns**.

```
[Sysname-hwping-administrator-dns] test-type dns
```

Configure the IP address of the DNS server as 10.2.2.2.

```
[Sysname-hwping-administrator-dns] dns-server 10.2.2.2
```

Configure to resolve the domain name www.test.com.

```
[Sysname-hwping-administrator-dns] dns resolve-target www.test.com
```

Configure to make 10 probes per test.

```
[Sysname-hwping-administrator-dns] count 10
```

Set the probe timeout time to 5 seconds.

```
[Sysname-hwping-administrator-dns] timeout 5
```

Start the test.

```
[Sysname-hwping-administrator-dns] test-enable
```

Display test results.

```
[Sysname-hwping-administrator-dns] display hwping results administrator dns
```

HWPing entry(admin administrator, tag dns) test result:

Destination ip address:10.2.2.2

Send operation times: 10

Receive response times: 10

Min/Max/Average Round Trip Time: 6/10/8

Square-Sum of Round Trip Time: 756

Last complete test time: 2006-11-28 11:50:40.9

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

Dns result:

DNS Resolve Current Time: 10

DNS Resolve Min Time: 6

DNS Resolve Times: 10

DNS Resolve Max Time: 10

DNS Resolve Timeout Times: 0

DNS Resolve Failed Times: 0

[Sysname-hwping-administrator-dns] display hwping history administrator dns

HWPing entry(admin administrator, tag dns) history record:

Index	Response	Status	LastRC	Time
1	10	1	0	2006-11-28 11:50:40.9
2	10	1	0	2006-11-28 11:50:40.9
3	10	1	0	2006-11-28 11:50:40.9
4	7	1	0	2006-11-28 11:50:40.9
5	8	1	0	2006-11-28 11:50:40.9
6	6	1	0	2006-11-28 11:50:40.9
7	8	1	0	2006-11-28 11:50:40.9
8	9	1	0	2006-11-28 11:50:40.9
9	9	1	0	2006-11-28 11:50:40.9
10	9	1	0	2006-11-28 11:50:40.9

For detailed output description, see the corresponding command manual.

Table of Contents

1 IPv6 Configuration	1-1
IPv6 Overview	1-1
IPv6 Features	1-1
Introduction to IPv6 Address	1-3
Introduction to IPv6 Neighbor Discovery Protocol	1-6
Introduction to IPv6 DNS	1-8
Protocols and Standards	1-8
IPv6 Configuration Task List	1-9
Configuring an IPv6 Unicast Address	1-9
Configuring IPv6 NDP	1-11
Configuring a Static IPv6 Route	1-13
Configuring IPv6 TCP Properties	1-13
Configuring the Maximum Number of IPv6 ICMP Error Packets Sent within a Specified Time	1-13
Configuring the Hop Limit of ICMPv6 Reply Packets	1-14
Configuring IPv6 DNS	1-14
Displaying and Maintaining IPv6	1-15
IPv6 Configuration Example	1-17
IPv6 Unicast Address Configuration	1-17
2 IPv6 Application Configuration	2-1
Introduction to IPv6 Application	2-1
Configuring IPv6 Application	2-1
IPv6 Ping	2-1
IPv6 Traceroute	2-2
IPv6 TFTP	2-2
IPv6 Telnet	2-3
IPv6 Application Configuration Example	2-4
IPv6 Applications	2-4
Troubleshooting IPv6 Application	2-6
Unable to Ping a Remote Destination	2-6
Unable to Run Traceroute	2-6
Unable to Run TFTP	2-6
Unable to Run Telnet	2-7

1 IPv6 Configuration

When configuring IPv6, go to these sections for information you are interested in:

- [IPv6 Overview](#)
- [IPv6 Configuration Task List](#)
- [IPv6 Configuration Example](#)



Note

- The term “router” in this document refers to a router in a generic sense or an Ethernet switch running a routing protocol.
 - H3C S3600 Series Ethernet Switches support IPv6 management features, but do not support IPv6 forwarding and related features.
-

IPv6 Overview

Internet Protocol Version 6 (IPv6), also called IP next generation (IPng), was designed by the Internet Engineering Task Force (IETF) as the successor to Internet Protocol Version 4 (IPv4). The significant difference between IPv6 and IPv4 is that IPv6 increases the IP address size from 32 bits to 128 bits.

IPv6 Features

Header format simplification

IPv6 cuts down some IPv4 header fields or moves them to extension headers to reduce the overhead of the basic IPv6 header. IPv6 uses a fixed-length header, thus making IPv6 packet handling simple and improving the forwarding efficiency. Although the IPv6 address size is four times that of IPv4 addresses, the size of the IPv6 header is only twice that of the IPv4 header (excluding the Options field). For the specific IPv6 header format, see [Figure 1-1](#).

The diagram illustrates the structure of IPv4 and IPv6 headers. The IPv4 header is 32 bits long, while the IPv6 header is 40 bits long. The IPv4 header includes fields like Ver, IHL, ToS, Total length, Identification, F, Fragment offset, TTL, Protocol, Header checksum, Source address (32 bits), Destination address (32 bits), Options, and Padding. The IPv6 header includes Ver, Traffic class, Flow label, Payload length, Next header, Hop limit, Source address (128 bits), and Destination address (128 bits).

0		3		7		15		23		31	
Ver	IHL		ToS		Total length						
Identification				F	Fragment offset						
TTL		Protocol		Header checksum							
Source address (32 bits)											
Destination address (32 bits)											
Options								Padding			

IPv4 header

0		3		7		11		15		23		31	
Ver	Traffic class		Flow label										
Payload length						Next header		Hop limit					
Source address (128 bits)													
Destination address (128 bits)													

Basic IPv6 header

The source IPv6 address and the destination IPv6 address are both 128 bits (16 bytes) long. IPv6 can provide 3.4×10^{38} addresses to completely meet the requirements of hierarchical address division as well as allocation of public and private addresses.

IPv6 adopts the hierarchical address structure to quicken route search and reduce the system source occupied by the IPv6 routing table by means of route aggregation.

To simplify the host configuration, IPv6 supports stateful address configuration and stateless address configuration.

- In addition, a host can automatically generate a link-local address based on its own link-layer address and the default prefix (FE80::/64) to communicate with other hosts on the link.

IPv6 uses IPSec as its standard extension header to provide end-to-end security. This feature provides a standard for network security solutions and improves the interoperability between different IPv6 applications.

The Flow Label field in the IPv6 header allows the device to label packets in a flow and provide special handling for these packets.

Enhanced neighbor discovery mechanism

The IPv6 neighbor discovery protocol is implemented by a group of Internet Control Message Protocol Version 6 (ICMPv6) messages. The IPv6 neighbor discovery protocol manages message exchange between neighbor nodes (nodes on the same link). The group of ICMPv6 messages takes the place of Address Resolution Protocol (ARP), Internet Control Message Protocol Version 4 (ICMPv4), and ICMPv4 redirect messages to provide a series of other functions.

Flexible extension headers

IPv6 cancels the Options field in IPv4 packets but introduces multiple extension headers. In this way, IPv6 enhances the flexibility greatly to provide scalability for IP while improving the processing efficiency. The Options field in IPv4 packets contains only 40 bytes, while the size of IPv6 extension headers is restricted by that of IPv6 packets.

Introduction to IPv6 Address

IPv6 addresses

An IPv6 address is represented as a series of 16-bit hexadecimals, separated by colons. An IPv6 address is divided into eight groups, 16 bits of each group are represented by four hexadecimal numbers which are separated by colons, for example, 2001:0000:130F:0000:0000:09C0:876A:130B.

To simplify the representation of IPv6 addresses, zeros in IPv6 addresses can be handled as follows:

- Leading zeros in each group can be removed. For example, the above-mentioned address can be represented in shorter format as 2001:0:130F:0:0:9C0:876A:130B.
- If an IPv6 address contains two or more consecutive groups of zeros, they can be replaced by the double-colon :: option. For example, the above-mentioned address can be represented in the shortest format as 2001:0:130F::9C0:876A:130B.



Caution

The double-colon :: can be used only once in an IPv6 address. Otherwise, the device is unable to determine how many zeros the double-colon represents when converting it to zeros to restore the IPv6 address to a 128-bit address.

An IPv6 address consists of two parts: address prefix and interface ID. The address prefix and the interface ID are respectively equivalent to the network ID and the host ID in an IPv4 address.

An IPv6 address prefix is written in IPv6-address/prefix-length notation, where IPv6-address is an IPv6 address in any of the notations and prefix-length is a decimal number indicating how many bits from the left of an IPv6 address are the address prefix.

IPv6 address classification

IPv6 addresses mainly fall into three types: unicast address, multicast address and anycast address.

- Unicast address: An identifier for a single interface, similar to an IPv4 unicast address. A packet sent to a unicast address is delivered to the interface identified by that address.

- Multicast address: An identifier for a set of interfaces (typically belonging to different nodes), similar to an IPv4 multicast address. A packet sent to a multicast address is delivered to all interfaces identified by that address.
- Anycast address: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the nearest one, according to the routing protocols' measure of distance).



Note

There are no broadcast addresses in IPv6. Their function is superseded by multicast addresses.

The type of an IPv6 address is designated by the format prefix. [Table 1-1](#) lists the mapping between major address types and format prefixes.

Table 1-1 Mapping between address types and format prefixes

Type		Format prefix (binary)	IPv6 prefix ID
Unicast address	Unassigned address	00...0 (128 bits)	::/128
	Loopback address	00...1 (128 bits)	::1/128
	Link-local address	1111111010	FE80::/10
	Site-local address	1111111011	FEC0::/10
	Global unicast address	other forms	—
Multicast address		11111111	FF00::/8
Anycast address		Anycast addresses are taken from unicast address space and are not syntactically distinguishable from unicast addresses.	

Unicast address

There are several forms of unicast address assignment in IPv6, including global unicast address, link-local address, and site-local address.

- The global unicast address, equivalent to an IPv4 public address, is used for aggregatable links and provided for network service providers. This type of address allows efficient routing aggregation to restrict the number of global routing entries.
- The link-local address is used in the neighbor discovery protocol and the stateless autoconfiguration process. Routers must not forward any packets with link-local source or destination addresses to other links.
- IPv6 unicast site-local addresses are similar to private IPv4 addresses. Routers must not forward any packets with site-local source or destination addresses outside of the site (equivalent to a private network).
- Loopback address: The unicast address 0:0:0:0:0:0:0:1 (represented in shorter format as ::1) is called the loopback address and may never be assigned to any physical interface. Like the loopback address in IPv4, it may be used by a node to send an IPv6 packet to itself.

- Unassigned address: The unicast address `::` is called the unassigned address and may not be assigned to any node. Before acquiring a valid IPv6 address, a node may fill this address in the source address field of an IPv6 packet, but may not use it as a destination IPv6 address.

Multicast address

Multicast addresses listed in [Table 1-2](#) are reserved for special purpose.

Table 1-2 Reserved IPv6 multicast addresses

Address	Application
FF01::1	Node-local scope all-nodes multicast address
FF02::1	Link-local scope all-nodes multicast address
FF01::2	Node-local scope all-routers multicast address
FF02::2	Link-local scope all-routers multicast address
FF05::2	Site-local scope all-routers multicast address

Besides, there is another type of multicast address: solicited-node address. The solicited-node multicast address is used to acquire the link-layer addresses of neighbor nodes on the same link and is also used for duplicate address detection. Each IPv6 unicast or anycast address has one corresponding solicited-node address. The format of a solicited-node multicast address is as follows:

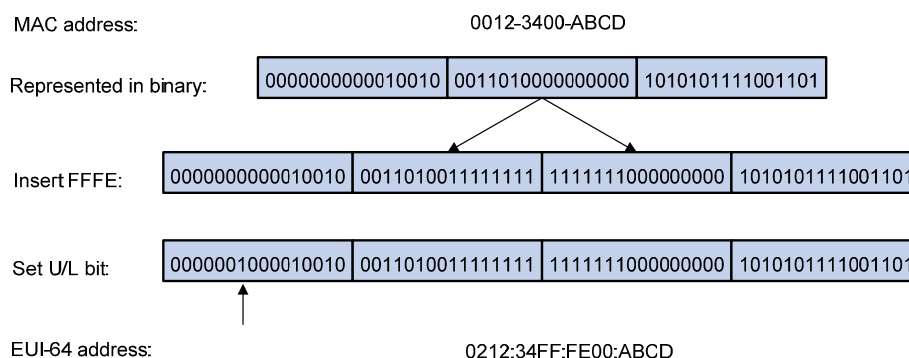
FF02:0:0:0:1:FFXX:XXXX

Where, FF02:0:0:0:1:FF is permanent and consists of 104 bits, and XX:XXXX is the last 24 bits of an IPv6 address.

Interface identifier in IEEE EUI-64 format

Interface identifiers in IPv6 unicast addresses are used to identify interfaces on a link and they are required to be unique on that link. Interface identifiers in IPv6 unicast addresses are currently required to be 64 bits long. An interface identifier is derived from the link-layer address of that interface. Interface identifiers in IPv6 addresses are 64 bits long, while MAC addresses are 48 bits long. Therefore, the hexadecimal number FFFE needs to be inserted in the middle of MAC addresses (behind the 24 high-order bits). To ensure the interface identifier obtained from a MAC address is unique, it is necessary to set the universal/local (U/L) bit (the seventh high-order bit) to “1”. Thus, an interface identifier in EUI-64 format is obtained.

Figure 1-2 Convert a MAC address into an EUI-64 address



Introduction to IPv6 Neighbor Discovery Protocol

The IPv6 Neighbor Discovery Protocol (NDP) uses five types of ICMPv6 messages to implement the following functions:

- Address resolution
- Neighbor unreachability detection
- Duplicate address detection
- Router/prefix discovery
- Address autoconfiguration
- Redirection

[Table 1-3](#) lists the types and functions of ICMPv6 messages used by the NDP.

Table 1-3 Types and functions of ICMPv6 messages

ICMPv6 message	Function
Neighbor solicitation (NS) message	Used to acquire the link-layer address of a neighbor
	Used to verify whether the neighbor is reachable
	Used to perform a duplicate address detection
Neighbor advertisement (NA) message	Used to respond to a neighbor solicitation message
	When the link layer address changes, the local node initiates a neighbor advertisement message to notify neighbor nodes of the change.
Router solicitation (RS) message	After started, a host sends a router solicitation message to request the router for an address prefix and other configuration information for the purpose of autoconfiguration.
Router advertisement (RA) message	Used to respond to a router solicitation message
	With the RA message suppression disabled, the router regularly sends a router advertisement message containing information such as address prefix and flag bits.
Redirect message	When a certain condition is satisfied, the default gateway sends a redirect message to the source host so that the host can reselect a correct next hop router to forward packets.



Note

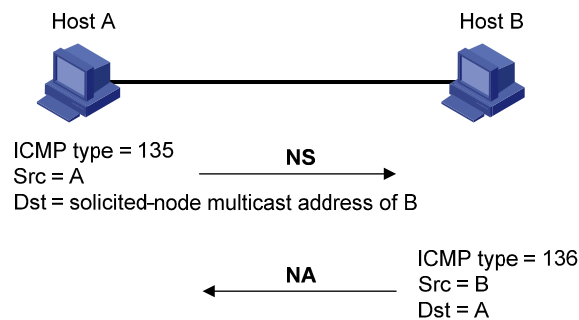
- H3C S3600 Series Ethernet Switches do not support the RS, RA, or Redirect message.
- Of the above mentioned IPv6 NDP functions, H3C S3600 Series Ethernet Switches support the following three functions: address resolution, neighbor unreachability detection, and duplicate address detection. The subsequent sections present a detailed description of these three functions and relevant configuration.

The NDP mainly provides the following functions:

Address resolution

Similar to the ARP function in IPv4, a node acquires the link-layer address of neighbor nodes on the same link through NS and NA messages. [Figure 1-3](#) shows how node A acquires the link-layer address of node B.

Figure 1-3 Address resolution



The address resolution procedure is as follows:

- 2) Node A multicasts an NS message. The source address of the NS message is the IPv6 address of the interface of node A and the destination address is the solicited-node multicast address of node B. The NS message contains the link-layer address of node A.
- 3) After receiving the NS message, node B judges whether the destination address of the packet is the corresponding solicited-node multicast address of its own IPv6 address. If yes, node B learns the link-layer address of node A and returns an NA message containing the link-layer address of node B in the unicast mode.
- 4) Node A acquires the link-layer address of node B from the NA message. After that, node A and node B can communicate with each other.

Neighbor unreachability detection

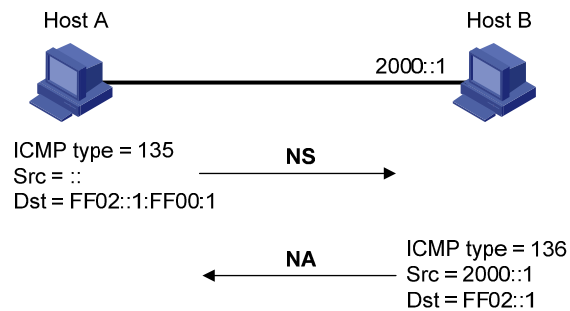
After node A acquires the link-layer address of its neighbor node B, node A can verify whether node B is reachable according to NS and NA messages.

- 1) Node A sends an NS message whose destination address is the IPv6 address of node B.
- 2) If node A receives an NA message from node B, node A considers that node B is reachable. Otherwise, node B is unreachable.

Duplicate address detection

After a node acquires an IPv6 address, it should perform the duplicate address detection to determine whether the address is being used by other nodes (similar to the gratuitous ARP function). The duplication address detection is accomplished through NS and NA messages. [Figure 1-4](#) shows the duplicate address detection procedure.

Figure 1-4 Duplicate address detection



The duplicate address detection procedure is as follows:

- 1) Node A sends an NS message whose source address is the unassigned address :: and the destination address is the corresponding solicited-node multicast address of the IPv6 address to be detected. The NS message also contains the IPv6 address.
- 2) If node B uses this IPv6 address, node B returns an NA message. The NA message contains the IPv6 address of node B.
- 3) Node A learns that the IPv6 address is being used by node B after receiving the NA message from node B. Otherwise, node B is not using the IPv6 address and node A can use it.

Introduction to IPv6 DNS

In the IPv6 network, a Domain Name System (DNS) supporting IPv6 converts domain names into IPv6 addresses. Different from an IPv4 DNS, an IPv6 DNS converts domain names into IPv6 addresses, instead of IPv4 addresses.

However, just like an IPv4 DNS, an IPv6 DNS also covers static domain name resolution and dynamic domain name resolution. The function and implementation of these two types of domain name resolution are the same as those of an IPv4 DNS. For details, refer to *DNS Operation* in this manual.

Usually, the DNS server connecting IPv4 and IPv6 networks contain not only A records (IPv4 addresses) but also AAAA records (IPv6 addresses). The DNS server can convert domain names into IPv4 addresses or IPv6 addresses. In this way, the DNS server has the functions of both IPv6 DNS and IPv4 DNS.

Protocols and Standards

Protocol specifications related to IPv6 include:

- RFC 1881: IPv6 Address Allocation Management
- RFC 1887: An Architecture for IPv6 Unicast Address Allocation
- RFC 1981: Path MTU Discovery for IP version 6
- RFC 2375: IPv6 Multicast Address Assignments
- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification.
- RFC 2461: Neighbor Discovery for IP Version 6 (IPv6)
- RFC 2462: IPv6 Stateless Address Autoconfiguration
- RFC 2463: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 2464: Transmission of IPv6 Packets over Ethernet Networks
- RFC 2526: Reserved IPv6 Subnet Anycast Addresses
- RFC 3307: Allocation Guidelines for IPv6 Multicast Addresses

- RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3596: DNS Extensions to Support IP Version 6

IPv6 Configuration Task List

Complete the following tasks to configure IPv6:

Task	Remarks
Configuring an IPv6 Unicast Address	Required
Configuring IPv6 NDP	Optional
Configuring a Static IPv6 Route	Optional
Configuring IPv6 TCP Properties	Optional
Configuring the Maximum Number of IPv6 ICMP Error Packets Sent within a Specified Time	Optional
Configuring the Hop Limit of ICMPv6 Reply Packets	Optional
Configuring IPv6 DNS	Optional
Displaying and Maintaining IPv6	Optional

Configuring an IPv6 Unicast Address

- An IPv6 address is required for a host to access an IPv6 network. A host can be assigned a global unicast address, a site-local address, or a link-local address.
- To enable a host to access a public IPv6 network, you need to assign an IPv6 global unicast address to it.

IPv6 site-local addresses and global unicast addresses can be configured in either of the following ways:

- EUI-64 format: When the EUI-64 format is adopted to form IPv6 addresses, the IPv6 address prefix of an interface is the configured prefix and the interface identifier is derived from the link-layer address of the interface.
- Manual configuration: IPv6 site-local addresses or global unicast addresses are configured manually.

IPv6 link-local addresses can be acquired in either of the following ways:

- Automatic generation: The device automatically generates a link-local address for an interface according to the link-local address prefix (FE80::/64) and the link-layer address of the interface.
- Manual assignment: IPv6 link-local addresses can be assigned manually.

Follow these steps to configure an IPv6 unicast address:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface <i>interface-type</i> <i>interface-number</i>	—

To do...		Use the command...	Remarks
Configure an IPv6 global unicast address or site-local address	Manually assign an IPv6 address	ipv6 address { <i>ipv6-address</i> <i>prefix-length</i> <i>ipv6-address/prefix-length</i> }	Use either command By default, no site-local address or global unicast address is configured for an interface.
	Adopt the EUI-64 format to form an IPv6 address	ipv6 address <i>ipv6-address/prefix-length</i> eui-64	Note that the prefix specified by the <i>prefix-length</i> argument in an EUI-64 address cannot exceed 64 bits in length.
Configure an IPv6 link-local address	Automatically generate a link-local address	ipv6 address auto link-local	Optional By default, after an IPv6 site-local address or global unicast address is configured for an interface, a link-local address will be generated automatically.
	Manually assign a link-local address for an interface.	ipv6 address <i>ipv6-address</i> link-local	



Note

- If IRF fabric ports are configured on an H3C S3600 switch, no IPv6 address can be configured for the switch.
- IPv6 unicast addresses can be configured for only one VLAN interface on an H3C S3600 Ethernet switch. The total number of global unicast addresses and site-local addresses on the VLAN interface can be up to four.
- After an IPv6 site-local address or global unicast address is configured for an interface, a link-local address will be generated automatically. The automatically generated link-local address is the same as the one generated by using the **ipv6 address auto link-local** command.
- The manual assignment takes precedence over the automatic generation. That is, if you first adopt the automatic generation and then the manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt the manual assignment and then the automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned one. If the manually assigned link-local address is deleted, the automatically generated link-local address takes effect.
- You must have carried out the **ipv6 address auto link-local** command before you carry out the **undo ipv6 address auto link-local** command. However, if an IPv6 site-local address or global unicast address is already configured for an interface, the interface still has a link-local address because the system automatically generates one for the interface. If no IPv6 site-local address or global unicast address is configured, the interface has no link-local address.

Configuring IPv6 NDP

Configuring a static neighbor entry

The IPv6 address of a neighbor node can be resolved into a link-layer address dynamically through NS and NA messages or statically through manual configuration.

You can configure a static neighbor entry in two ways:

- Mapping a VLAN interface to an IPv6 address and a link-layer address
- Mapping a port in a VLAN to an IPv6 address and a link-layer address

If you configure a static neighbor entry in the second way, make sure the corresponding VLAN interface exists. In this case, the device associates the VLAN interface to the IPv6 address to uniquely identify a static neighbor entry.

Follow these steps to configure a static neighbor entry:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a static neighbor entry	ipv6 neighbor <i>ipv6-address mac-address { vlan-id port-type port-number interface interface-type interface-number }</i>	Required

Configuring the maximum number of neighbors dynamically learned

The device can dynamically acquire the link-layer address of a neighbor node through NS and NA messages and add it to the neighbor table. Too large a neighbor table may lead to the forwarding performance degradation of the device. Therefore, you can restrict the size of the neighbor table by setting the maximum number of neighbors that an interface can dynamically learn. When the number of dynamically learned neighbors reaches the threshold, the interface will stop learning neighbor information.

Follow these steps to configure the maximum number of neighbors dynamically learned:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface <i>interface-type interface-number</i>	—
Configure the maximum number of neighbors dynamically learned by an interface	ipv6 neighbors max-learning-num <i>number</i>	Optional The default value is 2,048

Configuring the attempts to send an ns message for duplicate address detection

The device sends a neighbor solicitation (NS) message for duplicate address detection. If the device does not receive a response within a specified time (set by the **ipv6 nd ns retrans-timer** command), the device continues to send an NS message. If the device still does not receive a response after the number of attempts to send an NS message reaches the maximum, the device judges the acquired address is available.

Follow these steps to configure the attempts to send an NS message for duplicate address detection:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the attempts to send an NS message for duplicate address detection	ipv6 nd dad attempts <i>value</i>	Optional 1 by default. When the <i>value</i> argument is set to 0, the duplicate address detection is disabled.

Configuring the NS Interval

After a device sends an NS message, if it does not receive a response within a specific period, the device will send another NS message. You can configure the interval for sending NS messages.

Follow these steps to configure the NS interval:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Specify the NS interval	ipv6 nd ns retrans-timer <i>value</i>	Optional 1,000 milliseconds by default.

Configuring the neighbor reachable timeout time on an interface

After a neighbor passed the reachability detection, the device considers the neighbor to be reachable in a specific period. However, the device will examine whether the neighbor is reachable again when there is a need to send packets to the neighbor after the neighbor reachable timeout time elapsed.

Follow these steps to configure the neighbor reachable timeout time on an interface:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter VLAN interface view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the neighbor reachable timeout time	ipv6 nd nud reachable-time <i>value</i>	Optional 30,000 milliseconds by default.

Configuring a Static IPv6 Route

You can configure static IPv6 routes for network interconnection in a small sized IPv6 network.

Follow these steps to configure a static IPv6 route:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a static IPv6 route	ipv6 route-static <i>ipv6-address prefix-length</i> [<i>interface-type interface-number</i>] <i>nexthop-address</i>	Required By default, no static IPv6 route is configured.

Configuring IPv6 TCP Properties

The IPv6 TCP properties you can configure include:

- synwait timer: When a SYN packet is sent, the synwait timer is triggered. If no response packet is received before the synwait timer expires, the IPv6 TCP connection establishment fails.
- finwait timer: When the IPv6 TCP connection status is FIN_WAIT_2, the finwait timer is triggered. If no packet is received before the finwait timer expires, the IPv6 TCP connection is terminated. If FIN packets are received, the IPv6 TCP connection status becomes TIME_WAIT. If other packets are received, the finwait timer is reset from the last packet and the connection is terminated after the finwait timer expires.
- Size of IPv6 TCP receiving/sending buffer.

Follow these steps to configure IPv6 TCP properties:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the finwait timer of IPv6 TCP packets	tcp ipv6 timer fin-timeout <i>wait-time</i>	Optional 675 seconds by default.
Set the synwait timer of IPv6 TCP packets	tcp ipv6 timer syn-timeout <i>wait-time</i>	Optional 75 seconds by default.
Configure the size of IPv6 TCP receiving/sending buffer	tcp ipv6 window size	Optional 8 KB by default.

Configuring the Maximum Number of IPv6 ICMP Error Packets Sent within a Specified Time

If too many IPv6 ICMP error packets are sent within a short time in a network, network congestion may occur. To avoid network congestion, you can control the maximum number of IPv6 ICMP error packets sent within a specified time. Currently, the token bucket algorithm is adopted.

You can set the capacity of a token bucket, namely, the number of tokens in the bucket. In addition, you can set the update period of the token bucket, namely, the interval for updating the number of tokens in the token bucket to the configured capacity. One token allows one IPv6 ICMP error packet to be sent. Each time an IPv6 ICMP error packet is sent, the number of tokens in a token bucket decreases by 1. If the number of the IPv6 ICMP error packets that are continuously sent out reaches the capacity of the

token bucket, the subsequent IPv6 ICMP error packets cannot be sent out until new tokens are put into the token bucket based on the specified update frequency.

Follow these steps to configure the maximum number of IPv6 ICMP error packets sent within a specified time:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the maximum number of IPv6 ICMP error packets sent within a specified time	ipv6 icmp-error { bucket bucket-size ratelimit interval }*	Optional By default, the capacity of a token bucket is 10 and the update period is 100 milliseconds. That is, at most 10 IPv6 ICMP error packets can be sent within an update period.

Configuring the Hop Limit of ICMPv6 Reply Packets

When sending an ICMPv6 reply packet, the device will fill a configurable value in the Hop Limit field in the ICMPv6 reply packet header.

Follow these steps to configure the hop limit of ICMPv6 reply packets:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure the hop limit of ICMPv6 reply packets	ipv6 nd hop-limit value	Optional 64 by default.

Configuring IPv6 DNS

Configuring a static IPv6 DNS entry

You can directly use a host name when applying telnet applications and the system will resolve the host name into an IPv6 address. Each host name can correspond to only one IPv6 address. A newly configured IPv6 address will overwrite the previous one.

Follow these steps to configure a static IPv6 DNS entry:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a static IPv6 DNS entry	ipv6 host hostname ipv6-address	Required

Configuring dynamic DNS resolution

If you want to use the dynamic domain name function, you can use the following command to enable the dynamic domain name resolution function. In addition, you should configure a DNS server so that a query request message can be sent to the correct server for resolution. The system can support at most six DNS servers.

You can configure a domain name suffix so that you only need to enter some fields of a domain name and the system automatically adds the preset suffix for address resolution. The system can support at most 10 domain name suffixes.

Follow these steps to configure dynamic DNS resolution:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable the dynamic domain name resolution function	dns resolve	Required Disabled by default.
Configure an IPv6 DNS server	dns server ipv6 <i>ipv6-address</i> [<i>interface-type</i> <i>interface-number</i>]	Required If the IPv6 address of the DNS server is a link-local address, the <i>interface-type</i> and <i>interface-number</i> arguments are required.
Configure the domain suffix.	dns domain <i>domain-name</i>	Required By default, no domain name suffix is configured, that is, the domain name is resolved according to the input information.



Note

The **dns resolve** and **dns domain** commands are the same as those of IPv4 DNS. For details about the commands, refer to *DNS Operation* in this manual.

Displaying and Maintaining IPv6

To do...	Use the command...	Remarks
Display DNS domain name suffix information	display dns domain [dynamic]	Available in any view
Display IPv6 dynamic domain name cache information.	display dns ipv6 dynamic-host	
Display DNS server information	display dns server [dynamic]	
Display the FIB entries	display ipv6 fib	
Display the mapping between host name and IPv6 address	display ipv6 host	
Display the brief IPv6 information of an interface	display ipv6 interface [<i>interface-type</i> <i>interface-number</i> brief]	

To do...	Use the command...	Remarks
Display neighbor information	display ipv6 neighbors [<i>ipv6-address</i> all dynamic interface <i>interface-type</i> <i>interface-number</i> static vlan <i>vlan-id</i>] [[{ begin exclude include } <i>regular-expression</i>]	
Display the total number of neighbor entries satisfying the specified conditions	display ipv6 neighbors { all dynamic static interface <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-id</i> } count	
Display information about the routing table	display ipv6 route-table [verbose]	
Display information related to a specified socket	display ipv6 socket [socktype <i>socket-type</i>] [<i>task-id</i> <i>socket-id</i>]	
Display the statistics of IPv6 packets and IPv6 ICMP packets	display ipv6 statistics	
Display the statistics of IPv6 TCP packets	display tcp ipv6 statistics	
Display the IPv6 TCP connection status	display tcp ipv6 status	
Display the statistics of IPv6 UDP packets	display udp ipv6 statistics	
Clear IPv6 dynamic domain name cache information	reset dns ipv6 dynamic-host	Available in user view
Clear IPv6 neighbor information	reset ipv6 neighbors [all dynamic interface <i>interface-type</i> <i>interface-number</i> static]	
Clear the statistics of IPv6 packets	reset ipv6 statistics	
Clear the statistics of all IPv6 TCP packets	reset tcp ipv6 statistics	
Clear the statistics of all IPv6 UDP packets	reset udp ipv6 statistics	



Note

The **display dns domain** and **display dns server** commands are the same as those of IPv4 DNS. For details about the commands, refer to *DNS Operation* in this manual.

IPv6 Configuration Example

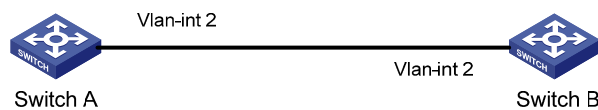
IPv6 Unicast Address Configuration

Network requirements

Two switches are directly connected through two Ethernet ports. The Ethernet ports belong to VLAN 2. Different types of IPv6 addresses are configured for the interface VLAN-interface 2 on each switch to verify the connectivity between the two switches. The IPv6 prefix in the EUI-64 format is 2001::/64, the global unicast address of Switch A is 3001::1/64, and the global unicast address of Switch B is 3001::2/64.

Network diagram

Figure 1-5 Network diagram for IPv6 address configuration



Configuration procedure

1) Configure Switch A.

Configure an automatically generated link-local address for the interface VLAN-interface 2.

```
<SwitchA> system-view
```

```
[SwitchA] interface Vlan-interface 2
```

```
[SwitchA-Vlan-interface2] ipv6 address auto link-local
```

Configure an EUI-64 address for the interface VLAN-interface 2.

```
[SwitchA-Vlan-interface2] ipv6 address 2001::/64 eui-64
```

Configure a global unicast address for the interface VLAN-interface 2.

```
[SwitchA-Vlan-interface2] ipv6 address 3001::1/64
```

2) Configure Switch B.

Configure an automatically generated link-local address for the interface VLAN-interface 2.

```
<SwitchA> system-view
```

```
[SwitchB] interface Vlan-interface 2
```

```
[SwitchB-Vlan-interface2] ipv6 address auto link-local
```

Configure an EUI-64 address for the interface VLAN-interface 2.

```
[SwitchB-Vlan-interface2] ipv6 address 2001::/64 eui-64
```

Configure a global unicast address for the interface VLAN-interface 2.

```
[SwitchB-Vlan-interface2] ipv6 address 3001::2/64
```

Verification

Display the brief IPv6 information of an interface on Switch A.

```
[SwitchA-Vlan-interface2] display ipv6 interface vlan-interface 2
```

```
Vlan-interface2 current state : UP
```

```
Line protocol current state : UP
```

```
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE49:8048
```

```

Global unicast address(es):
  2001::20F:E2FF:FE49:8048, subnet is 2001::/64
  3001::1, subnet is 3001::/64
Joined group address(es):
  FF02::1:FF00:1
  FF02::1:FF49:8048
  FF02::1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses

# Display the brief IPv6 information of the interface on Switch B.

[SwitchB-Vlan-interface2] display ipv6 interface Vlan-interface 2
Vlan-interface2 current state : UP
Line protocol current state : UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1
Global unicast address(es):
  2001::20F:E2FF:FE00:1, subnet is 2001::/64
  3001::2, subnet is 3001::/64
Joined group address(es):
  FF02::1:FF00:2
  FF02::1:FF00:1
  FF02::1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses

# On Switch A, ping the link-local address, EUI-64 address, and global unicast address of Switch B. If
the configurations are correct, the above three types of IPv6 addresses can be pinged.

```



Caution

When you use the **ping ipv6** command to verify the reachability of the destination, you must specify the “-i” keyword if the destination address is a link-local address. For the operation of IPv6 ping, refer to section [IPv6 Ping](#).

```

[SwitchA-Vlan-interface2] ping ipv6 FE80::20F:E2FF:FE00:1 -i Vlan-interface 2
PING FE80::20F:E2FF:FE00:1 : 56 data bytes, press CTRL_C to break
  Reply from FE80::20F:E2FF:FE00:1
    bytes=56 Sequence=1 hop limit=255 time = 80 ms
  Reply from FE80::20F:E2FF:FE00:1
    bytes=56 Sequence=2 hop limit=255 time = 60 ms

```



```

Reply from FE80::20F:E2FF:FE00:1
bytes=56 Sequence=3 hop limit=255 time = 60 ms
Reply from FE80::20F:E2FF:FE00:1
bytes=56 Sequence=4 hop limit=255 time = 70 ms
Reply from FE80::20F:E2FF:FE00:1
bytes=56 Sequence=5 hop limit=255 time = 60 ms
--- FE80::20F:E2FF:FE00:1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 60/66/80 ms

[SwitchA-Vlan-interface2] ping ipv6 2001::20F:E2FF:FE00:1
PING 2001::20F:E2FF:FE00:1 : 56 data bytes, press CTRL_C to break
Reply from 2001::20F:E2FF:FE00:1
bytes=56 Sequence=1 hop limit=255 time = 40 ms
Reply from 2001::20F:E2FF:FE00:1
bytes=56 Sequence=2 hop limit=255 time = 70 ms
Reply from 2001::20F:E2FF:FE00:1
bytes=56 Sequence=3 hop limit=255 time = 60 ms
Reply from 2001::20F:E2FF:FE00:1
bytes=56 Sequence=4 hop limit=255 time = 60 ms
Reply from 2001::20F:E2FF:FE00:1
bytes=56 Sequence=5 hop limit=255 time = 60 ms

--- 2001::20F:E2FF:FE00:1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 40/58/70 ms

[SwitchA-Vlan-interface2] ping ipv6 3001::2
PING 3001::2 : 56 data bytes, press CTRL_C to break
Reply from 3001::2
bytes=56 Sequence=1 hop limit=255 time = 50 ms
Reply from 3001::2
bytes=56 Sequence=2 hop limit=255 time = 60 ms
Reply from 3001::2
bytes=56 Sequence=3 hop limit=255 time = 60 ms
Reply from 3001::2
bytes=56 Sequence=4 hop limit=255 time = 70 ms
Reply from 3001::2
bytes=56 Sequence=5 hop limit=255 time = 60 ms

--- 3001::2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received

```

0.00% packet loss

round-trip min/avg/max = 50/60/70 ms

2 IPv6 Application Configuration

When configuring IPv6 application, go to these sections for information you are interested in:

- [Introduction to IPv6 Application](#)
- [Configuring IPv6 Application](#)
- [IPv6 Application Configuration Example](#)
- [Troubleshooting IPv6 Application](#)

Introduction to IPv6 Application

IPv6 are supporting more and more applications. Most of IPv6 applications are the same as those of IPv4. The applications supported on H3C S3600 Series Ethernet Switches are:

- Ping
- Traceroute
- TFTP
- Telnet

Configuring IPv6 Application

IPv6 Ping

The **ping ipv6** command is commonly used for testing the reachability of a host. This command sends an ICMPv6 message to the destination host and records the time for the response message to be received. For details about the **ping** command, refer to *System Maintenance and Debugging Operation* in this manual.

After you execute the **ping ipv6** command, you can press **Ctrl+C** to terminate the ping operation.

Follow these steps to ping IPv6:

To do...	Use the command...	Remarks
Ping IPv6	ping ipv6 [-a source-ipv6 -c count -m interval -s packet-size -t timeout]* remote-system [-i interface-type interface-number]	Required Available in any view



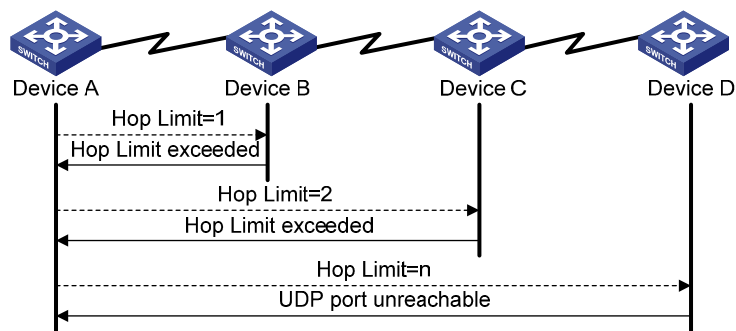
Caution

When you use the **ping ipv6** command to verify the reachability of the destination, you must specify the “-i” keyword if the destination address is a link-local address.

IPv6 Traceroute

The **traceroute ipv6** command is used to record the route of IPv6 packets from source to destination, so as to check whether the link is available and determine the point of failure.

Figure 2-1 Traceroute process



As [Figure 2-1](#) shows, the traceroute process is as follows:

- The source sends an IP datagram with the Hop Limit of 1.
- If the first hop device receiving the datagram reads the Hop Limit of 1, it will discard the packet and return an ICMP timeout error message. Thus, the source can get the first device's address in the route.
- The source sends a datagram with the Hop Limit of 2 and the second hop device returns an ICMP timeout error message. The source gets the second device's address in the route.
- This process continues until the datagram reaches the destination host. As there is no application using the UDP port, the destination returns a "port unreachable" ICMP error message.
- The source receives the "port unreachable" ICMP error message and understands that the packet has reached the destination, and thus determines the route of the packet from source to destination.

Follow these steps to traceroute IPv6:

To do...	Use the command...	Remarks
Traceroute IPv6	tracert ipv6 [-f <i>first-ttl</i> -m <i>max-ttl</i> -p <i>port</i> -q <i>packet-num</i> -w <i>timeout</i>]* <i>remote-system</i>	Required Available in any view

IPv6 TFTP

IPv6 supports Trivial File Transfer Protocol (TFTP). As a client, the device can download files from or upload files to a TFTP server. For details about TFTP, see *TFTP-SFTP-TFTP Operation*.

Configuration preparation

Enable TFTP on the TFTP server and specify the path to download or upload files. For specific operations, refer to TFTP server configuration specifications.

IPv6 TFTP configuration

Follow these steps to download or upload files to TFTP servers:

To do...	Use the command...	Remarks
Download/Upload files from TFTP server	tftp ipv6 <i>remote-system</i> [-i <i>interface-type</i> <i>interface-number</i>] { get put } <i>source-filename</i> [<i>destination-filename</i>]	Required Available in user view



Caution

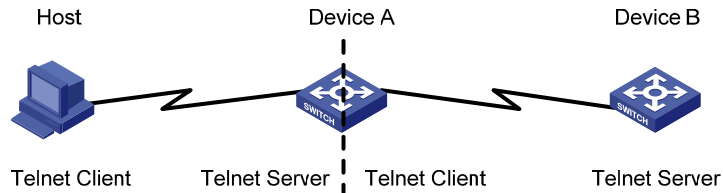
When you use the **tftp ipv6** command to connect to the TFTP server, you must specify the “-i” keyword if the destination address is a link-local address.

IPv6 Telnet

Telnet protocol belongs to application layer protocols of the TCP/IP protocol suite, and is used to provide remote login and virtual terminals. The device can be used either as a Telnet client or a Telnet server.

As the following figure shows, the Host is running Telnet client application of IPv6 to set up an IPv6 Telnet connection with Device A, which serves as the Telnet server. If Device A again connects to Device B through Telnet, the Device A is the Telnet client and Device B is the Telnet server.

Figure 2-2 Provide Telnet services



Configuration prerequisites

Enable Telnet on the Telnet server and configure the authentication method. For details, refer to *Login Operation* in this manual.

Follow these steps to set up IPv6 Telnet connections:

To do...	Use the command...	Remarks
Perform the telnet command on the Telnet client to log in to other devices	telnet ipv6 <i>remote-system</i> [-i <i>interface-type</i> <i>interface-number</i>] [<i>port-number</i>]	Required Available in user view



Caution

When you use the **telnet ipv6** command to connect to the Telnet server, you must specify the “-i” keyword if the destination address is a link-local address.

Displaying and maintaining IPv6 Telnet

To do...	Use the command...	Remarks
Display the use information of the users who have logged in	display users [all]	Available in any view

IPv6 Application Configuration Example

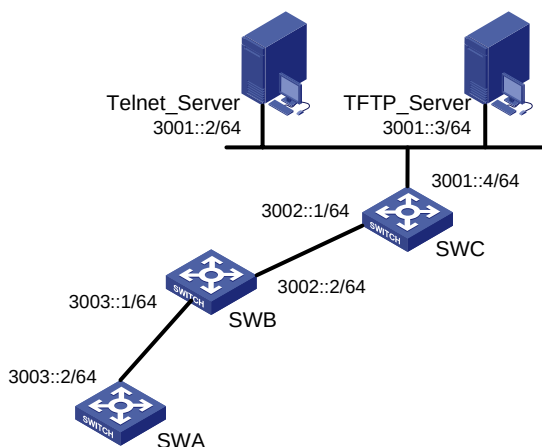
IPv6 Applications

Network requirements

In [Figure 2-3](#), SWA, SWB, and SWC are three switches, among which SWA is an H3C S3600 Ethernet switch, SWB and SWC are two switches supporting IPv6 forwarding. In a LAN, there is a Telnet server and a TFTP server for providing Telnet service and TFTP service to the switch respectively. It is required that you telnet to the telnet server from SWA and download files from the TFTP server.

Network diagram

Figure 2-3 Network diagram for IPv6 applications



Configuration procedure



Note

You need configure IPv6 address at the switch's and server's interfaces and ensure that the route between the switch and the server is accessible before the following configuration.

Ping SWB's IPv6 address from SWA.

```
<SWA> ping ipv6 3003::1
PING 3003::1 : 64 data bytes, press CTRL_C to break
  Reply from 3003::1:
    bytes=56 Sequence=1 hop limit=64  time = 110 ms
  Reply from 3003::1:
    bytes=56 Sequence=2 hop limit=64  time = 31 ms
  Reply from 3003::1:
    bytes=56 Sequence=3 hop limit=64  time = 31 ms
  Reply from 3003::1:
    bytes=56 Sequence=4 hop limit=64  time = 31 ms
  Reply from 3003::1:
    bytes=56 Sequence=5 hop limit=64  time = 31 ms

--- 3003::1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
    round-trip min/avg/max = 31/46/110 ms
```

On SWA, configure static routes to SWC, the Telnet Server, and the TFTP Server.

```
<SWA> system-view
[SWA] ipv6 route-static 3002:: 64 3003::1
[SWA] ipv6 route-static 3001:: 64 3003::1
[SWA] quit
```

Trace the IPv6 route from SWA to SWC.

```
<SWA> traceroute ipv6 3002::1
traceroute to 3002::1 30 hops max, 60 bytes packet
 1  3003::1 30 ms  0 ms  0 ms
 2  3002::1 10 ms 10 ms  0 ms
```

SWA downloads a file from TFTP server 3001::3.

```
<SWA> tftp ipv6 3001::3 get filetoget flash:/filegothere
.
File will be transferred in binary mode
Downloading file from remote tftp server, please wait....
TFTP:      13 bytes received in 1.243 second(s)
File downloaded successfully.
```

```
# SWA Connect to Telnet server 3001::2.  
  
<SWA> telnet ipv6 3001::2  
Trying 3001::2...  
Press CTRL+K to abort  
Connected to 3001::2 ...  
Telnet Server>
```

Troubleshooting IPv6 Application

Unable to Ping a Remote Destination

Symptom

Unable to ping a remote destination and return an error message.

Solution

- Check that the IPv6 addresses are configured correctly.
- Use the **display ipv6 interface** command to determine the interfaces of the source and the destination and the link-layer protocol between them are up.
- Use the **display ipv6 route-table** command to verify that the destination is reachable.
- Use the **ping ipv6 -t timeout { destination-ipv6-address | hostname } [-i interface-type interface-number]** command to increase the timeout time limit, so as to determine whether it is due to the timeout limit is too small.

Unable to Run Traceroute

Symptom

Unable to trace the route by performing traceroute operations.

Solution

- Check that the destination host can be pinged.
- If the host can be pinged through, check whether the UDP port that was included in the **tracert ipv6** command is used by an application on the host. If yes, you need to use the **tracert ipv6** command with an unreachable UDP port.

Unable to Run TFTP

Symptom

Unable to download and upload files by performing TFTP operations.

Solution

- Check that the route between the device and the TFTP server is up.
- Check that the file system of the device is usable. You can check it by running the **dir** command in user view.
- Check that the ACL configured for the TFTP server does not block the connection to the TFTP server.

Unable to Run Telnet

Symptom

Unable to login to Telnet server by performing Telnet operations.

Solution

- Check that the Telnet server application is running on the server. Check the configuration allows the server reachable.
- Check that the route between the device and the TFTP server is up.

Table of Contents

1 DNS Configuration	1-1
DNS Overview	1-1
Static Domain Name Resolution	1-1
Dynamic Domain Name Resolution	1-1
Configuring Domain Name Resolution	1-3
Configuring Static Domain Name Resolution	1-3
Configuring Dynamic Domain Name Resolution	1-3
Displaying and Maintaining DNS	1-4
DNS Configuration Examples	1-4
Static Domain Name Resolution Configuration Example	1-4
Dynamic Domain Name Resolution Configuration Example	1-5
Troubleshooting DNS	1-6

1 DNS Configuration

When configuring DNS, go to these sections for information you are interested in:

- [DNS Overview](#)
- [Configuring Domain Name Resolution](#)
- [Displaying and Maintaining DNS](#)
- [DNS Configuration Examples](#)
- [Troubleshooting DNS](#)



Note

This chapter covers only IPv4 DNS configuration. For details about IPv6 DNS, refer to *IPv6 Management Operation*.

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.

Currently, S3600 series Ethernet switches support both static and dynamic DNS clients.

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 domain name resolution table for applications, such as Telnet.

Dynamic Domain Name Resolution

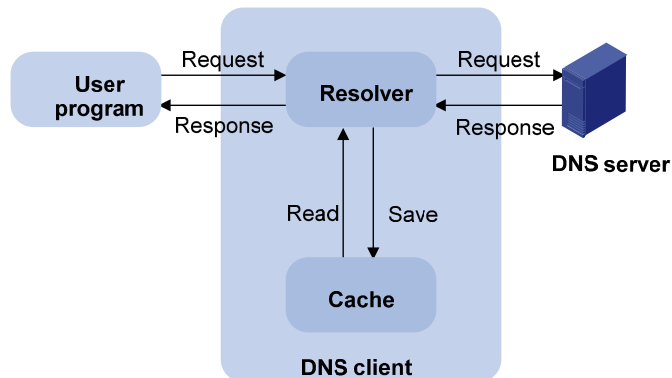
Resolution procedure

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-level 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, DNS client, and DNS server.

The resolver and cache comprise the DNS client. The user program and DNS client run on the same device, while the DNS server and the DNS client usually run on different devices.

Dynamic domain name resolution allows the DNS client to store latest mappings between name and IP address in the dynamic domain name cache of the DNS client. 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.

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 (automatic domain name addition). 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** and **aabbcc.**, the resolver will directly use this domain name to do DNS lookup first. If the lookup fails, the resolver adds a DNS suffix for another lookup.

Configuring Domain Name Resolution

Configuring Static Domain Name Resolution

Follow these steps to configure static domain name resolution:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Configure a mapping between a host name and an IP address	ip host <i>hostname ip-address</i>	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.

Configuring Dynamic Domain Name Resolution

Follow these steps to configure dynamic domain name resolution:

To do...	Use the command...	Remarks
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 <i>ip-address</i>	Required No IP address is configured for the DNS server by default.
Configure DNS suffixes	dns domain <i>domain-name</i>	Optional No DNS suffix is configured by default



Note

You may configure up to six DNS servers and ten DNS suffixes.

Displaying and Maintaining DNS

To do...	Use the command...	Remarks
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 }	
Clear the information in the dynamic domain name cache	reset dns dynamic-host	Available in user view

DNS Configuration Examples

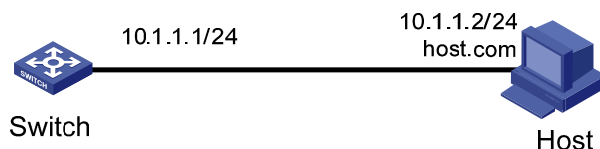
Static Domain Name Resolution Configuration Example

Network requirements

The switch uses static domain name resolution to access host 10.1.1.2 through domain name host.com.

Network diagram

Figure 1-2 Network diagram for static DNS configuration



Configuration procedure

Configure a mapping between host name host.com and IP address 10.1.1.2.

```
<Sysname> system-view
```

```
[Sysname] ip host host.com 10.1.1.2
```

Execute the **ping host.com** command to verify that the device can use static domain name resolution to get the IP address 10.1.1.2 corresponding to host.com.

```
[Sysname] ping host.com
```

```
PING host.com (10.1.1.2): 56 data bytes, press CTRL_C to break
```

```
Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=127 time=3 ms
```

```
Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=127 time=3 ms
```

```
Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=127 time=2 ms
```

```
Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=127 time=5 ms
```

```
Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=127 time=3 ms
```

```
--- host.com ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 2/3/5 ms
```

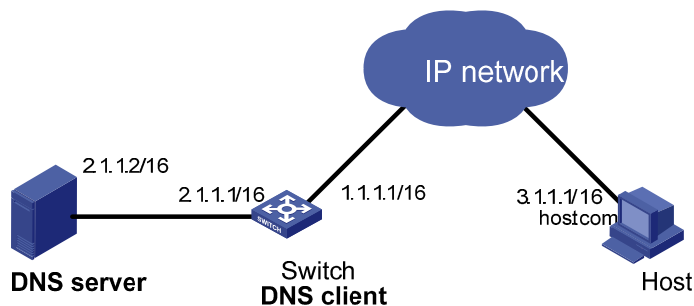
Dynamic Domain Name Resolution Configuration Example

Network requirements

As shown in [Figure 1-3](#), the switch serving as a DNS client uses dynamic domain name resolution to access the host at 3.1.1.1/16 through its domain name **host**. The DNS server has the IP address 2.1.1.2/16. The DNS suffix is **com**.

Network diagram

Figure 1-3 Network diagram for dynamic DNS configuration



Configuration procedure



Note

Before doing the following configuration, make sure that:

- The routes between the DNS server, Switch, and Host are reachable.
- Necessary configurations are done on the devices. For the IP addresses of the interfaces, see the figure above.
- There is a mapping between domain name **host** and IP address 3.1.1.1/16 on the DNS server.
- The DNS server works normally.

```
# Enable dynamic domain name resolution.
```

```
<Sysname> system-view
```

```
[Sysname] dns resolve
```

```
# Configure the IP address 2.1.1.2 for the DNS server.
```

```
[Sysname] dns server 2.1.1.2
```

```
# Configure com as the DNS suffix
```

```
[Sysname] dns domain com
```

Execute the **ping host** command on Switch to verify that the communication between Switch and Host is normal and that the corresponding IP address is 3.1.1.1.

```
[Sysname] ping host
Trying DNS server (2.1.1.2)
PING host.com (3.1.1.1): 56 data bytes, press CTRL_C to break
  Reply from 3.1.1.1: bytes=56 Sequence=1 ttl=125 time=4 ms
  Reply from 3.1.1.1: bytes=56 Sequence=2 ttl=125 time=4 ms
  Reply from 3.1.1.1: bytes=56 Sequence=3 ttl=125 time=4 ms
  Reply from 3.1.1.1: bytes=56 Sequence=4 ttl=125 time=4 ms
  Reply from 3.1.1.1: bytes=56 Sequence=5 ttl=125 time=5 ms

--- host.com ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 4/4/5 ms
```

Troubleshooting DNS

Symptom

After enabling the dynamic domain name resolution, the user cannot get the correct IP address.

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

1 Smart Link Configuration	1-1
Smart Link Overview	1-1
Basic Concepts in Smart Link	1-1
Operating Mechanism of Smart Link	1-3
Configuring Smart Link	1-3
Configuration Task List	1-3
Configuring a Smart Link Device	1-4
Configuring Associated Devices	1-5
Precautions	1-5
Displaying and Maintaining Smart Link	1-6
Smart Link Configuration Example	1-6
Implementing Link Redundancy Backup	1-6
2 Monitor Link Configuration	2-1
Introduction to Monitor Link	2-1
How Monitor Link Works	2-2
Configuring Monitor Link	2-3
Configuration Task List	2-3
Creating a Monitor Link Group	2-3
Configuring the Uplink Port	2-3
Configuring a Downlink Port	2-4
Displaying Monitor Link Configuration	2-5
Monitor Link Configuration Example	2-5
Implementing Collaboration Between Smart Link and Monitor Link	2-5

1 Smart Link Configuration

When configuring smart link, go to these sections for information you are interested in:

- [Smart Link Overview](#)
- [Configuring Smart Link](#)
- [Displaying and Maintaining Smart Link](#)
- [Smart Link Configuration Example](#)

Smart Link Overview

As shown in [Figure 1-1](#), dual-uplink networking is widely applied currently. Usually, Spanning Tree Protocol (STP) is used to implement link redundancy backup in the network. However, STP is not suitable for users with a high demand for convergence time. Smart Link can achieve active/standby link redundancy backup and fast convergence to meet the user demand.

Smart Link has the following features:

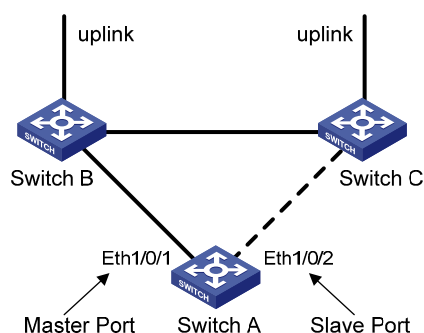
- Active/standby backup for dual-uplink networking
- Simple configuration and operation

Basic Concepts in Smart Link

Smart link group

A smart link group consists of two member ports, one master port and one slave port. Normally, only one port (master or slave) is active, and the other port is blocked, that is, in the standby state. When link failure occurs on the port in active state, the smart link group will block the port automatically and turn standby state to active state on the blocked port.

Figure 1-1 Network diagram of Smart Link



In [Figure 1-1](#), Ethernet 1/0/1 and Ethernet 1/0/2 on Switch A are two member ports of a smart link group.

Master port

The master port can be either an Ethernet port or a manually-configured or static LACP aggregation group. For example, you can configure Ethernet 1/0/1 of switch A in [Figure 1-1](#) as the master port through the command line.

Slave port

The slave port can be either an Ethernet port or a manually-configured or static LACP aggregation group. For example, you can configure Ethernet 1/0/2 of switch A in [Figure 1-1](#) as the slave port through the command line.

Flush message

When a forwarding link fails, the device will switch the traffic to the blocked standby link. The former forwarding entries of each device in the network are no longer suitable for the new topology, so MAC address forwarding entries and ARP entries must be updated throughout the network. In this case, the smart link group sends flush messages to notify other devices to refresh MAC address forwarding entries and ARP entries.

Control VLAN for sending flush messages

This control VLAN sends flush messages. When link switching occurs, the device (Switch A in [Figure 1-1](#)) broadcasts flush messages in this control VLAN.

Control VLAN for receiving flush messages

This control VLAN is used for receiving and processing flush messages. When link switching occurs, the devices (Switch B and Switch C in [Figure 1-1](#)) receive and process flush messages of this control VLAN, and then refresh MAC forwarding table entries and ARP entries.

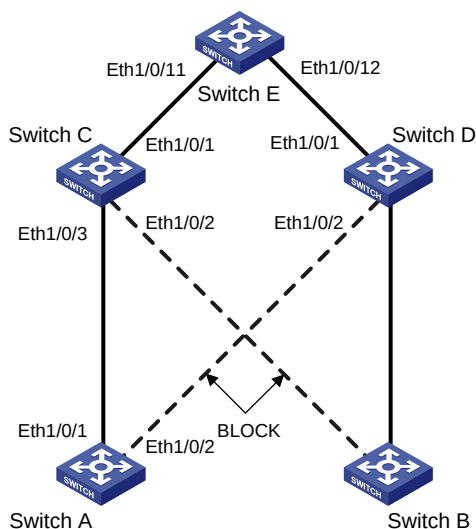


Note

- Currently, the member ports of a smart link group cannot be dynamic link aggregation groups.
 - If the master port or slave port of a smart link group is a link aggregation group, you cannot remove this link aggregation group directly or change the aggregation group into a dynamic aggregation group. Before removing this aggregation group, you must unbind the link aggregation group from the Smart Link.
-

Operating Mechanism of Smart Link

Figure 1-2 Network diagram of Smart Link operating mechanism



As shown in [Figure 1-2](#), Ethernet 1/0/1 on Switch A is active and Ethernet 1/0/2 on Switch A is blocked. When the link connected to Ethernet 1/0/1 fails, Ethernet 1/0/1 is blocked automatically, and the state of Ethernet 1/0/2 turns to active state.

- When link switching occurs in the smart link group, MAC forwarding entries and ARP entries of each device in the network may be out of date. In order to guarantee correct packet transmission, you must enable the Smart Link device to send flush messages to notify the other devices in the network to refresh their own MAC forwarding entries and ARP entries. In this case, all the uplink devices must be capable of identifying flush messages from the smart link group and refreshing MAC forwarding entries and ARP entries.
- On a Smart Link-enabled device, if a port is blocked due to link failure, the port remains blocked after the link recovers from the failure, and does not preempt the traffic resource. Therefore, the traffic stays stable. The port does not come into the forwarding state until the next link switching.

Configuring Smart Link



Note

Before configuring a member port of a smart link group, you must:

- Disable the port to avoid loops, thus preventing broadcast storm.
- Disable STP on the port.

After completing the configuration, you need to enable the Ethernet ports disabled before configuring the smart link group.

Configuration Task List

Complete the following tasks to configure Smart Link:

Task		Remarks
Configuring a Smart Link Device	Create a smart link group	Required
	Add member ports to the smart link group	
	Enable the function of sending flush messages in the specified control VLAN	
Configuring Associated Devices	Enable the function of processing flush messages received from the specified control VLAN	Required

Configuring a Smart Link Device

A Smart Link device refers to a device on which Smart Link is enabled and a smart link group is configured, and that sends flush messages from the specified control VLAN. A member port of a smart link group can be either an Ethernet port or a manually-configured or static LACP aggregation group. You can configure a port or a link aggregation group as a member of a smart link group.

Follow these steps to configure Smart Link (with ports as the members of the smart link group):

To do...		Use the command...	Remarks
Enter system view		system-view	—
Create a smart link group and enter smart link group view		smart-link group <i>group-id</i>	Required
Enable the function of sending flush messages in the specified control VLAN		flush enable control-vlan <i>vlan-id</i>	Required By default, no control VLAN for sending flush messages is specified.
Configure a port as a smart link group member	smart link group view	port <i>interface-type interface-number</i> { master slave }	Required Use either approach
	Ethernet port view	quit	
		interface <i>interface-type interface-number</i>	
		port smart-link group <i>group-id</i> { master slave }	

Follow these steps to configure Smart Link (with link aggregation groups are the members of the smart link group):

To do...		Use the command...	Remarks
Enter system view		system-view	—
Create a smart link group and enter smart link group view		smart-link group <i>group-id</i>	Required
Configure a link aggregation group as a member of the smart link group		link-aggregation group <i>group-id</i> { master slave }	Optional
Enable the function of sending flush messages in the specified control VLAN		flush enable control-vlan <i>vlan-id</i>	Optional By default, no control VLAN for sending flush messages is specified.

Configuring Associated Devices

An associated device mentioned in this document refers to a device that supports Smart Link and locally configured to process flush messages received from the specified control VLAN so as to work with the corresponding Smart Link device. As shown in [Figure 1-2](#), all the devices including Switch C, Switch D, and Switch E on the active and backup links connecting the Smart Link device (Switch A) and the target uplink device (Switch E) are all associated devices.

However, you do not have to enable all the ports of an associated device to process flush messages received from the specified control VLAN. You need to enable this function only on the ports that are on the active and backup links connecting the Smart Link device and the target device. As shown in [Figure 1-2](#), you need to enable this function on Ethernet 1/0/2 and Ethernet 1/0/3 of Switch C, Ethernet 1/0/2 and Ethernet 1/0/3 of Switch D, and Ethernet 1/0/11 and Ethernet 1/0/12 of Switch E.

Follow these steps to enable the specified port to process flush messages received from the specified control VLAN:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Enable the specified port(s) to process flush messages received from the control VLAN	System view	smart-link flush enable control-vlan <i>vlan-id</i> port <i>interface-type interface-number</i> [to <i>interface-type interface-number</i>]	Required, use either approach. By default, no control VLAN for receiving flush messages is specified.
	Ethernet port view	interface <i>interface-type interface-number</i>	
		smart-link flush enable control-vlan <i>vlan-id</i>	

Precautions

When configuring Smart Link, pay attention to the following points:

- 1) A port or a link aggregation group cannot serve as a member port for two smart link groups. On the other hand, a port or a link aggregation group cannot serve as a member for a smart link group and a monitor link group at the same time.
- 2) STP cannot be enabled on the member ports of a smart link group. An STP-enabled port or a link aggregation group with an STP-enabled port cannot serve as a member port for a smart link group.
- 3) A smart link/monitor link group with members cannot be deleted.
- 4) Smart Link/Monitor Link is mutually exclusive with remote port mirroring.
- 5) If you configure both the Smart Link and Monitor Link functions on an Intelligent Resilient Fabric (IRF) enabled device, the Smart Link and Monitor Link functions will function abnormally. Thus, you are recommended to disable the IRF function when configuring the Smart Link or Monitor Link function.
- 6) When a Combo port operates as a member port of a smart link group, the optical port and the electrical port of the Combo port must not be both engaged with a cable at the same time.
- 7) When you copy a port, the smart link/monitor link group member information configured on the port will not be copied to other ports.
- 8) If a single port is specified as a member of a smart link/monitor link group, you cannot execute the **lACP enable** command on this port or add this port into other dynamic link aggregation groups, because these operations will make this port become a link aggregation group member.
- 9) If no control VLAN is configured for flush message processing, the device will forward received flush messages without processing them.

- 10) If the control VLAN for receiving flush messages configured on an associated device is different than the one for sending flush messages configured on the corresponding Smart Link device, the device will forward received flush messages without processing them.
- 11) In the static or manual link aggregation group which serves as a smart link group member, if a member port can process flush messages, this function cannot be synchronized to the other ports in the aggregation group automatically, that is, the other member ports in the aggregation group cannot process flush messages. The function of processing flush messages must be manually configured for each port in the aggregation group.
- 12) The VLAN configured as a control VLAN to send and receive flush messages must exist. You cannot directly remove the control VLAN. When a dynamic VLAN is configured as the control VLAN for the smart link group, this VLAN will become a static VLAN, and the prompt information is displayed.

Displaying and Maintaining Smart Link

To do...	Use the command...	Remarks
Display the information of a smart link group	display smart-link group { <i>group-id</i> all }	Available in any view.
Display the statistics information of flush messages received and processed by the current device	display smart-link flush	
Clear flush message statistics	reset smart-link packets counter	Available in user view.

Smart Link Configuration Example

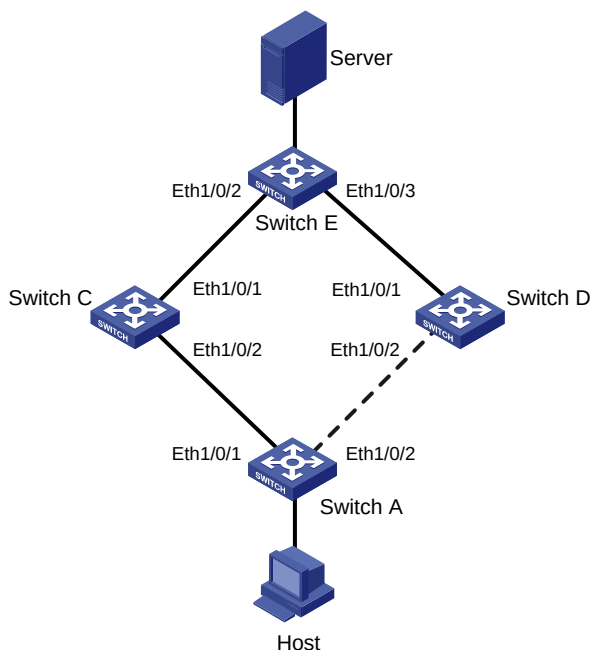
Implementing Link Redundancy Backup

Network requirements

As shown in [Figure 1-3](#), Switch A is an H3C S3600 series Ethernet switch. Switch C, Switch D and Switch E support Smart Link. Configure Smart Link feature to provide remote PCs with reliable access to the server.

Network diagram

Figure 1-3 Network diagram for Smart Link configuration



Configuration procedure

- 1) Configure a smart link group on Switch A and configure member ports for it. Enable the function of sending flush messages in Control VLAN 1.

Enter system view.

```
<switchA> system-view
```

Enter Ethernet port view. Disable STP on Ethernet 1/0/1 and Ethernet 1/0/2.

```
[SwitchA] interface Ethernet 1/0/1
```

```
[SwitchA-Ethernet1/0/1] stp disable
```

```
[SwitchA-Ethernet1/0/1] quit
```

```
[SwitchA] interface Ethernet 1/0/2
```

```
[SwitchA-Ethernet1/0/2] stp disable
```

Return to system view.

```
[SwitchA-Ethernet1/0/2] quit
```

Create smart link group 1 and enter the corresponding smart link group view.

```
[SwitchA] smart-link group 1
```

Configure Ethernet 1/0/1 as the master port and Ethernet 1/0/2 as the slave port for smart link group 1.

```
[SwitchA-smlk-group1] port Ethernet 1/0/1 master
```

```
[SwitchA-smlk-group1] port Ethernet 1/0/2 slave
```

Configure to send flush messages within VLAN 1.

```
[SwitchA-smlk-group1] flush enable control-vlan 1
```

- 2) Enable the function of processing flush messages received from VLAN 1 on Switch C.

Enter system view.

```
<SwitchC> system-view
```


Enable the function of processing flush messages received from VLAN 1 on Ethernet 1/0/2.

```
<SwitchC> smart-link flush enable control-vlan 1 port Ethernet 1/0/2
```

3) Enable the function of processing flush messages received from VLAN 1 on Switch D.

Enter system view.

```
<SwitchD> system-view
```

Enable the function of processing flush messages received from VLAN 1 on Ethernet 1/0/2.

```
[SwitchD] smart-link flush enable control-vlan 1 port Ethernet 1/0/2
```

4) Enable the function of processing flush messages received from VLAN 1 on Switch E.

Enter system view.

```
<SwitchE> system-view
```

Enable the function of processing flush messages received from VLAN 1 on Ethernet 1/0/2 and Ethernet 1/0/3.

```
[SwitchE] smart-link flush enable control-vlan 1 port Ethernet 1/0/2 to Ethernet 1/0/3
```

2 Monitor Link Configuration

When configuring Monitor Link, go to these sections for information you are interested in:

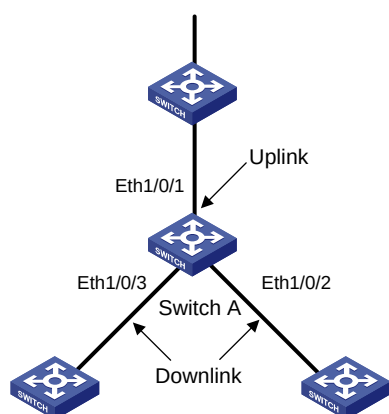
- [Introduction to Monitor Link](#)
- [Configuring Monitor Link](#)
- [Displaying Monitor Link Configuration](#)
- [Monitor Link Configuration Example](#)

Introduction to Monitor Link

Monitor Link is a collaboration scheme introduced to complement for Smart Link. It is used to monitor uplink and to perfect the backup function of Smart Link.

A monitor Link consists of an uplink port and one or multiple downlink ports. When the link for the uplink port of a monitor link group fails, all the downlink ports in the monitor link group are forced down. When the link for the uplink port recovers, all the downlink ports in the group are re-enabled.

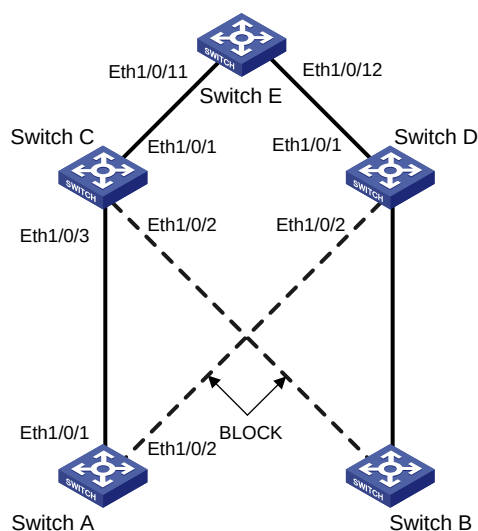
Figure 2-1 Network diagram for a monitor link group implementation



As shown in [Figure 2-1](#), the monitor link group configured on the device Switch A consists of an uplink port (Ethernet 1/0/1) and two downlink ports (Ethernet 1/0/2 and Ethernet 1/0/3). A member port can be an Ethernet port, static LACP aggregation group, manual link aggregation group, or smart link group. A smart link group can serve as the uplink port only.

How Monitor Link Works

Figure 2-2 Network diagram for a monitor link group implementation



As shown in [Figure 2-2](#), the devices Switch C and Switch D are connected to the uplink device Switch E. Switch C is configured with a monitor link group, where Ethernet 1/0/1 is the uplink port, while Ethernet 1/0/2 and Ethernet 1/0/3 are the downlink ports. Switch A is configured with a smart link group, where Ethernet 1/0/1 is the master port and Ethernet 1/0/2 is the slave port.

- If Switch C is not configured with monitor link group, when the link for the uplink port Ethernet 1/0/1 on Switch C fails, the links in the smart link group are not switched because the link for the master port Ethernet 1/0/1 of Switch A configured with smart link group operates normally. Actually, however, the traffic on Switch A cannot be up-linked to Switch E through the link of Ethernet 1/0/1.
- If Switch C is configured with monitor link group and monitor link group detects that the link for the uplink port Ethernet 1/0/1 fails, all the downlink ports in the group are shut down; therefore, Ethernet 1/0/3 on Switch C is blocked. Now, smart link group configured on Switch A detects that a link fault occurs on the master port Ethernet 1/0/1. Then, Smart Link immediately activates the slave port Ethernet 1/0/2 so that traffic is switched to the backup link.



Note

- Currently, member ports of a monitor link group cannot be dynamic link aggregation groups.
 - If the uplink or downlink port in the monitor link group is a link aggregation group, you cannot directly delete this aggregation group or change this aggregation group into a dynamic aggregation group. To delete this aggregation group, you must first unbind this aggregation group from the Monitor Link.
-

Configuring Monitor Link



Note

Before configuring a monitor link group, you must create a monitor link group and configure member ports for it. A monitor link group consists of an uplink port and one or multiple downlink ports. The uplink port can be a manually-configured or static LACP link aggregation group, an Ethernet port, or a smart link group. The downlink ports can be manually-configured link aggregation groups or static LACP link aggregation groups, or Ethernet ports.

Configuration Task List

Complete the following tasks to configure Monitor Link:

Task	Remarks
Creating a Monitor Link Group	Required
Configuring the Uplink Port	Required
Configuring a Downlink Port	Required

Creating a Monitor Link Group

Follow these steps to create a monitor link group:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a monitor link group	monitor-link group <i>group-id</i>	Required

Configuring the Uplink Port

Follow these steps to configure the uplink port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter the specified monitor link group view	monitor-link group <i>group-id</i>	—

To do...			Use the command...	Remarks
Configure the uplink port for the monitor link group	Configure the specified link aggregation group as the uplink port of the monitor link group		link-aggregation group <i>group-id uplink</i>	Required Use any of the three approaches
	Configure the specified smart link group as the uplink port of the monitor link group		smart-link group <i>group-id uplink</i>	
	Configure the specified Ethernet port as the uplink port of the monitor link group	Monitor link group view	port <i>interface-type interface-number uplink</i>	
		Ethernet port view	quit	
			interface <i>interface-type interface-number</i>	
			port monitor-link group <i>group-id uplink</i>	

Configuring a Downlink Port

Follow these steps to configure a downlink port:

To do...			Use the command...	Remarks
Enter system view			system-view	—
Enter the specified monitor link group view			monitor-link group <i>group-id</i>	Required
Configure a downlink port for the monitor link group	Configure the specified link aggregation group as a downlink port of the monitor link group		link-aggregation group <i>group-id downlink</i>	Required Use either approach
	Configure the specified Ethernet port as a downlink port of the monitor link group	Monitor link group view	port <i>interface-type interface-number downlink</i>	
		Ethernet port view	quit	
			interface <i>interface-type interface-number</i>	
			port monitor-link group <i>group-id downlink</i>	



Caution

- A smart link/monitor link group with members cannot be deleted. A smart link group as a monitor link group member cannot be deleted.
 - The smart link/monitor link function and the port mirroring function are incompatible with each other.
 - If a single port is specified as a smart link/monitor link group member, do not use the **lacp enable** command on the port or add the port to another dynamic link aggregation group because doing so will cause the port to become an aggregation group member.
 - Using the copy command on a port does not copy the smart link/monitor link group member information configured on the port to any other port.
-

Displaying Monitor Link Configuration

To do...	Use the command...	Remarks
Display the information about one or all monitor link groups	display monitor-link group { <i>group-id</i> all }	Available in any view.

Monitor Link Configuration Example

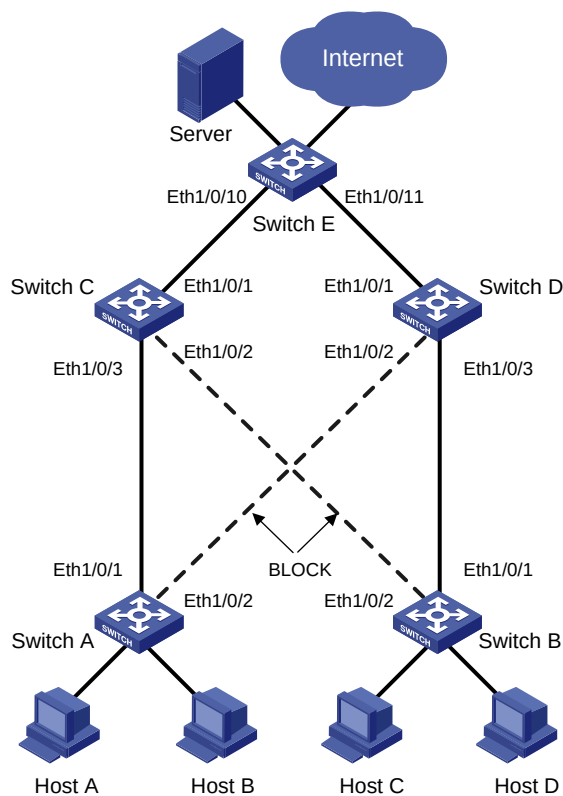
Implementing Collaboration Between Smart Link and Monitor Link

Network requirements

As shown in [Figure 2-3](#), the PCs access the server and Internet through the switch. Configure Smart Link and Monitor Link to prevent the PCs from failing to access the server and Internet due to uplink link or port failure.

Network diagram

Figure 2-3 Network diagram for Monitor Link configuration



Configuration procedure

- 1) Enable Smart Link on Switch A and Switch B to implement link redundancy backup. Perform the following configuration on Switch A. The configuration on Switch B is the same as on Switch A.

Enter system view.

```
<switchA> system-view
```

Enter Ethernet port view. Disable STP on Ethernet1/0/1 and Ethernet1/0/2.

```
[SwitchA] interface Ethernet 1/0/1
[SwitchA-Ethernet1/0/1] stp disable
[SwitchA-Ethernet1/0/1] quit
[SwitchA] interface Ethernet 1/0/2
[SwitchA-Ethernet1/0/2] stp disable
```

Return to system view.

```
[SwitchA-Ethernet1/0/2] quit
```

Create smart link group 1 and enter smart link group view.

```
[SwitchA] smart-link group 1
```

Configure Ethernet 1/0/1 as the master port of the smart link group and Ethernet 1/0/2 as the slave port.

```
[SwitchA-smlk-group1] port Ethernet 1/0/1 master
[SwitchA-smlk-group1] port Ethernet 1/0/2 slave
```

Configure to send flush messages in VLAN 1.

```
[SwitchA-smk-group1] flush enable control-vlan 1
```

- 2) Enable Monitor Link on Switch C and Switch D and enable the function of processing flush messages received from VLAN 1. Perform the following configuration on Switch C. The operation procedure on Switch D is the same as that performed on Switch C.

Enter system view.

```
<SwitchC> system-view
```

Create monitor link group 1 and enter monitor link group view

```
[SwitchC] monitor-link group 1
```

Configure Ethernet 1/0/1 as the uplink port of the monitor link group and Ethernet 1/0/2 and Ethernet 1/0/3 as the downlink ports.

```
[SwitchC-mtlk-group1] port Ethernet 1/0/1 uplink
```

```
[SwitchC-mtlk-group1] port Ethernet 1/0/2 downlink
```

```
[SwitchC-mtlk-group1] port Ethernet 1/0/3 downlink
```

Return to system view. Enable the function of processing flush messages received from VLAN 1 on Ethernet 1/0/2 and Ethernet 1/0/3.

```
[SwitchC-mtlk-group1] quit
```

```
[SwitchC] smart-link flush enable control-vlan 1 port Ethernet 1/0/2 to Ethernet 1/0/3
```

- 3) Enable the function of processing flush messages received from VLAN 1 on Ethernet 1/0/10 and Ethernet 1/0/11 of Switch E.

Enter system view.

```
<SwitchE> system-view
```

Enable the function of processing flush messages received from VLAN 1 on Ethernet 1/0/10 and Ethernet 1/0/11.

```
[SwitchE] smart-link flush enable control-vlan 1 port Ethernet 1/0/10 to Ethernet 1/0/11
```


Table of Contents

1 Access Management Configuration	1-1
Access Management Overview	1-1
Configuring Access Management	1-2
Access Management Configuration Examples	1-2
Access Management Configuration Example	1-2
Combining Access Management with Port Isolation	1-3

1 Access Management Configuration

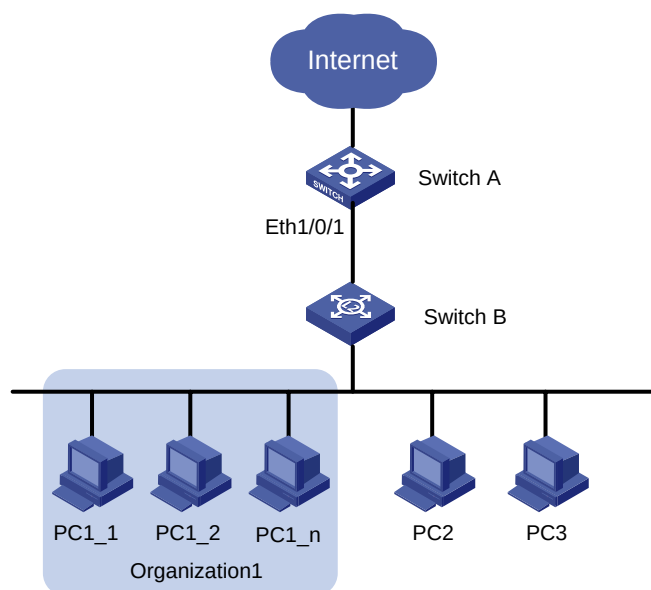
When configuring access management, go to these sections for information you are interested in:

- [Access Management Overview](#)
- [Configuring Access Management](#)
- [Access Management Configuration Examples](#)

Access Management Overview

Normally, client PCs in a network are connected to switches operating on the network access layer (also referred to as access switches) through Layer 2 switches; and the access switches provide external network accesses for the client PCs through their upstream links. In the network shown in [Figure 1-1](#), Switch A is an access switch; Switch B is a Layer 2 switch.

Figure 1-1 Typical Ethernet access networking scenario



The access management function aims to manage user access rights on access switches. It enables you to manage the external network access rights of the hosts connected to ports of an access switch. To implement the access management function, you need to configure an IP address pool on a port of an access switch, that is, bind a specified range of IP addresses to the port.

- A port with an access management IP address pool configured only allows the hosts with their IP addresses in the access management IP address pool to access external networks.
- A port without an access management IP address pool configured allows the hosts to access external networks only if their IP addresses are not in the access management IP address pools of other ports of the switch.

Note that the IP addresses in the access management IP address pool configured on a port must be in the same network segment as the IP address of the VLAN (where the port belongs to) interface.

Configuring Access Management

Follow these steps to configure access management:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable access management function	am enable	Required By default, the system disables the access management function.
Enable access management trap	am trap enable	Required By default, access management trap is disabled
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	—
Configure the access management IP address pool of the port	am ip-pool <i>address-list</i>	Required By default, no access management IP address pool is configured.
Display current configuration of access management	display am [<i>interface-list</i>]	Execute this command in any view.



Note

- Before configuring the access management IP address pool of a port, you need to configure the interface IP address of the VLAN to which the port belongs, and the IP addresses in the access management IP address pool of a port must be in the same network segment as the interface IP address of the VLAN which the port belongs to.
- If an access management address pool configured contains IP addresses that belong to the static ARP entries of other ports, the system prompts you to delete the corresponding static ARP entries to ensure the access management IP address pool can take effect.
- To allow only the hosts with their IP addresses in the access management address pool of a port to access external networks, do not configure static ARP entries for IP addresses not in the IP address pool.

Access Management Configuration Examples

Access Management Configuration Example

Network requirements

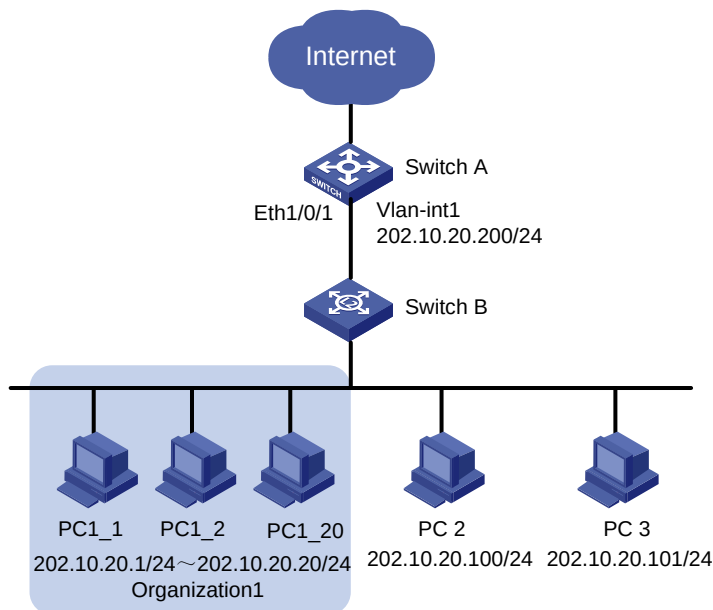
Client PCs are connected to the external network through Switch A (an Ethernet switch). The IP addresses of the PCs of Organization 1 are in the range 202.10.20.1/24 to 202.10.20.20/24. The IP address of PC 2 is 202.10.20.100/24, and that of PC 3 is 202.10.20.101/24.

- Allow the PCs of Organization 1 to access the external network through Ethernet 1/0/1 on Switch A. The port belongs to VLAN 1, and the IP address of VLAN-interface 1 is 202.10.20.200/24.

- Disable the PCs that are not of Organization 1 (PC 2 and PC 3) from accessing the external network through Ethernet 1/0/1 of Switch A.

Network diagram

Figure 1-2 Network diagram for access management configuration



Configuration procedure

Perform the following configuration on Switch A.

Enable access management.

```
<Sysname> system-view
```

```
[Sysname] am enable
```

Set the IP address of VLAN-interface 1 to 202.10.20.200/24.

```
[Sysname] interface Vlan-interface 1
```

```
[Sysname-Vlan-interface1] ip address 202.10.20.200 24
```

```
[Sysname-Vlan-interface1] quit
```

Configure the access management IP address pool on Ethernet 1/0/1.

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] am ip-pool 202.10.20.1 20
```

Combining Access Management with Port Isolation

Network requirements

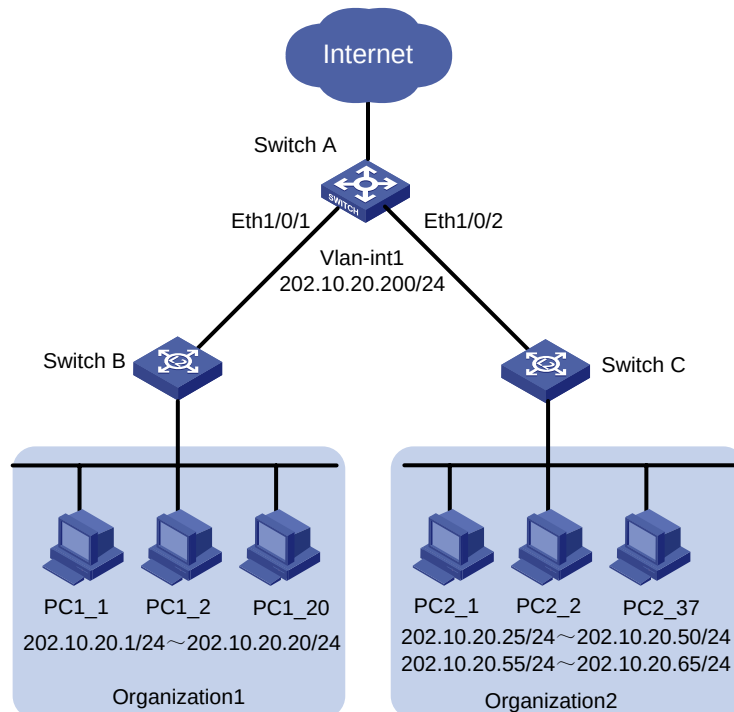
Client PCs are connected to the external network through Switch A (an Ethernet switch). The IP addresses of the PCs of Organization 1 are in the range 202.10.20.1/24 to 202.10.20.20/24, and those of the PCs in Organization 2 are in the range 202.10.20.25/24 to 202.10.20.50/24 and the range 202.10.20.55 to 202.10.20.65/24.

- Allow the PCs of Organization 1 to access the external network through Ethernet 1/0/1 of Switch A.
- Allow the PCs of Organization 2 to access the external network through Ethernet 1/0/2 of Switch A.

- Ethernet 1/0/1 and Ethernet 1/0/2 belong to VLAN 1. The IP address of VLAN-interface 1 is 202.10.20.200/24.
- PCs of Organization 1 are isolated from those of Organization 2 on Layer 2.

Network diagram

Figure 1-3 Network diagram for combining access management and port isolation



Configuration procedure

Perform the following configuration on Switch A.

For information about port isolation and the corresponding configuration, refer to the *Port Isolation Operation*.

Enable access management.

```
<Sysname> system-view
[Sysname] am enable
```

Set the IP address of VLAN-interface 1 to 202.10.20.200/24.

```
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ip address 202.10.20.200 24
[Sysname-Vlan-interface1] quit
```

Configure the access management IP address pool on Ethernet 1/0/1.

```
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] am ip-pool 202.10.20.1 20
```

Add Ethernet 1/0/1 to the port isolation group.

```
[Sysname-Ethernet1/0/1] port isolate
[Sysname-Ethernet1/0/1] quit
```

Configure the access management IP address pool on Ethernet 1/0/2.

```
[Sysname] interface Ethernet 1/0/2
```

```
[Sysname-Ethernet1/0/2] am ip-pool 202.10.20.25 26 202.10.20.55 11
```

```
# Add Ethernet 1/0/2 to the port isolation group.
```

```
[Sysname-Ethernet1/0/2] port isolate
```

```
[Sysname-Ethernet1/0/2] quit
```

Table of Contents

1 LLDP Configuration	1-1
Overview	1-1
Background	1-1
Basic Concepts	1-2
Operating Modes of LLDP	1-5
How LLDP Works	1-6
Protocols and Standards	1-6
LLDP Configuration Task List	1-6
Performing Basic LLDP Configuration	1-7
Enabling LLDP	1-7
Setting LLDP Operating Mode	1-7
Setting the LLDP Re-Initialization Delay	1-8
Enabling LLDP Polling	1-8
Configuring the TLVs to Be Advertised	1-8
Configuring the Management Address	1-9
Setting Other LLDP Parameters	1-9
Setting an Encapsulation Format for LLDPDUs	1-10
Configuring CDP Compatibility	1-10
Configuration Prerequisites	1-11
Configuring CDP Compatibility	1-11
Configuring LLDP Trapping	1-12
Displaying and Maintaining LLDP	1-12
LLDP Configuration Examples	1-13
Basic LLDP Configuration Example	1-13
CDP-Compatible LLDP Configuration Example	1-15

1 LLDP Configuration

When configuring LLDP, go to these sections for information you are interested in:

- [Overview](#)
- [LLDP Configuration Task List](#)
- [Performing Basic LLDP Configuration](#)
- [Configuring CDP Compatibility](#)
- [Configuring LLDP Trapping](#)
- [Displaying and Maintaining LLDP](#)
- [LLDP Configuration Examples](#)



Note

S3600 series Ethernet Switches support LLDP in Release 1702.

Overview

Background

In a heterogeneous network, it is important that different types of network devices from different vendors can discover one other and exchange configuration for interoperability and management sake. This calls for a standard configuration exchange platform.

To address the needs, the IETF drafted the Link Layer Discovery Protocol (LLDP) in IEEE 802.1AB. The protocol operates on the data link layer to exchange device information between directly connected devices. With LLDP, a device sends local device information (including its major functions, management IP address, device ID, and port ID) as TLV (type, length, and value) triplets in LLDPDUs to the directly connected devices, and at the same time, stores the device information received in LLDPDUs sent from the LLDP neighbors in a standard management information base (MIB). It allows a network management system to fast detect Layer-2 network topology change and identify what the change is.



Note

For more information about MIBs, refer to *SNMP-RMON Operation* in this manual.

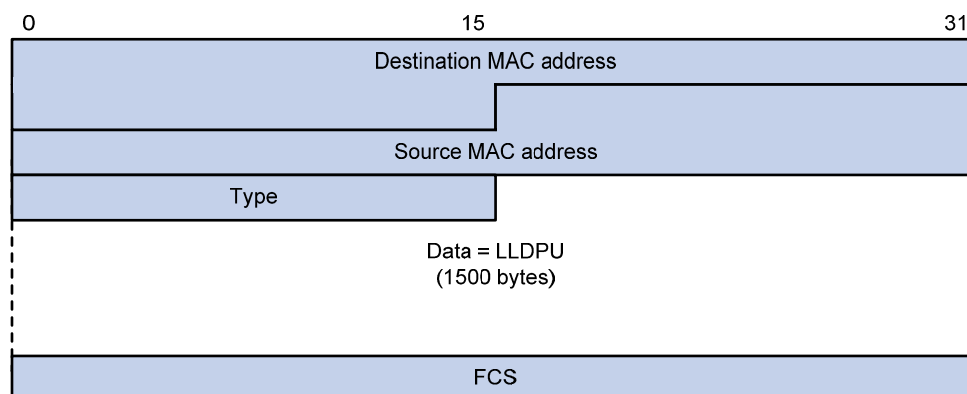
Basic Concepts

LLDP frames

LLDP sends device information in LLDP data units (LLDPDUs). LLDPDUs are encapsulated in Ethernet II or SNAP frames.

1) Ethernet II-encapsulated LLDP frame format

Figure 1-1 Ethernet II-encapsulated LLDP frame format



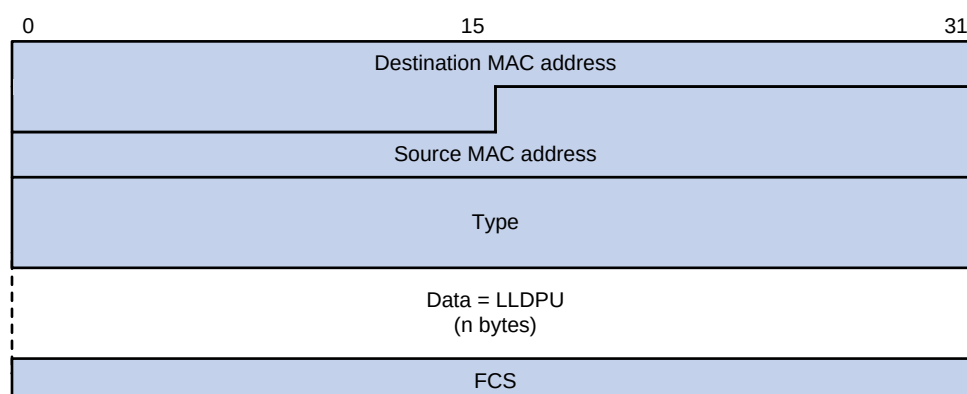
The fields in the frame are described in [Table 1-1](#):

Table 1-1 Description of the fields in an Ethernet II-encapsulated LLDP frame

Field	Description
Destination MAC address	The MAC address to which the LLDPDU is advertised. It is fixed to 0x0180-C200-000E, a multicast MAC address.
Source MAC address	The MAC address of the sending port. If the port does not have a MAC address, the MAC address of the sending bridge is used.
Type	The Ethernet type for the upper layer protocol. It is 0x88CC for LLDP.
Data	LLDP data unit (LLDPDU).
FCS	Frame check sequence, a 32-bit CRC value used to determine the validity of the received Ethernet frame.

2) SNAP-encapsulated LLDP frame format

Figure 1-2 SNAP-encapsulated LLDP frame format



The fields in the frame are described in [Table 1-2](#):

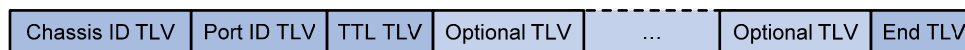
Table 1-2 Description of the fields in a SNAP-encapsulated LLDP frame

Field	Description
Destination MAC address	The MAC address to which the LLDPDU is advertised. It is fixed to 0x0180-C200-000E, a multicast MAC address.
Source MAC address	The MAC address of the sending port. If the port does not have a MAC address, the MAC address of the sending bridge is used.
Type	The SNAP type for the upper layer protocol. It is 0xAAAA-0300-0000-88CC for LLDP.
Data	LLDPDU.
FCS	Frame check sequence, a 32-bit CRC value used to determine the validity of the received Ethernet frame.

LLDPDUs

LLDP uses LLDPDUs to exchange information. An LLDPDU comprises multiple type, length, and value (TLV) sequences, each carrying a type of device information, as shown in [Figure 1-3](#).

Figure 1-3 An LLDPDU



An LLDPDU can carry up to 28 types of TLVs, of which the chassis ID TLV, port ID TLV, TTL TLV, and end of LLDPDU TLV (end TLV in the figure) are mandatory TLVs that must be carried and other TLVs are optional.

TLVs

TLVs are type, length, and value sequences that carry information elements, where the type field identifies the type of information, the length field indicates the length of the information field in octets, and the value field contains the information itself.

LLDPDU TLVs fall into these categories: basic management TLVs, organizationally (IEEE 802.1 and IEEE 802.3) specific TLVs, and LLDP-MED (media endpoint discovery) TLVs. Basic management TLVs are essential to device management. Organizationally specific TLVs and LLDP-MED TLVs are used for enhanced device management; they are defined by standardization or other organizations and thus are optional to LLDPDUs.

1) Basic management TLVs

[Table 1-1](#) lists the basic management TLV types currently in use. Some of them are mandatory to LLDPDUs, that is, must be included in every LLDPDU.

Table 1-3 Basic LLDP TLVs

Type	Description	Remarks
Chassis ID	Bridge MAC address of the sending device.	Mandatory

Type	Description	Remarks
Port ID	ID of the sending port. If MED TLVs are included in the LLDPDU, the port ID TLV carries the MAC address of the sending port or the bridge MAC in case the port does not have a MAC address. If no MED TLVs are included, the port ID TLV carries the port name.	
Time To Live	Life of the transmitted information on the receiving device.	
End of LLDPDU	Marks the end of the TLV sequence in the LLDPDU.	
Port Description	Port description of the sending port.	
System Name	Assigned name of the sending device.	Optional
System Description	Description of the sending device.	
System Capabilities	Identifies the primary functions of the sending device and the primary functions that have been enabled.	
Management Address	Management address used to reach higher level entities to assist discovery by network management, and the interface number and OID (object identifier) associated with the address.	

2) IEEE 802.1 organizationally specific TLVs

Table 1-4 IEEE 802.1 organizationally specific TLVs

Type	Description
Port VLAN ID	PVID of the sending port
Port And Protocol VLAN ID	Port and protocol VLAN IDs
VLAN Name	A specific VLAN name on the port
Protocol Identity	Protocols supported on the port



Note

Currently, H3C devices support receiving but not sending protocol identity TLVs.

3) IEEE 802.3 organizationally specific TLVs

Table 1-5 IEEE 802.3 organizationally specific TLVs

Type	Description
MAC/PHY Configuration/Status	Contains the rate and duplex capabilities of the sending port, support for auto negotiation, enabling status of auto negotiation, and the current rate and duplex mode.
Power Via MDI	Contains Power supply capability of the port, including the PoE type (PSE or PD), PoE mode, support for the PSE power supply, whether PSE power supply is enabled, and whether the PoE mode is controllable.

Type	Description
Link Aggregation	Indicates the support of the port for link aggregation, the aggregation capability of the port, and the aggregation status (that is, whether the link is in an aggregation).
Maximum Frame Size	Indicates the supported maximum frame size. It is now the MTU of the port.

LLDP-MED TLVs

LLDP-MED TLVs provide multiple advanced applications for voice over IP (VoIP), such as basic configuration, network policy configuration, and address and directory management. LLDP-MED TLVs satisfy the voice device vendors' requirements for cost effectiveness, ease of deployment, and ease of management. In addition, LLDP-MED TLVs make deploying voice devices in Ethernet easier. LLDP-MED TLVs are shown in [Table 1-6](#):

Table 1-6 LLDP-MED TLVs

Type	Description
LLDP-MED Capabilities	Allows a MED endpoint to advertise the supported LLDP-MED TLVs and its device type.
Network Policy	Allows a network device or MED endpoint to advertise LAN type and VLAN ID of the specific port, and the Layer 2 and Layer 3 priorities for a specific set of applications.
Extended Power-via-MDI	Allows a network device or MED endpoint to advertise power-related information (according to IEEE 802.3AF).
Hardware Revision	Allows a MED endpoint device to advertise its hardware version.
Firmware Revision	Allows a MED endpoint to advertise its firmware version.
Software Revision	Allows a MED endpoint to advertise its software version.
Serial Number	Allows an LLDP-MED endpoint device to advertise its serial number.
Manufacturer Name	Allows a MED endpoint to advertise its vendor name.
Model Name	Allows a MED endpoint to advertise its model name.
Asset ID	Allows a MED endpoint to advertise its asset ID. The typical case is that the user specifies the asset ID for the endpoint to facilitate directory management and asset tracking.
Location Identification	Allows a network device to advertise the appropriate location identifier information for an endpoint to use in the context of location-based applications.

Management address

The management address of a device is used by the network management system to identify and manage the device for topology maintenance and network management. The management address is encapsulated in the management address TLV.

Operating Modes of LLDP

LLDP can operate in one of the following modes:

- TxRx mode. A port in this mode sends and receives LLDP frames.
- Tx mode. A port in this mode only sends LLDP frames.
- Rx mode. A port in this mode only receives LLDP frames.
- Disable mode. A port in this mode does not send or receive LLDP frames.

Each time the LLDP operating mode of a port changes, its LLDP protocol state machine re-initializes. To prevent LLDP from being initialized too frequently at times of frequent operating mode change, an initialization delay, which is user configurable, is introduced. With this delay mechanism, a port must wait for the specified interval before it can initialize LLDP after the LLDP operating mode changes.

How LLDP Works

Transmitting LLDP frames

An LLDP-enabled port operating in TxRx mode or Tx mode sends LLDP frames to its directly connected devices both periodically and when the local configuration changes. To prevent the network from being overwhelmed by LLDP frames at times of frequent local device information change, an interval is introduced between two successive LLDP frames.

This interval is shortened to 1 second in either of the following two cases:

- A new neighbor is discovered, that is, a new LLDP frame is received carrying device information new to the local device.
- The LLDP operating mode of the port changes from Disable/Rx to TxRx or Tx.

This is the fast sending mechanism of LLDP. With this mechanism, a specific number of LLDP frames are sent successively at the 1-second interval to help LLDP neighbors discover the local device as soon as possible. Then, the normal LLDP frame transmit interval resumes.

Receiving LLDP frames

An LLDP-enabled port operating in TxRx mode or Rx mode checks the TLVs carried in every LLDP frame it receives for validity violation. If valid, the information is saved and an aging timer is set for it based on the time to live (TTL) TLV carried in the LLDPDU. If the TTL TLV is zero, the information is aged out immediately.

Protocols and Standards

The protocols and standards related to LLDP include:

- IEEE 802.1AB-2005, *Station and Media Access Control Connectivity Discovery*
- ANSI/TIA-1057, *Link Layer Discovery Protocol for Media Endpoint Devices*

LLDP Configuration Task List

Complete these tasks to configure LLDP:

Task		Remarks
Performing Basic LLDP Configuration	Enabling LLDP	Required
	Setting LLDP Operating Mode	Optional
	Setting the LLDP Re-Initialization Delay	Optional
	Enabling LLDP Polling	Optional
	Configuring the TLVs to Be Advertised	Optional

Task		Remarks
	Configuring the Management Address	Optional
	Setting Other LLDP Parameters	Optional
	Setting an Encapsulation Format for LLDPDUs	Optional
Configuring CDP Compatibility		Optional
Configuring LLDP Trapping		Optional

Performing Basic LLDP Configuration

Enabling LLDP

To make LLDP take effect on certain ports, you need to enable LLDP both globally and on these ports.

Follow these steps to enable LLDP:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable LLDP globally	lldp enable	Required By default, LLDP is disabled globally.
Enter Ethernet interface view	interface <i>interface-type interface-number</i>	Required
Enable LLDP	lldp enable	Optional By default, LLDP is enabled on a port.

Setting LLDP Operating Mode

LLDP can operate in one of the following modes.

- TxRx mode. A port in this mode sends and receives LLDP frames.
- Tx mode. A port in this mode only sends LLDP frames.
- Rx mode. A port in this mode only receives LLDP frames.
- Disable mode. A port in this mode does not send or receive LLDP frames.

Follow these steps to set LLDP operating mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet interface view	interface <i>interface-type interface-number</i>	Required
Set the LLDP operating mode	lldp admin-status { disable rx tx txrx }	Optional TxRx by default.

Setting the LLDP Re-Initialization Delay

When LLDP operating mode changes on a port, the port initializes the protocol state machines after a certain delay. By adjusting the LLDP re-initialization delay, you can avoid frequent initializations caused by frequent LLDP operating mode changes on a port.

Follow these steps to set the LLDP re-initialization delay for ports:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the LLDP re-initialization delay	lldp timer reinit-delay <i>delay</i>	Optional 2 seconds by default

Enabling LLDP Polling

With LLDP polling enabled, a device checks for local configuration changes periodically. Upon detecting a configuration change, the device sends LLDP frames to inform the neighboring devices of the change.

Follow these steps to enable LLDP polling:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet interface view	interface <i>interface-type</i> <i>interface-number</i>	Required
Enable LLDP polling and set the polling interval	lldp check-change-interval <i>interval</i>	Required Disabled by default

Configuring the TLVs to Be Advertised

Follow these steps to configure the LLDPDU TLVs to be advertised out the specified port or ports:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet interface view	interface <i>interface-type</i> <i>interface-number</i>	Required
Configure the TLVs to be advertised	lldp tlv-enable { basic-tlv { all port-description system-capability system-description system-name } dot1-tlv { all port-vlan-id protocol-vlan-id [<i>vlan-id</i>] vlan-name [<i>vlan-id</i>] } dot3-tlv { all link-aggregation mac-physic max-frame-size power } med-tlv { all capability inventory location-id { civic-address <i>device-type</i> <i>country-code</i> { <i>ca-type</i> <i>ca-value</i> }&<1–10> elin-address <i>tel-number</i> } network-policy power-over-ethernet } }	Optional By default, all types of LLDP TLVs except location identification TLV are advertisable.

Configuring the Management Address

The management address of a device is used by the network management system to identify and manage the device for topology maintenance and network management. The management address is encapsulated in the management address TLV. LLDP encodes management addresses in numeric format in management address TLVs.

Make sure that a neighbor also encodes its management address in numeric format to guarantee normal communication with the neighbor.

Follow these steps to configure a management address to be advertised on a port:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet interface view	interface <i>interface-type</i> <i>interface-number</i>	Required
Enable LLDP to advertise management address TLVs and configure the advertised management IP address	lldp management-address-tlv [<i>ip-address</i>]	Optional By default, the management address is sent through LLDPDUs, and the management address is the main IP address of the lowest-ID VLAN carried on the interface. If the VLAN is not assigned a main IP address, 127.0.0.1 is used.

Setting Other LLDP Parameters

The TTL TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device.

You can configure the TTL of locally sent LLDP frames to determine how long information about the local device can be saved on a neighbor device by setting the TTL multiplier. The TTL is expressed as follows:

$$\text{TTL} = \text{Min} (65535, (\text{TTL multiplier} \times \text{LLDPDU transmit interval}))$$

As the expression shows, the TTL can be up to 65535 seconds. TTLs greater than it will be rounded down to 65535 seconds.

Follow these steps to change the TTL multiplier:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Set the TTL multiplier	lldp hold-multiplier <i>value</i>	Optional 4 by default.
Set the LLDPDU transmit interval	lldp timer tx-interval <i>interval</i>	Optional 30 seconds by default
Set LLDPDU transmit delay	lldp timer tx-delay <i>delay</i>	Optional 2 seconds by default

To do...	Use the command...	Remarks
Set the number of LLDP frames sent each time fast LLDPDU transmission is triggered.	lldp fast-count <i>count</i>	Optional 3 by default



Note

Both the LLDPDU transmit interval and delay must be less than the TTL to ensure that the LLDP neighbors can receive LLDP frames to update information about the device you are configuring before it is aged out.

Setting an Encapsulation Format for LLDPDUs

LLDPDUs can be encapsulated in Ethernet II or SNAP frames.

- With Ethernet II encapsulation configured, an LLDP port sends LLDPDUs in Ethernet II frames and processes an incoming LLDP frame only when it is Ethernet II encapsulated.
- With SNAP encapsulation configured, an LLDP port sends LLDPDUs in SNAP frames and processes an incoming LLDP frame only when it is SNAP encapsulated.

By default, LLDPDUs are encapsulated in Ethernet II frames. If the neighbor devices encapsulate LLDPDUs in SNAP frames, configure the encapsulation format for LLDPDUs as SNAP to guarantee normal communication with the neighbors.

Follow these steps to set the encapsulation format for LLDPDUs to SNAP:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet interface view	interface <i>interface-type</i> <i>interface-number</i>	Required
Set the encapsulation format for LLDPDUs to SNAP	lldp encapsulation snap	Required Ethernet II encapsulation format applies by default. To restore the default, use the undo lldp encapsulation command.



Note

LLDP-CDP (CDP is short for the Cisco Discovery Protocol) packets use only SNAP encapsulation.

Configuring CDP Compatibility



Note

On a S3600 series switch, only one voice VLAN exists at any given point in time. For detailed information about voice VLAN, refer to *Voice VLAN Operation* in this manual.

You need to enable CDP compatibility for your device to work with Cisco IP phones.

As your LLDP-enabled device cannot recognize CDP packets, it does not respond to the requests of Cisco IP phones for the voice VLAN ID configured on the device. This can cause a requesting Cisco IP phone to send voice traffic without any tag to your device, disabling your device from differentiating voice traffic from other types of traffic.

With CDP compatibility enabled, the device can use LLDP to receive and recognize CDP packets from Cisco IP phones and respond with CDP packets carrying the voice VLAN ID of the device for the IP phones to configure the voice VLAN automatically. In this way, voice traffic is confined in the configured voice VLAN and is thus differentiated from other types of traffic.

Configuration Prerequisites

Before configuring CDP compatibility, make sure that:

- LLDP is enabled globally.
- LLDP is enabled on the port connected to an IP phone and is configured to operate in TxRx mode on the port.

Configuring CDP Compatibility

CDP-compatible LLDP operates in one of the follows two modes:

- TxRx, where CDP packets can be transmitted and received.
- Disable, where CDP packets can neither be transmitted nor be received.

To make CDP-compatible LLDP take effect on certain ports, first enable CDP-compatible LLDP globally and configure CDP-compatible LLDP to operate in TxRx mode.

Follow these steps to enable LLDP to be compatible with CDP:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enable CDP compatibility globally	lldp compliance cdp	Required Disabled by default.
Enter Ethernet interface view	interface <i>interface-type</i> <i>interface-number</i>	Required
Configure CDP-compatible LLDP to operate in TxRx mode	lldp compliance admin-status cdp txrx	Required By default, CDP-compatible LLDP operates in disable mode.



Caution

As the maximum TTL allowed by CDP is 255 seconds, ensure that the product of the TTL multiplier and the LLDPDU transmit interval is less than 255 seconds for CDP-compatible LLDP to work properly with Cisco IP phones. You can use related commands to configure the TTL multiplier and the LLDPDU transmit interval. For details, see [Setting Other LLDP Parameters](#).

Configuring LLDP Trapping

LLDP trapping is used to notify the network management system (NMS) of events such as new neighboring devices detected and link malfunctions.

To prevent excessive LLDP traps from being sent when topology is unstable, you can set a minimum trap sending interval for LLDP.

Follow these steps to configure LLDP trapping:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter Ethernet interface view	interface <i>interface-type</i> <i>interface-number</i>	Required
Enable LLDP trap sending	lldp notification remote-change enable	Required Disabled by default
Quit to system view	quit	—
Set the interval to send LLDP traps	lldp timer notification-interval <i>interval</i>	Optional 5 seconds by default

Displaying and Maintaining LLDP

To do...	Use the command...	Remarks
Display the global LLDP information or the information contained in the LLDP TLVs to be sent through a port	display lldp local-information [global interface <i>interface-type</i> <i>interface-number</i>]	Available in any view
Display the information contained in the LLDP TLVs sent from neighboring devices	display lldp neighbor-information [interface <i>interface-type</i> <i>interface-number</i>] [brief]	Available in any view
Display LLDP statistics	display lldp statistics [global interface <i>interface-type</i> <i>interface-number</i>]	Available in any view
Display LLDP status of a port	display lldp status [interface <i>interface-type</i> <i>interface-number</i>]	Available in any view
Display types of advertisable optional LLDP TLVs	display lldp tlv-config [interface <i>interface-type</i> <i>interface-number</i>]	Available in any view

LLDP Configuration Examples

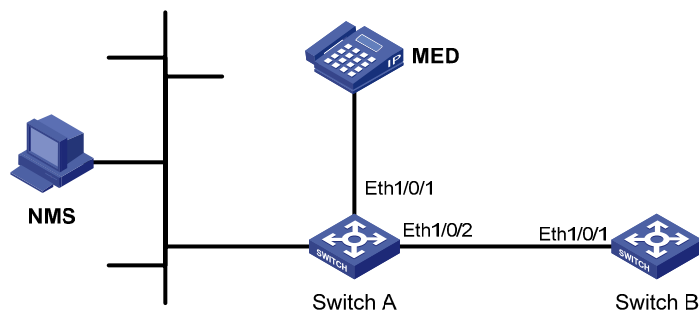
Basic LLDP Configuration Example

Network requirements

As shown in [Figure 1-4](#), the NMS and Switch A are located in the same Ethernet. An MED device and Switch B are connected to Ethernet 1/0/1 and Ethernet 1/0/2 of Switch A.

Enable LLDP on the ports of Switch A and Switch B to monitor the link between Switch A and Switch B and the link between Switch A and the MED device on the NMS.

Figure 1-4 Network diagram for basic LLDP configuration



Configuration procedure

1) Configure Switch A.

Enable LLDP globally.

```
<SwitchA> system-view
```

```
[SwitchA] lldp enable
```

Enable LLDP on Ethernet 1/0/1 and Ethernet 1/0/2 (you can skip this step because LLDP is enabled on ports by default), and set the LLDP operating mode to Rx.

```
[SwitchA] interface ethernet 1/0/1
```

```
[SwitchA-Ethernet1/0/1] lldp enable
```

```
[SwitchA-Ethernet1/0/1] lldp admin-status rx
```

```
[SwitchA-Ethernet1/0/1] quit
```

```
[SwitchA] interface ethernet 1/0/2
```

```
[SwitchA-Ethernet1/0/2] lldp enable
```

```
[SwitchA-Ethernet1/0/2] lldp admin-status rx
```

```
[SwitchA-Ethernet1/0/2] quit
```

2) Configure Switch B.

Enable LLDP globally.

```
<SwitchB> system-view
```

```
[SwitchB] lldp enable
```

Enable LLDP on Ethernet1/0/1 (you can skip this step because LLDP is enabled on ports by default), and set the LLDP operating mode to Tx.

```
[SwitchB] interface ethernet 1/0/1
```

```
[SwitchB-Ethernet1/0/1] lldp enable
```

```
[SwitchB-Ethernet1/0/1] lldp admin-status tx
```

```
[SwitchB-Ethernet1/0/1] quit
```

3) Verify the configuration.

Display the global LLDP status and port LLDP status on Switch A.

```
[SwitchA] display lldp status
```

```
Global status of LLDP : Enable
```

```
The current number of LLDP neighbors : 2
```

```
The current number of CDP neighbors : 0
```

```
LLDP neighbor information last changed time: 0 days,0 hours,4 minutes,40 seconds
```

```
Transmit interval      : 30s
```

```
Hold multiplier        : 4
```

```
Reinit delay          : 2s
```

```
Transmit delay         : 2s
```

```
Trap interval         : 5s
```

```
Fast start times       : 3
```

```
Port 1 [Ethernet1/0/1]:
```

```
Port status of LLDP      : Enable
```

```
Admin status             : Rx_Only
```

```
Trap flag                : No
```

```
Roll time                : 0s
```

```
Number of neighbors      : 1
```

```
Number of MED neighbors  : 1
```

```
Number of CDP neighbors  : 0
```

```
Number of sent optional TLV : 0
```

```
Number of received unknown TLV : 0
```

```
Port 2 [Ethernet1/0/2]:
```

```
Port status of LLDP      : Enable
```

```
Admin status             : Rx_Only
```

```
Trap flag                : No
```

```
Roll time                : 0s
```

```
Number of neighbors      : 1
```

```
Number of MED neighbors  : 0
```

```
Number of CDP neighbors  : 0
```

```
Number of sent optional TLV : 0
```

```
Number of received unknown TLV : 3
```

As the sample output shows, Ethernet 1/0/1 of Switch A connects a MED device, and Ethernet 1/0/2 of Switch A connects a non-MED device. Both ports operate in Rx mode, that is, they only receive LLDP frames.

Tear down the link between Switch A and Switch B and then display the global LLDP status and port LLDP status on Switch A.

```
[SwitchA] display lldp status
```

```
Global status of LLDP : Enable
```

```
The current number of LLDP neighbors : 1
```

```
The current number of CDP neighbors : 0
LLDP neighbor information last changed time: 0 days,0 hours,5 minutes,20 seconds
Transmit interval          : 30s
Hold multiplier             : 4
Reinit delay               : 2s
Transmit delay             : 2s
Trap interval              : 5s
Fast start times           : 3
```

Port 1 [Ethernet1/0/1]:

```
Port status of LLDP      : Enable
Admin status             : Rx_Only
Trap flag                : No
Roll time                : 0s
```

```
Number of neighbors      : 1
Number of MED neighbors   : 1
Number of CDP neighbors   : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 5
```

Port 2 [Ethernet1/0/2]:

```
Port status of LLDP      : Enable
Admin status             : Rx_Only
Trap flag                : No
Roll time                : 0s
```

```
Number of neighbors      : 0
Number of MED neighbors   : 0
Number of CDP neighbors   : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 0
```

As shown in the sample output, Ethernet 1/0/2 of Switch A does not connect any neighboring devices.

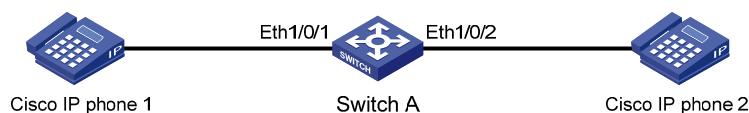
CDP-Compatible LLDP Configuration Example

Network requirements

As shown in [Figure 1-5](#):

- Ethernet 1/0/1 and Ethernet 1/0/2 of Switch A are each connected to a Cisco IP phone.
- Configure voice VLAN 2 on Switch A. Enable CDP compatibility of LLDP on Switch A to allow the Cisco IP phones to automatically configure the voice VLAN, thus confining their voice traffic within the voice VLAN to be isolated from other types of traffic.

Figure 1-5 Network diagram for CDP-compatible LLDP configuration



Configuration procedure

1) Configure a voice VLAN on Switch A

Create VLAN 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] quit
```

Set the link type of Ethernet 1/0/1 and Ethernet 1/0/2 to trunk and enable voice VLAN on them.

```
[SwitchA] interface ethernet 1/0/1
[SwitchA-Ethernet1/0/1] port link-type trunk
[SwitchA-Ethernet1/0/1] voice vlan 2 enable
[SwitchA-Ethernet1/0/1] quit
[SwitchA] interface ethernet 1/0/2
[SwitchA-Ethernet1/0/2] port link-type trunk
[SwitchA-Ethernet1/0/2] voice vlan 2 enable
[SwitchA-Ethernet1/0/2] quit
```

2) Configure CDP-compatible LLDP on Switch A.

Enable LLDP globally and enable LLDP to be compatible with CDP globally.

```
[SwitchA] lldp enable
[SwitchA] lldp compliance cdp
```

Enable LLDP (you can skip this step because LLDP is enabled on ports by default), configure LLDP to operate in TxRx mode, and configure CDP-compatible LLDP to operate in TxRx mode on Ethernet 1/0/1 and Ethernet 1/0/2.

```
[SwitchA] interface ethernet 1/0/1
[SwitchA-Ethernet1/0/1] lldp enable
[SwitchA-Ethernet1/0/1] lldp admin-status txrx
[SwitchA-Ethernet1/0/1] lldp compliance admin-status cdp txrx
[SwitchA-Ethernet1/0/1] quit
[SwitchA] interface ethernet 1/0/2
[SwitchA-Ethernet1/0/2] lldp enable
[SwitchA-Ethernet1/0/2] lldp admin-status txrx
[SwitchA-Ethernet1/0/2] lldp compliance admin-status cdp txrx
[SwitchA-Ethernet1/0/2] quit
```

3) Verify the configuration

Display the neighbor information on Switch A.

```
[SwitchA] display lldp neighbor-information
CDP neighbor-information of port 1[Ethernet1/0/1]:
  CDP neighbor index : 1
  Chassis ID         : SEP00141CBCDBFE
  Port ID            : Port 1
  Software version    : P0030301MFG2
  Platform           : Cisco IP Phone 7960
  Duplex              : Full
```

CDP neighbor-information of port 2[Ethernet1/0/2]:

CDP neighbor index : 2
Chassis ID : SEP00141CBCDBFF
Port ID : Port 1
Software version : P0030301MFG2
Platform : Cisco IP Phone 7960
Duplex : Full

As the sample output shows, Switch A has discovered the IP phones connected to Ethernet 1/0/1 and Ethernet 1/0/2, and has obtained their LLDP device information.

Table of Contents

1 PKI Configuration	1-1
Introduction to PKI	1-1
PKI Overview	1-1
PKI Terms	1-1
Architecture of PKI	1-2
Applications of PKI	1-3
Operation of PKI	1-3
PKI Configuration Task List	1-4
Configuring an Entity DN	1-4
Configuring a PKI Domain	1-6
Submitting a PKI Certificate Request	1-7
Submitting a Certificate Request in Auto Mode	1-7
Submitting a Certificate Request in Manual Mode	1-8
Retrieving a Certificate Manually	1-9
Configuring PKI Certificate Verification	1-10
Destroying a Local RSA Key Pair	1-11
Deleting a Certificate	1-11
Configuring an Access Control Policy	1-12
Displaying and Maintaining PKI	1-12
PKI Configuration Examples	1-13
Requesting a Certificate from a CA Running RSA Keon	1-13
Requesting a Certificate from a CA Running Windows 2003 Server	1-16
Troubleshooting PKI	1-19
Failed to Retrieve a CA Certificate	1-19
Failed to Request a Local Certificate	1-20
Failed to Retrieve CRLs	1-20

1 PKI Configuration

When configuring PKI, go to these sections for information you are interested in:

- [Introduction to PKI](#)
- [PKI Configuration Task List](#)
- [Displaying and Maintaining PKI](#)
- [PKI Configuration Examples](#)
- [Troubleshooting PKI](#)

Introduction to PKI

This section covers these topics:

- [PKI Overview](#)
- [PKI Terms](#)
- [Architecture of PKI](#)
- [Applications of PKI](#)
- [Operation of PKI](#)

PKI Overview

The Public Key Infrastructure (PKI) is a general security infrastructure for providing information security through public key technologies.

PKI, also called asymmetric key infrastructure, uses a key pair to encrypt and decrypt the data. The key pair consists of a private key and a public key. The private key must be kept secret while the public key needs to be distributed. Data encrypted by one of the two keys can only be decrypted by the other.

A key problem of PKI is how to manage the public keys. Currently, PKI employs the digital certificate mechanism to solve this problem. The digital certificate mechanism binds public keys to their owners, helping distribute public keys in large networks securely.

With digital certificates, the PKI system provides network communication and e-commerce with security services such as user authentication, data non-repudiation, data confidentiality, and data integrity.

Currently, PKI system provides Secure Sockets Layer (SSL)..

PKI Terms

Digital certificate

A digital certificate is a file signed by a certificate authority (CA) for an entity. It includes mainly the identity information of the entity, the public key of the entity, the name and signature of the CA, and the validity period of the certificate, where the signature of the CA ensures the validity and authority of the certificate. A digital certificate must comply with the international standard of ITU-T X.509. Currently, the most common standard is X.509 v3.

This manual involves two types of certificates: local certificate and CA certificate. A local certificate is a digital certificate signed by a CA for an entity, while a CA certificate is the certificate of a CA. If multiple

CAs are trusted by different users in a PKI system, the CAs will form a CA tree with the root CA at the top level. The root CA has a CA certificate signed by itself while each lower level CA has a CA certificate signed by the CA at the next higher level.

CRL

An existing certificate may need to be revoked when, for example, the user name changes, the private key leaks, or the user stops the business. Revoking a certificate is to remove the binding of the public key with the user identity information. In PKI, the revocation is made through certificate revocation lists (CRLs). Whenever a certificate is revoked, the CA publishes one or more CRLs to show all certificates that have been revoked. The CRLs contain the serial numbers of all revoked certificates and provide an effective way for checking the validity of certificates.

A CA may publish multiple CRLs when the number of revoked certificates is so large that publishing them in a single CRL may degrade network performance, and it uses CRL distribution points to indicate the URLs of these CRLs.

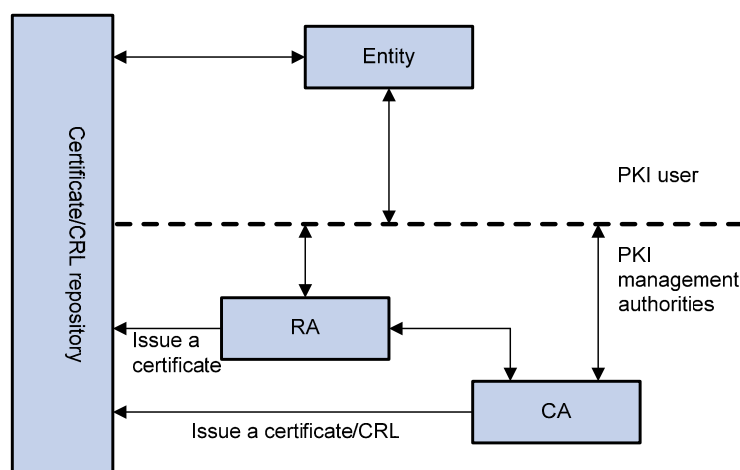
CA policy

A CA policy is a set of criteria that a CA follows in processing certificate requests, issuing and revoking certificates, and publishing CRLs. Usually, a CA advertises its policy in the form of certification practice statement (CPS). A CA policy can be acquired through out-of-band means such as phone, disk, and e-mail. As different CAs may use different methods to check the binding of a public key with an entity, make sure that you understand the CA policy before selecting a trusted CA for certificate request.

Architecture of PKI

A PKI system consists of entities, a CA, a registration authority (RA) and a PKI repository, as shown in [Figure 1-1](#).

Figure 1-1 PKI architecture



Entity

An entity is an end user of PKI products or services, such as a person, an organization, a device like a switch, or a process running on a computer.

CA

A CA is a trusted authority responsible for issuing and managing digital certificates. A CA issues certificates, specifies the validity periods of certificates, and revokes certificates as needed by publishing CRLs.

RA

A registration authority (RA) is an extended part of a CA or an independent authority. An RA can implement functions including identity authentication, CRL management, key pair generation and key pair backup. The PKI standard recommends that an independent RA be used for registration management to achieve higher security of application systems.

PKI repository

A PKI repository can be a Lightweight Directory Access Protocol (LDAP) server or a common database. It stores and manages information like certificate requests, certificates, keys, CRLs and logs while providing a simple query function.

LDAP is a protocol for accessing and managing PKI information. An LDAP server stores user information and digital certificates from the RA server and provides directory navigation service. From an LDAP server, an entity can retrieve local and CA certificates of its own as well as certificates of other entities.

Applications of PKI

The PKI technology can satisfy the security requirements of online transactions. As an infrastructure, PKI has a wide range of applications. Here are some application examples.

VPN

A virtual private network (VPN) is a private data communication network built on the public communication infrastructure. A VPN can leverage network layer security protocols (for instance, IPSec) in conjunction with PKI-based encryption and digital signature technologies for confidentiality.

Secure E-mail

E-mails require confidentiality, integrity, authentication, and non-repudiation. PKI can address these needs. The secure E-mail protocol that is currently developing rapidly is Secure/Multipurpose Internet Mail Extensions (S/MIME), which is based on PKI and allows for transfer of encrypted mails with signature.

Web security

For Web security, two peers can establish an SSL connection first for transparent and secure communications at the application layer. With PKI, SSL enables encrypted communications between a browser and a server. Both the communication parties can verify the identity of each other through digital certificates.

Operation of PKI

In a PKI-enabled network, an entity can request a local certificate from the CA and the device can check the validity of certificates. Here is how it works:

- 1) An entity submits a certificate request to the RA.

- 2) The RA reviews the identity of the entity and then sends the identity information and the public key with a digital signature to the CA.
- 3) The CA verifies the digital signature, approves the application, and issues a certificate.
- 4) The RA receives the certificate from the CA, sends it to the LDAP server to provide directory navigation service, and notifies the entity that the certificate is successfully issued.
- 5) The entity retrieves the certificate. With the certificate, the entity can communicate with other entities safely through encryption and digital signature.
- 6) The entity makes a request to the CA when it needs to revoke its certificate, while the CA approves the request, updates the CRLs and publishes the CRLs on the LDAP server.

PKI Configuration Task List

Complete the following tasks to configure PKI:

Task		Remarks
Configuring an Entity DN		Required
Configuring a PKI Domain		Required
Submitting a PKI Certificate Request	Submitting a Certificate Request in Auto Mode	Required
	Submitting a Certificate Request in Manual Mode	Use either approach
Retrieving a Certificate Manually		Optional
Configuring PKI Certificate		Optional
Destroying a Local RSA Key Pair		Optional
Deleting a Certificate		Optional
Configuring an Access Control Policy		Optional

Configuring an Entity DN

A certificate is the binding of a public key and the identity information of an entity, where the identity information is identified by an entity distinguished name (DN). A CA identifies a certificate applicant uniquely by entity DN.

An entity DN is defined by these parameters:

- Common name of the entity.
- Country code of the entity, a standard 2-character code. For example, CN represents China and US represents the United States of America.
- Fully qualified domain name (FQDN) of the entity, a unique identifier of an entity on the network. It consists of a host name and a domain name and can be resolved to an IP address. For example, **www.whatever.com** is an FQDN, where www is a host name and whatever.com a domain name.
- IP address of the entity.
- Locality where the entity resides.
- Organization to which the entity belongs.
- Unit of the entity in the organization.
- State where the entity resides.



Note

The configuration of an entity DN must comply with the CA certificate issue policy. You need to determine, for example, which entity DN parameters are mandatory and which are optional. Otherwise, certificate request may be rejected.

Follow these steps to configure an entity DN:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create an entity and enter its view	pki entity <i>entity-name</i>	Required No entity exists by default.
Configure the common name for the entity	common-name <i>name</i>	Optional No common name is specified by default.
Configure the country code for the entity	country <i>country-code-str</i>	Optional No country code is specified by default.
Configure the FQDN for the entity	fqdn <i>name-str</i>	Optional No FQDN is specified by default.
Configure the IP address for the entity	ip <i>ip-address</i>	Optional No IP address is specified by default.
Configure the locality of the entity	locality <i>locality-name</i>	Optional No locality is specified by default.
Configure the organization name for the entity	organization <i>org-name</i>	Optional No organization is specified by default.
Configure the unit name for the entity	organization-unit <i>org-unit-name</i>	Optional No unit is specified by default.
Configure the state or province for the entity	state <i>state-name</i>	Optional No state or province is specified by default.



Note

- Currently, up to two entities can be created on a device.
- The Windows 2000 CA server has some restrictions on the data length of a certificate request. If the entity DN in a certificate request goes beyond a certain limit, the server will not respond to the certificate request.

Configuring a PKI Domain

Before requesting a PKI certificate, an entity needs to be configured with some enrollment information, which is referred to as a PKI domain. A PKI domain is intended only for convenience of reference by other applications like SSL, and has only local significance.

A PKI domain is defined by these parameters:

- Trusted CA

An entity requests a certificate from a trusted CA.

- Entity

A certificate applicant uses an entity to provide its identity information to a CA.

- RA

Generally, an independent RA is in charge of certificate request management. It receives the registration request from an entity, checks its qualification, and determines whether to ask the CA to sign a digital certificate. The RA only checks the application qualification of an entity; it does not issue any certificate. Sometimes, the registration management function is provided by the CA, in which case no independent RA is required. You are recommended to deploy an independent RA.

- URL of the registration server

An entity sends a certificate request to the registration server through Simple Certification Enrollment Protocol (SCEP), a dedicated protocol for an entity to communicate with a CA.

- Polling interval and count

After an applicant makes a certificate request, the CA may need a long period of time if it verifies the certificate request manually. During this period, the applicant needs to query the status of the request periodically to get the certificate as soon as possible after the certificate is signed. You can configure the polling interval and count to query the request status.

- IP address of the LDAP server

An LDAP server is usually deployed to store certificates and CRLs. If this is the case, you need to configure the IP address of the LDAP server.

- Fingerprint for root certificate verification

Upon receiving the root certificate of the CA, an entity needs to verify the fingerprint of the root certificate, namely, the hash value of the root certificate content. This hash value is unique to every certificate. If the fingerprint of the root certificate does not match the one configured for the PKI domain, the entity will reject the root certificate.

Follow these steps to configure a PKI domain:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a PKI domain and enter its view	pki domain <i>domain-name</i>	Required No PKI domain exists by default.
Specify the trusted CA	ca identifier <i>name</i>	Required No trusted CA is specified by default.

To do...	Use the command...	Remarks
Specify the entity for certificate request	certificate request entity <i>entity-name</i>	Required No entity is specified by default. The specified entity must exist.
Specify the authority for certificate request	certificate request from { ca ra }	Required No authority is specified by default.
Configure the URL of the server for certificate request	certificate request url <i>url-string</i>	Required No URL is configured by default.
Configure the polling interval and attempt limit for querying the certificate request status	certificate request polling { count <i>count</i> interval <i>minutes</i> }	Optional The polling is executed for up to 5 times at the interval of 20 minutes by default.
Specify the LDAP server	ldap-server ip <i>ip-address</i> [port <i>port-number</i>] [version <i>version-number</i>]	Optional No LDP server is specified by default.
Configure the fingerprint for root certificate verification	root-certificate fingerprint { md5 sha1 } <i>string</i>	Required when the certificate request mode is auto and optional when the certificate request mode is manual. In the latter case, if you do not configure this command, the fingerprint of the root certificate must be verified manually. No fingerprint is configured by default.



Note

- Currently, up to two PKI domains can be created on a device.
- The CA name is required only when you retrieve a CA certificate. It is not used when in local certificate request.
- Currently, the URL of the server for certificate request does not support domain name resolving.

Submitting a PKI Certificate Request

When requesting a certificate, an entity introduces itself to the CA by providing its identity information and public key, which will be the major components of the certificate. A certificate request can be submitted to a CA in two ways: online and offline. In offline mode, a certificate request is submitted to a CA by an “out-of-band” means such as phone, disk, or e-mail.

Online certificate request falls into two categories: manual mode and auto mode.

Submitting a Certificate Request in Auto Mode

In auto mode, an entity automatically requests a certificate through the SCEP protocol when it has no local certificate or the present certificate is about to expire.

Follow these steps to configure an entity to submit a certificate request in auto mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter PKI domain view	pki domain <i>domain-name</i>	—
Set the certificate request mode to auto	certificate request mode auto [key-length <i>key-length</i> password { cipher simple } <i>password</i>] *	Required Manual by default

Submitting a Certificate Request in Manual Mode

In manual mode, you need to retrieve a CA certificate, generate a local RSA key pair, and submit a local certificate request for an entity.

The goal of retrieving a CA certificate is to verify the authenticity and validity of a local certificate.

Generating an RSA key pair is an important step in certificate request. The key pair includes a public key and a private key. The private key is kept by the user, while the public key is transferred to the CA along with some other information.

Follow these steps to submit a certificate request in manual mode:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter PKI domain view	pki domain <i>domain-name</i>	—
Set the certificate request mode to manual	certificate request mode manual	Optional Manual by default
Return to system view	quit	—
Retrieve a CA certificate manually	Refer to Retrieving a Certificate Manually	Required
Generate a local RSA key pair	public-key local create rsa	Required No local RSA key pair exists by default.
Submit a local certificate request manually	pki request-certificate domain <i>domain-name</i> [<i>password</i>] [pkcs10 [<i>filename filename</i>]]	Required



Note

- If a PKI domain already has a local certificate, creating an RSA key pair will result in inconsistency between the key pair and the certificate. To generate a new RSA key pair, delete the local certificate and then issue the **public-key local create** command.
- A newly created key pair will overwrite the existing one. If you perform the **public-key local create** command in the presence of a local RSA key pair, the system will ask you whether you want to overwrite the existing one.
- If a PKI domain has already a local certificate, you cannot request another certificate for it. This is to avoid inconsistency between the certificate and the registration information resulting from configuration changes. To request a new certificate, use the **pki delete-certificate** command to delete the existing local certificate and the CA certificate stored locally.
- When it is impossible to request a certificate from the CA through SCEP, you can save the request information by using the **pki request-certificate domain** command with the **pkcs10** and **filename** keywords, and then send the file to the CA by an out-of-band means.
- Make sure the clocks of the entity and the CA are synchronous. Otherwise, the validity period of the certificate will be abnormal.
- The **pki request-certificate domain** configuration will not be saved in the configuration file.

Retrieving a Certificate Manually

You can download an existing CA certificate, local certificate, or peer entity certificate from the CA server and save it locally. To do so, you can use two ways: online and offline. In offline mode, you need to retrieve a certificate by an out-of-band means like FTP, disk, e-mail and then import it into the local PKI system.

Certificate retrieval serves two purposes:

- Locally store the certificates associated with the local security domain for improved query efficiency and reduced query count,
- Prepare for certificate verification.

Before retrieving a local certificate in online mode, be sure to complete LDAP server configuration.

Follow these steps to retrieve a certificate manually:

To do...		Use the command...	Remarks
Enter system view		system-view	—
Retrieve a certificate manually	Online	pki retrieval-certificate { ca local } domain domain-name	Required Use either command.
	Offline	pki import-certificate { ca local } domain domain-name { der p12 pem } [filename filename]	



Caution

- If a PKI domain already has a CA certificate, you cannot retrieve another CA certificate for it. This is in order to avoid inconsistency between the certificate and registration information due to related configuration changes. To retrieve a new CA certificate, use the **pki delete-certificate** command to delete the existing CA certificate and local certificate first.
- The **pki retrieval-certificate** configuration will not be saved in the configuration file.

Configuring PKI Certificate Verification

A certificate needs to be verified before being used. Verifying a certificate is to check that the certificate is signed by the CA and that the certificate has neither expired nor been revoked.

Before verifying a certificate, you need to retrieve the CA certificate.

You can specify whether CRL checking is required in certificate verification. If you enable CRL checking, CRLs will be used in verification of a certificate.

Configuring CRL-checking-enabled PKI certificate verification

Follow these steps to configure CRL-checking-enabled PKI certificate verification:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Enter PKI domain view	pki domain <i>domain-name</i>	—
Specify the URL of the CRL distribution point	crl url <i>url-string</i>	Optional No CRL distribution point URL is specified by default.
Set the CRL update period	crl update-period <i>hours</i>	Optional 0 by default
Enable CRL checking	undo crl check disable	Optional Enabled by default
Return to system view	quit	—
Retrieve the CA certificate	Refer to Retrieving a Certificate Manually	Required
Retrieve CRLs	pki retrieval-crl domain <i>domain-name</i>	Required
Verify the validity of a certificate	pki validate-certificate { ca local } domain <i>domain-name</i>	Required

Configuring CRL-checking-disabled PKI certificate verification

Follow these steps to configure CRL-checking-disabled PKI certificate verification:

To do...	Use the command...	Remarks
Enter system view	system-view	—

To do...	Use the command...	Remarks
Enter PKI domain view	pki domain <i>domain-name</i>	—
Disable CRL checking	crl check disable	Required Enabled by default
Return to system view	quit	—
Retrieve the CA certificate	Refer to Retrieving a Certificate Manually	Required
Verify the validity of the certificate	pki validate-certificate { ca local } domain <i>domain-name</i>	Required



Note

- The CRL update period refers to the interval at which the entity downloads CRLs from the CRL server. The CRL update period configured manually is prior to that specified in the CRLs.
- The **pki retrieval-crl domain** configuration will not be saved in the configuration file.
- Currently, the URL of the CRL distribution point does not support domain name resolving.

Destroying a Local RSA Key Pair

A certificate has a lifetime, which is determined by the CA. When the private key leaks or the certificate is about to expire, you can destroy the old RSA key pair and then create a pair to request a new certificate.

Follow these steps to destroy a local RSA key pair:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Destroy a local RSA key pair	public-key local destroy rsa	Required

Deleting a Certificate

When a certificate requested manually is about to expire or you want to request a new certificate, you can delete the current local certificate or CA certificate.

Follow these steps to delete a certificate:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Delete certificates	pki delete-certificate { ca local } domain <i>domain-name</i>	Required

Configuring an Access Control Policy

By configuring a certificate attribute-based access control policy, you can further control access to the server, providing additional security for the server.

Follow these steps to configure a certificate attribute-based access control policy:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create a certificate attribute group and enter its view	pki certificate attribute-group <i>group-name</i>	Required No certificate attribute group exists by default.
Configure an attribute rule for the certificate issuer name, certificate subject name, or alternative subject name	attribute <i>id</i> { alt-subject-name { fqdn ip } { issuer-name subject-name } { dn fqdn ip } } { ctn equ nctn nequ } <i>attribute-value</i>	Optional There is no restriction on the issuer name, certificate subject name and alternative subject name by default.
Return to system view	quit	—
Create a certificate attribute-based access control policy and enter its view	pki certificate access-control-policy <i>policy-name</i>	Required No access control policy exists by default.
Configure a certificate attribute-based access control rule	rule [<i>id</i>] { deny permit } <i>group-name</i>	Required No access control rule exists by default.



Caution

A certificate attribute group must exist to be associated with a rule.

Displaying and Maintaining PKI

To do...	Use the command...	Remarks
Display the contents or request status of a certificate	display pki certificate { { ca local } domain <i>domain-name</i> request-status }	Available in any view
Display CRLs	display pki crl domain <i>domain-name</i>	Available in any view
Display information about one or all certificate attribute groups	display pki certificate attribute-group { <i>group-name</i> all }	Available in any view
Display information about one or all certificate attribute-based access control policies	display pki certificate access-control-policy { <i>policy-name</i> all }	Available in any view

PKI Configuration Examples



Caution

- The SCEP plug-in is required when you use the Windows Server as the CA. In this case, when configuring the PKI domain, you need to use the **certificate request from ra** command to specify that the entity requests a certificate from an RA.
 - The SCEP plug-in is not required when RSA Keon is used. In this case, when configuring a PKI domain, you need to use the **certificate request from ca** command to specify that the entity requests a certificate from a CA.
-

Requesting a Certificate from a CA Running RSA Keon



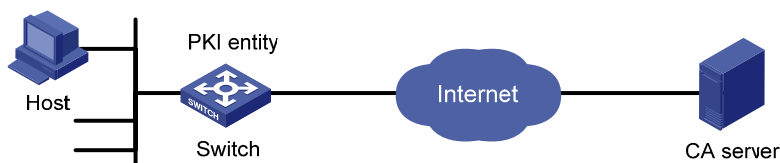
Note

The CA server runs RSA Keon in this configuration example.

Network requirements

- The device submits a local certificate request to the CA server.
- The device acquires the CRLs for certificate verification.

Figure 1-2 Request a certificate from a CA running RSA Keon



Configuration procedure

1) Configure the CA server

Create a CA server named **myca**.

In this example, you need to configure these basic attributes on the CA server at first:

- Nickname: Name of the trusted CA.
- Subject DN: DN information of the CA, including the Common Name (CN), Organization Unit (OU), Organization (O), and Country (C).

The other attributes may be left using the default values.

Configure extended attributes.

After configuring the basic attributes, you need to perform configuration on the jurisdiction configuration page of the CA server. This includes selecting the proper extension profiles, enabling the SCEP autovetting function, and adding the IP address list for SCEP autovetting.

Configure the CRL distribution behavior.

After completing the above configuration, you need to perform CRL related configurations. In this example, select the local CRL distribution mode of HTTP and set the HTTP URL to `http://4.4.4.133:447/myca.crl`.

After the above configuration, make sure that the system clock of the device is synchronous to that of the CA, so that the device can request certificates and retrieve CRLs properly.

2) Configure the Switch

- Configure the entity DN

Configure the entity name as **aaa** and the common name as **Switch**.

```
<Switch> system-view
[switch] pki entity aaa
[switch-pki-entity-aaa] common-name Switch
[Switch-pki-entity-aaa] quit
```

- Configure the PKI domain

Create PKI domain **torsa** and enter its view.

```
[Switch] pki domain torsa
```

Configure the name of the trusted CA as **myca**.

```
[Switch-pki-domain-torsa] ca identifier myca
```

Configure the URL of the registration server in the format of `http://host:port/Issuing Jurisdiction ID`, where Issuing Jurisdiction ID is a hexadecimal string generated on the CA server.

```
[Switch-pki-domain-torsa] certificate request url
http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337
```

Set the registration authority to **CA**.

```
[Switch-pki-domain-torsa] certificate request from ca
```

Specify the entity for certificate request as **aaa**.

```
[Switch-pki-domain-torsa] certificate request entity aaa
```

Configure the URL for the CRL distribution point.

```
[Switch-pki-domain-torsa] crl url http://4.4.4.133:447/myca.crl
[Switch-pki-domain-torsa] quit
```

- Generate a local key pair using RSA

```
[Switch] public-key local create rsa
```

The range of public key size is (512 ~ 2048).

NOTES: If the key modulus is greater than 512,

It may take a few minutes.

Input the bits in the modulus [default = 1024]:

Generating keys...

```
.....+++++
.....+++++
.....+++++
.....+++++
```

- Apply for certificates

Retrieve the CA certificate and save it locally.

```
[Switch] pki retrieval-certificate ca domain torsa
```

Retrieving CA/RA certificates. Please wait a while.....

The trusted CA's finger print is:

MD5 fingerprint:EDE9 0394 A273 B61A F1B3 0072 A0B1 F9AB

SHA1 fingerprint: 77F9 A077 2FB8 088C 550B A33C 2410 D354 23B2 73A8

Is the finger print correct?(Y/N):y

Saving CA/RA certificates chain, please wait a moment.....

CA certificates retrieval success.

Retrieve CRLs and save them locally.

```
[Switch] pki retrieval-crl domain torsa
```

Connecting to server for retrieving CRL. Please wait a while.....

CRL retrieval success!

Request a local certificate manually.

```
[Switch] pki request-certificate domain torsa challenge-word
```

Certificate is being requested, please wait.....

Certificate request Successfully!

Saving the local certificate to device.....

Done!

3) Verify your configuration

Use the following command to view information about the local certificate acquired.

```
<Switch> display pki certificate local domain torsa
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

9A96A48F 9A509FD7 05FFF4DF 104AD094

Signature Algorithm: sha1WithRSAEncryption

Issuer:

C=cn

O=org

OU=test

CN=myca

Validity

Not Before: Jan 8 09:26:53 2007 GMT

Not After : Jan 8 09:26:53 2008 GMT

Subject:

CN=Switch

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

```
00D67D50 41046F6A 43610335 CA6C4B11
F8F89138 E4E905BD 43953BA2 623A54C0
EA3CB6E0 B04649CE C9CDDD38 34015970
981E96D9 FF4F7B73 A5155649 E583AC61
D3A5C849 CBDE350D 2A1926B7 0AE5EF5E
D1D8B08A DBF16205 7C2A4011 05F11094
73EB0549 A65D9E74 0F2953F2 D4F0042F
19103439 3D4F9359 88FB59F3 8D4B2F6C
2B
```

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 CRL Distribution Points:

URI:http://4.4.4.133:447/myca.crl

Signature Algorithm: sha1WithRSAEncryption

```
836213A4 F2F74C1A 50F4100D B764D6CE
B30C0133 C4363F2F 73454D51 E9F95962
EDE9E590 E7458FA6 765A0D3F C4047BC2
9C391FF0 7383C4DF 9A0CCFA9 231428AF
987B029C C857AD96 E4C92441 9382E798
8FCC1E4A 3E598D81 96476875 E2F86C33
75B51661 B6556C5E 8F546E97 5197734B
C8C29AC7 E427C8E4 B9AAF5AA 80A75B3C
```

You can also use some other **display** commands to view detailed information about the CA certificate and CRLs. Refer to the parts related to **display pki certificate ca domain** and **display pki crl domain** commands in *PKI Commands of the Security Volume*.

Requesting a Certificate from a CA Running Windows 2003 Server



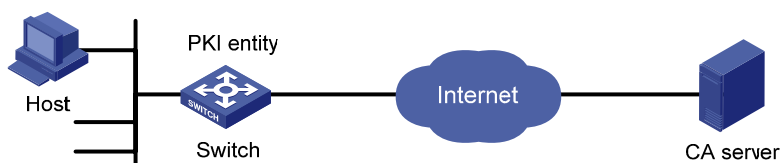
Note

The CA server runs the Windows 2003 server in this configuration example.

Network requirements

Configure PKI entity Switch to request a local certificate from the CA server.

Figure 1-3 Request a certificate from a CA running Windows 2003 server



Configuration procedure

- 1) Configure the CA server
 - Install the certificate server suites

From the start menu, select **Control Panel > Add or Remove Programs**, and then select **Add/Remove Windows Components > Certificate Services** and click **Next** to begin the installation.

- Install the SCEP plug-in

As a CA server running the Windows 2003 server does not support SCEP by default, you need to install the SCEP plug-in so that the Switch can register and obtain its certificate automatically. After the SCEP plug-in installation completes, a URL is displayed, which you need to configure on the switch as the URL of the server for certificate registration.

- Modify the certificate service attributes

From the start menu, select **Control Panel > Administrative Tools > Certificate Authority**. If the CA server and SCEP plug-in have been installed successfully, there should be two certificates issued by the CA to the RA. Right-click on the CA server in the navigation tree and select **Properties > Policy Module**. Click **Properties** and then select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate**.

- Modify the Internet Information Services (IIS) attributes

From the start menu, select **Control Panel > Administrative Tools > Internet Information Services (IIS) Manager** and then select **Web Sites** from the navigation tree. Right-click on **Default Web Site** and select **Properties > Home Directory**. Specify the path for certificate service in the **Local path** text box. In addition, you are recommended to specify an available port number as the TCP port number of the default Web site to avoid conflict with existing services.

After completing the above configuration, check that the system clock of the switch is synchronous to that of the CA server, ensuring that the switch can request a certificate normally.

- 2) Configure the switch
 - Configure the entity DN

Configure the entity name as **aaa** and the common name as **switch**.

```
<Switch> system-view
[Switch] pki entity aaa
[Switch-pki-entity-aaa] common-name switch
[Switch-pki-entity-aaa] quit
```

- Configure the PKI domain

Create PKI domain **torsa** and enter its view.

```
[Switch] pki domain torsa
```

Configure the name of the trusted CA as **myca**.

```
[Switch-pki-domain-torsa] ca identifier myca
```

Configure the URL of the registration server in the format of `http://host:port/certsrv/mscep/mscep.dll`, where `host:port` indicates the IP address and port number of the CA server.

```
[Switch-pki-domain-torsa] certificate request url
http://4.4.4.1:8080/certsrv/mscep/mscep.dll
```

Set the registration authority to **RA**.

```
[Switch-pki-domain-torsa] certificate request from ra
```

Specify the entity for certificate request as **aaa**.

```
[Switch-pki-domain-torsa] certificate request entity aaa
```

- Generate a local key pair using RSA

```
[Switch] public-key local create rsa
```

The range of public key size is (512 ~ 2048).

NOTES: If the key modulus is greater than 512,

It may take a few minutes.

Input the bits in the modulus [default = 1024]:

Generating keys...

.....+++++

.....+++++

.....+++++

.....+++++

.

- Apply for certificates

Retrieve the CA certificate and save it locally.

```
[Switch] pki retrieval-certificate ca domain tora
```

Retrieving CA/RA certificates. Please wait a while.....

The trusted CA's finger print is:

MD5 fingerprint:766C D2C8 9E46 845B 4DCE 439C 1C1F 83AB

SHA1 fingerprint:97E5 DDED AB39 3141 75FB DB5C E7F8 D7D7 7C9B 97B4

Is the finger print correct?(Y/N):y

Saving CA/RA certificates chain, please wait a moment.....

CA certificates retrieval success.

Request a local certificate manually.

```
[Switch] pki request-certificate domain tora challenge-word
```

Certificate is being requested, please wait.....

Certificate request Successfully!

Saving the local certificate to device.....

Done!

3) Verify your configuration

Use the following command to view information about the local certificate acquired.

```
<Switch> display pki certificate local domain tora
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

48FA0FD9 00000000 000C

Signature Algorithm: sha1WithRSAEncryption

Issuer:

CN=CA server

Validity

Not Before: Nov 21 12:32:16 2007 GMT

Not After : Nov 21 12:42:16 2008 GMT

Subject:

CN=switch

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

```
00A6637A 8CDEA1AC B2E04A59 F7F6A9FE
5AEE52AE 14A392E4 E0E5D458 0D341113
0BF91E57 FA8C67AC 6CE8FE8B 5570178B
10242FDD D3947F5E 2DA70BD9 1FAF07E5
1D167CE1 FC20394F 476F5C08 C5067DF9
CB4D05E6 55DC11B6 9F4C014D EA600306
81D403CF 2D93BC5A 8AF3224D 1125E439
78ECEFE1 7FA9AE7B 877B50B8 3280509F
6B
```

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

B68E4107 91D7C44C 7ABCE3BA 9BF385F8 A448F4E1

X509v3 Authority Key Identifier:

keyid:9D823258 EADFEFA2 4A663E75 F416B6F6 D41EE4FE

X509v3 CRL Distribution Points:

URI:http://l00192b/CertEnroll/CA%20server.crl

URI:file://\\l00192b\CertEnroll\CA server.crl

Authority Information Access:

CA Issuers - URI:http://l00192b/CertEnroll/l00192b_CA%20server.crt

CA Issuers - URI:file://\\l00192b\CertEnroll\l00192b_CA server.crt

1.3.6.1.4.1.311.20.2:

.0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.0.f.f.l.i.n.e

Signature Algorithm: sha1WithRSAEncryption

81029589 7BFA1CBD 20023136 B068840B

(Omitted)

You can also use some other **display** commands to view detailed information about the CA certificate. Refer to the **display pki certificate ca domain** command in *PKI Commands of the Security Volume*.

Troubleshooting PKI

Failed to Retrieve a CA Certificate

Symptom

Failed to retrieve a CA certificate.

Analysis

Possible reasons include these:

- The network connection is not proper. For example, the network cable may be damaged or loose.
- No trusted CA is specified.
- The URL of the registration server for certificate request is not correct or not configured.
- No authority is specified for certificate request.
- The system clock of the device is not synchronized with that of the CA.

Solution

- Make sure that the network connection is physically proper.
- Check that the required commands are configured properly.
- Use the **ping** command to check that the RA server is reachable.
- Specify the authority for certificate request.
- Synchronize the system clock of the device with that of the CA.

Failed to Request a Local Certificate

Symptom

Failed to request a local certificate.

Analysis

Possible reasons include these:

- The network connection is not proper. For example, the network cable may be damaged or loose.
- No CA certificate has been retrieved.
- The current key pair has been bound to a certificate.
- No trusted CA is specified.
- The URL of the registration server for certificate request is not correct or not configured.
- No authority is specified for certificate request.
- Some required parameters of the entity DN are not configured.

Solution

- Make sure that the network connection is physically proper.
- Retrieve a CA certificate.
- Regenerate a key pair.
- Specify a trusted CA.
- Use the **ping** command to check that the RA server is reachable.
- Specify the authority for certificate request.
- Configure the required entity DN parameters.

Failed to Retrieve CRLs

Symptom

Failed to retrieve CRLs.

Analysis

Possible reasons include these:

- The network connection is not proper. For example, the network cable may be damaged or loose.
- No CA certificate has been retrieved before you try to retrieve CRLs.
- The IP address of LDAP server is not configured.

- The CRL distribution URL is not configured.
- The LDAP server version is wrong.

Solution

- Make sure that the network connection is physically proper.
- Retrieve a CA certificate.
- Specify the IP address of the LDAP server.
- Specify the CRL distribution URL.
- Re-configure the LDAP version.

Table of Contents

1 SSL Configuration	1-1
SSL Overview	1-1
SSL Security Mechanism	1-1
SSL Protocol Stack	1-2
SSL Configuration Task List	1-2
Configuring an SSL Server Policy	1-2
Configuration Prerequisites	1-3
Configuration Procedure	1-3
SSL Server Policy Configuration Example	1-4
Configuring an SSL Client Policy	1-6
Configuration Prerequisites	1-6
Configuration Procedure	1-6
Displaying and Maintaining SSL	1-7
Troubleshooting SSL	1-7
SSL Handshake Failure	1-7

1 SSL Configuration

When configuring SSL, go to these sections for information you are interested in:

- [SSL Overview](#)
- [SSL Configuration Task List](#)
- [Displaying and Maintaining SSL](#)
- [Troubleshooting SSL](#)

SSL Overview

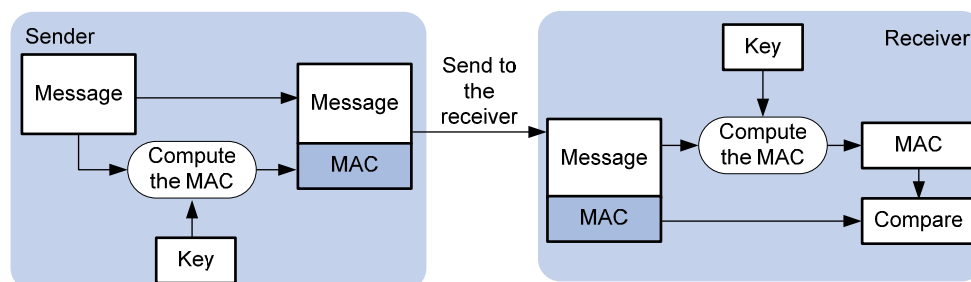
Secure Sockets Layer (SSL) is a security protocol providing secure connection service for TCP-based application layer protocols, for example, HTTP protocol. It is widely used in E-business and online bank fields to provide secure data transmission over the Internet.

SSL Security Mechanism

SSL provides these security services:

- Confidentiality: SSL uses a symmetric encryption algorithm to encrypt data and uses the Rivest, Shamir, and Adelman (RSA) algorithm to encrypt the key to be used by the symmetric encryption algorithm.
- Authentication: SSL supports certificate-based authentication of the server and the client by using the digital signatures, with the authentication of the client being optional. The SSL server and client obtain certificates from a certificate authority (CA) through the Public Key Infrastructure (PKI).
- Reliability: SSL uses the key-based message authentication code (MAC) to verify message integrity. A MAC algorithm transforms a message of any length to a fixed-length message. [Figure 1-1](#) illustrates how SSL uses a MAC algorithm to verify message integrity. With the key, the sender uses the MAC algorithm to compute the MAC value of a message. Then, the sender suffixes the MAC value to the message and sends the result to the receiver. The receiver uses the same key and MAC algorithm to compute the MAC value of the received message, and compares the locally computed MAC value with that received. If the two matches, the receiver considers the message intact; otherwise, the receiver considers the message tampered and discards the message.

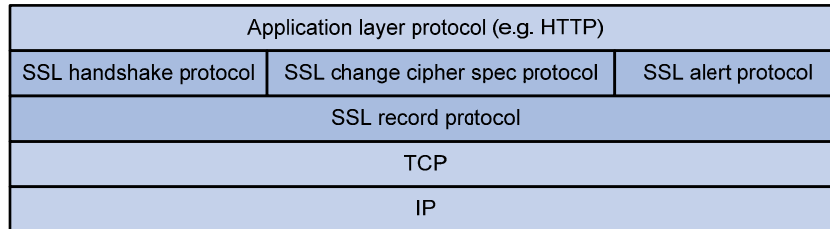
Figure 1-1 Message integrity verification by a MAC algorithm



SSL Protocol Stack

As shown in [Figure 1-2](#), the SSL protocol consists of two layers of protocols: the SSL record protocol at the lower layer and the SSL handshake protocol, change cipher spec protocol, and alert protocol at the upper layer.

Figure 1-2 SSL protocol stack



- **SSL handshake protocol:** As a very important part of the SSL protocol stack, it is responsible for negotiating the cipher suite to be used during communication (including the symmetric encryption algorithm, key exchange algorithm, and MAC algorithm), exchanging the key between the server and client, and implementing identity authentication of the server and client. Through the SSL handshake protocol, a session is established between a client and the server. A session consists of a set of parameters, including the session ID, peer certificate, cipher suite, and master secret.
- **SSL change cipher spec protocol:** Used for notification between a client and the server that the subsequent packets are to be protected and transmitted based on the newly negotiated cipher suite and key.
- **SSL alert protocol:** Allowing a client and the server to send alert messages to each other. An alert message contains the alert severity level and a description.
- **SSL record protocol:** Fragmenting data to be transmitted, computing and adding MAC to the data, and encrypting the data before transmitting it to the peer end.

SSL Configuration Task List

Different parameters are required on the SSL server and the SSL client.

Complete the following tasks to configure SSL:

Task	Remarks
Configuring an SSL Server Policy	Required
Configuring an SSL Client Policy	Optional

Configuring an SSL Server Policy

An SSL server policy is a set of SSL parameters for a server to use when booting up. An SSL server policy takes effect only after it is associated with an application layer protocol, HTTP protocol, for example.

Configuration Prerequisites

When configuring an SSL server policy, you need to specify the PKI domain to be used for obtaining the server side certificate. Therefore, before configuring an SSL server policy, you must configure a PKI domain.

Configuration Procedure

Follow these steps to configure an SSL server policy:

To do...	Use the command...	Remarks
Enter system view	system-view	—
Create an SSL server policy and enter its view	ssl server-policy <i>policy-name</i>	Required
Specify a PKI domain for the SSL server policy	pki-domain <i>domain-name</i>	Required By default, no PKI domain is specified for an SSL server policy.
Specify the cipher suite(s) for the SSL server policy to support	ciphersuite [<i>rsa_3des_edc_cbc_sha</i> <i>rsa_aes_128_cbc_sha</i> <i>rsa_aes_256_cbc_sha</i> <i>rsa_des_cbc_sha</i> <i>rsa_rc4_128_md5</i> <i>rsa_rc4_128_sha</i>] *	Optional By default, an SSL server policy supports all cipher suites.
Set the handshake timeout time for the SSL server	handshake timeout <i>time</i>	Optional 3,600 seconds by default
Configure the SSL connection close mode	close-mode <i>wait</i>	Optional Not wait by default
Set the maximum number of cached sessions and the caching timeout time	session { <i>cachesize size</i> <i>timeout time</i> } *	Optional The defaults are as follows: 500 for the maximum number of cached sessions, 3600 seconds for the caching timeout time.
Enable certificate-based SSL client authentication	client-verify <i>enable</i>	Optional Not enabled by default

Note

- If you enable client authentication here, you must request a local certificate for the client.
 - Currently, SSL mainly comes in these versions: SSL 2.0, SSL 3.0, and TLS 1.0, where TLS 1.0 corresponds to SSL 3.1. When the device acts as an SSL server, it can communicate with clients running SSL 3.0 or TLS 1.0, and can identify Hello packets from clients running SSL 2.0. If a client running SSL 2.0 also supports SSL 3.0 or TLS 1.0 (information about supported versions is carried in the packet that the client sends to the server), the server will notify the client to use SSL 3.0 or TLS 1.0 to communicate with the server.
-

SSL Server Policy Configuration Example

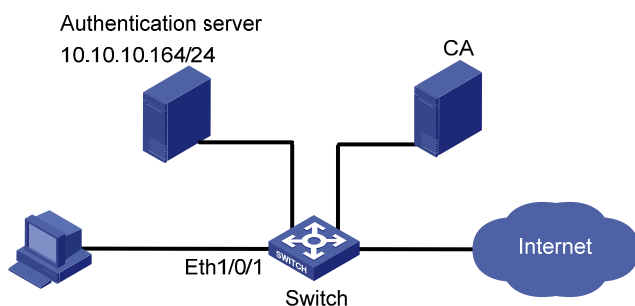
Network requirements

- The switch offers Web authentication to preform access authentication for clients.
 - The client opens the authentication page in SSL-based HTTPS mode, thus guaranteeing information transmission security.
 - A CA issues a certificate to Switch.
-

Caution

In this instance, Windows Server works as the CA and the Simple Certificate Enrollment Protocol (SCEP) plug-in is installed on the CA.

Figure 1-3 Network diagram for SSL server policy configuration



Configuration procedure

- 1) Request a certificate for Switch
- # Create a PKI entity named **en** and configure it.
- ```
<Switch> system-view
[Switch] pki entity en
[Switch-pki-entity-en] common-name http-server1
[Switch-pki-entity-en] fqdn ssl.security.com
```

```

[Switch-pki-entity-en] quit

Create a PKI domain and configure it.

[Switch] pki domain 1
[Switch-pki-domain-1] ca identifier ca1
[Switch-pki-domain-1] certificate request url http://10.1.2.2/certsrv/mscep/mscep.dll
[Switch-pki-domain-1] certificate request from ra
[Switch-pki-domain-1] certificate request entity en
[Switch-pki-domain-1] quit

Create the local RSA key pairs.

[Switch] public-key local create rsa

Retrieve the CA certificate.

[Switch] pki retrieval-certificate ca domain 1

Request a local certificate.

[Switch] pki request-certificate domain 1

2) Configure an SSL server policy

Create an SSL server policy named myssl.

[Switch] ssl server-policy myssl

Specify the PKI domain for the SSL server policy as 1.

[Switch-ssl-server-policy-myssl] pki-domain 1

Enable client authentication.

[Switch-ssl-server-policy-myssl] client-verify enable
[Switch-ssl-server-policy-myssl] quit

3) Configure Web authentication

Set the IP address and port number of the Web authentication server.

<Sysname> system-view
[Sysname] web-authentication web-server ip 10.10.10.10 port 8080

Configure to perform Web authentication in HTTPS mode using SSL server policy myssl.

[Switch] web-authentication protocol https server-policy myssl

Enable Web authentication on Ethernet1/0/1 and set the user access method to designated.

[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] web-authentication select method designated

Create RADIUS scheme radius1 and enter its view.

[Sysname] radius scheme radius1

Set the IP address of the primary RADIUS authentication server.

[Sysname-radius-radius1] primary authentication 10.10.10.164

Enable accounting optional.

[Sysname-radius-radius1] accounting optional

Set the password that will be used to encrypt the messages exchanged between the switch and the RADIUS authentication server.

[Sysname -radius-radius1] key authentication expert

```

# Configure the system to strip domain name off a user name before transmitting the user name to the RADIUS server.

```
[Sysname-radius-radius1] user-name-format without-domain
[Sysname-radius-radius1] quit
```

# Create ISP domain aabbcc.net for Web authentication users and enter the domain view.

```
[Sysname] domain aabbcc.net
```

# Configure domain aabbcc.net as the default user domain.

```
[Sysname] domain default enable aabbcc.net
```

# Reference scheme radius1 in domain aabbcc.net.

```
[Sysname-isp-aabbcc.net] scheme radius-scheme radius1
```

# Enable Web authentication globally. (It is recommended to take this step as the last step, so as to avoid the case that a valid user cannot access the network due to that some other related configurations are not finished.)

```
[Sysname] web-authentication enable
```

Now, Web authentication takes effect. Before the user passes the Web authentication, it cannot access external networks and can only access the free resource.

The user can perform the following steps to access the Internet:

Step 1: Enter `http://10.10.10.10:8080` in the address column of IE.

Step 2: Enter the correct user name and password and then click [login]. The following page will be displayed: "Authentication passed!".

Now the user can access external networks.

## Configuring an SSL Client Policy

An SSL client policy is a set of SSL parameters for a client to use when connecting to the server. An SSL client policy takes effect only after it is associated with an application layer protocol.

### Configuration Prerequisites

If the SSL server is configured to authenticate the SSL client, when configuring the SSL client policy, you need to specify the PKI domain to be used for obtaining the certificate of the client. Therefore, before configuring an SSL client policy, you must configure a PKI domain.

### Configuration Procedure

Follow these steps to configure an SSL client policy:

| To do...                                       | Use the command...                          | Remarks                                             |
|------------------------------------------------|---------------------------------------------|-----------------------------------------------------|
| Enter system view                              | <b>system-view</b>                          | —                                                   |
| Create an SSL client policy and enter its view | <b>ssl client-policy</b> <i>policy-name</i> | Required                                            |
| Specify a PKI domain for the SSL client policy | <b>pki-domain</b> <i>domain-name</i>        | Optional<br>No PKI domain is configured by default. |

| To do...                                                     | Use the command...                                                                                                                                                                                          | Remarks                                       |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Specify the preferred cipher suite for the SSL client policy | <b>prefer-cipher</b><br>{ <b>rsa_3des_edc_cbc_sha</b>  <br><b>rsa_aes_128_cbc_sha</b>  <br><b>rsa_aes_256_cbc_sha</b>  <br><b>rsa_des_cbc_sha</b>  <br><b>rsa_rc4_128_md5</b>  <br><b>rsa_rc4_128_sha</b> } | Optional<br><b>rsa_rc4_128_md5</b> by default |
| Specify the SSL protocol version for the SSL client policy   | <b>version</b> { <b>ssl3.0</b>   <b>tls1.0</b> }                                                                                                                                                            | Optional<br>TLS 1.0 by default                |



#### Note

If you enable client authentication on the server, you must request a local certificate for the client.

## Displaying and Maintaining SSL

| To do...                              | Use the command...                                                      | Remarks               |
|---------------------------------------|-------------------------------------------------------------------------|-----------------------|
| Display SSL server policy information | <b>display ssl server-policy</b><br>{ <i>policy-name</i>   <b>all</b> } | Available in any view |
| Display SSL client policy information | <b>display ssl client-policy</b><br>{ <i>policy-name</i>   <b>all</b> } |                       |

## Troubleshooting SSL

### SSL Handshake Failure

#### Symptom

As the SSL server, the device fails to handshake with the SSL client.

#### Analysis

SSL handshake failure may result from the following causes:

- No SSL server certificate exists, or the certificate is not trusted.
- The server is expected to authenticate the client, but the SSL client has no certificate or the certificate is not trusted.
- The cipher suites used by the server and the client do not match.

#### Solution

- 1) You can issue the **debugging ssl** command and view the debugging information to locate the problem:
  - If the SSL server has no certificate, request one for it.
  - If the server certificate cannot be trusted, install on the SSL client the root certificate of the CA that issues the local certificate to the SSL server, or let the server requests a certificate from the CA that the SSL client trusts.

- If the SSL server is configured to authenticate the client, but the certificate of the SSL client does not exist or cannot be trusted, request and install a certificate for the client.
- 2) You can use the **display ssl server-policy** command to view the cipher suite used by the SSL server policy. If the cipher suite used by the SSL server does not match that used by the client, use the **ciphersuite** command to modify the cipher suite of the SSL server.

# Table of Contents

|                                                                                       |            |
|---------------------------------------------------------------------------------------|------------|
| <b>1 HTTPS Configuration .....</b>                                                    | <b>1-1</b> |
| HTTPS Overview .....                                                                  | 1-1        |
| HTTPS Configuration Task List .....                                                   | 1-1        |
| Associating the HTTPS Service with an SSL Server Policy .....                         | 1-2        |
| Enabling the HTTPS Service .....                                                      | 1-2        |
| Associating the HTTPS Service with a Certificate Attribute Access Control Policy..... | 1-3        |
| Associating the HTTPS Service with an ACL .....                                       | 1-3        |
| Displaying and Maintaining HTTPS .....                                                | 1-3        |
| HTTPS Configuration Example .....                                                     | 1-4        |



# 1 HTTPS Configuration

---

When configuring HTTPS, go to these sections for information you are interested in:

- [HTTPS Overview](#)
- [HTTPS Configuration Task List](#)
- [Associating the HTTPS Service with an SSL Server Policy](#)
- [Enabling the HTTPS Service](#)
- [Associating the HTTPS Service with a Certificate Attribute Access Control Policy](#)
- 
- [Associating the HTTPS Service with an ACL](#)
- [Displaying and Maintaining HTTPS](#)
- [HTTPS Configuration Example](#)

## HTTPS Overview

The Secure HTTP (HTTPS) refers to the HTTP protocol that supports the Security Socket Layer (SSL) protocol.

The SSL protocol of HTTPS enhances the security of the device in the following ways:

- Uses the SSL protocol to ensure the legal clients to access the device securely and prohibit the illegal clients;
- Encrypts the data exchanged between the HTTPS client and the device to ensure the data security and integrity, thus realizing the security management of the device;
- Defines certificate attribute-based access control policy for the device to control the access right of the client, in order to further avoid attacks from illegal clients.



### Note

- The total number of HTTP connections and HTTPS connections on a device cannot exceed ten.
  - For SSL details, refer to *SSL Configuration*.
- 

## HTTPS Configuration Task List

Complete these tasks to configure HTTPS:

| Configuration task                                                                               | Remarks  |
|--------------------------------------------------------------------------------------------------|----------|
| <a href="#">Associating the HTTPS Service with an SSL Server Policy</a>                          | Required |
| <a href="#">Enabling the HTTPS Service</a>                                                       | Required |
| <a href="#">Associating the HTTPS Service with a Certificate Attribute Access Control Policy</a> | Optional |
| <a href="#">Associating the HTTPS Service with an ACL</a>                                        | Optional |

## Associating the HTTPS Service with an SSL Server Policy

You need to associate the HTTPS service with a created SSL server policy before enabling the HTTPS service.

Follow these steps to associate the HTTPS service with an SSL server policy:

| To do...                                              | Use the command...                                      | Remarks                               |
|-------------------------------------------------------|---------------------------------------------------------|---------------------------------------|
| Enter system view                                     | <b>system-view</b>                                      | —                                     |
| Associate the HTTPS service with an SSL server policy | <b>ip https ssl-server-policy</b><br><i>policy-name</i> | Required<br>Not associated by default |



### Note

- If the **ip https ssl-server-policy** command is executed repeatedly, the HTTPS service is only associated with the last specified SSL server policy.
- When the HTTPS service is enabled, no modification of its associated SSL server policy takes effect.

## Enabling the HTTPS Service

The device can act as the HTTPS server and users can access and control the device through the Web function only when the HTTPS service is enabled.

Follow these steps to enable the HTTPS service:

| To do...                 | Use the command...     | Remarks                          |
|--------------------------|------------------------|----------------------------------|
| Enter system view        | <b>system-view</b>     | —                                |
| Enable the HTTPS service | <b>ip https enable</b> | Required<br>Disabled by default. |



### Note

- After the HTTPS service is enabled, you can use the **display ip https** command to view the state of the HTTPS service and verify the configuration.
- Enabling of the HTTPS service will trigger an SSL handshake negotiation process. During the process, if the local certificate of the device already exists, the SSL negotiation is successfully performed, and the HTTPS service can be started normally. If no local certificate exists, a certificate application process will be triggered by the SSL negotiation. Since the application process takes much time, the SSL negotiation may fail and the HTTPS service cannot be started normally. Therefore, the **ip https enable** command must be executed for multiple times to ensure normal startup of the HTTPS service.

## Associating the HTTPS Service with a Certificate Attribute Access Control Policy

Associating the HTTPS service with a configured certificate access control policy helps control the access right of the client, thus providing the device with enhanced security.

Follow these steps to associate the HTTPS service with a certificate attribute access control policy:

| To do...                                                                       | Use the command...                                                      | Remarks                                |
|--------------------------------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------------|
| Enter system view                                                              | <b>system-view</b>                                                      | —                                      |
| Associate the HTTPS service with a certificate attribute access control policy | <b>ip https certificate access-control-policy</b><br><i>policy-name</i> | Required<br>Not associated by default. |



### Note

- If the **ip https certificate access-control-policy** command is executed repeatedly, the HTTPS server is only associated with the last specified certificate attribute access control policy.
- If the HTTPS service is associated with a certificate attribute access control policy, the **client-verify enable** command must be configured in the SSL server policy. Otherwise, the client cannot log onto the device.
- If the HTTPS service is associated with a certificate attribute access control policy, the latter must contain at least one **permit** rule. Otherwise, no HTTPS client can log onto the device.

## Associating the HTTPS Service with an ACL

Associating the HTTPS service with an ACL can filter out requests from some clients to let pass only clients that pass the ACL filtering.

Follow these steps to associate the HTTPS service with an ACL:

| To do...                                | Use the command...                    | Remarks                                |
|-----------------------------------------|---------------------------------------|----------------------------------------|
| Enter system view                       | <b>system-view</b>                    | —                                      |
| Associate the HTTPS service with an ACL | <b>ip https acl</b> <i>acl-number</i> | Required<br>Not associated by default. |

## Displaying and Maintaining HTTPS

| To do...                        | Use the command...      | Remarks               |
|---------------------------------|-------------------------|-----------------------|
| Display information about HTTPS | <b>display ip https</b> | Available in any view |

# HTTPS Configuration Example

## Network requirements

- Host acts as the HTTPS client and Device acts as the HTTPS server.
- Host accesses Device through Web to control Device.
- CA (Certificate Authority) issues certificate to Device. The common name of CA is **new-ca**.

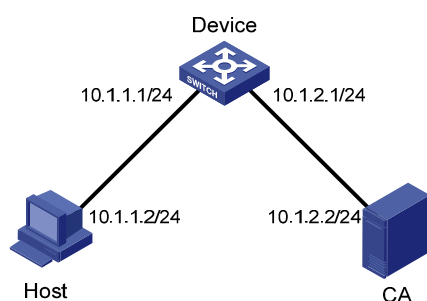


### Caution

In this configuration example, Windows Server serves as CA and you need to install Simple Certificate Enrollment Protocol (SCEP) component.

---

**Figure 1-1** Network diagram for HTTPS configuration



## Configuration procedure

Perform the following configurations on Device:

1) Apply for a certificate for Device

# Configure a PKI entity.

```
<Device> system-view
[Device] pki entity en
[Device-pki-entity-en] common-name http-server1
[Device-pki-entity-en] fqdn ssl.security.com
[Device-pki-entity-en] quit
```

# Configure a PKI domain.

```
[Device] pki domain 1
[Device-pki-domain-1] ca identifier new-ca
[Device-pki-domain-1] certificate request url http://10.1.2.2:8080/certsrv/mscep/mscep.dll
[Device-pki-domain-1] certificate request from ra
[Device-pki-domain-1] certificate request entity en
[Device-pki-domain-1] quit
```

# Generate a local RSA key pair.

```
[Device] public-key local create rsa
```

# Obtain a server certificate from CA.

```
[Device] pki retrieval-certificate ca domain 1
```

# Apply for a local certificate.

```
[Device] pki request-certificate domain 1
```

2) Configure an SSL server policy associated with the HTTPS service

# Configure an SSL server policy.

```
[Device] ssl server-policy myssl
```

```
[Device-ssl-server-policy-myssl] pki-domain 1
```

```
[Device-ssl-server-policy-myssl] client-verify enable
```

```
[Device-ssl-server-policy-myssl] quit
```

3) Configure a certificate access control policy

# Configure a certificate attribute group.

```
[Device] pki certificate attribute-group mygroup1
```

```
[Device-cert-attribute-group-mygroup1] attribute 1 issuer-name dn ctn new-ca
```

```
[Device-cert-attribute-group-mygroup1] quit
```

# Configure certificate access control policy **myacp** and create a control rule.

```
[Device] pki certificate access-control-policy myacp
```

```
[Device-pki-cert-acp-myacp] rule 1 permit mygroup1
```

```
[Device-pki-cert-acp-myacp] quit
```

4) Reference an SSL server policy

# Associate the HTTPS service with the SSL server policy **myssl**.

```
[Device] ip https ssl-server-policy myssl
```

5) Associate the HTTPS service with a certificate attribute access control policy

# Associate the HTTPS service with certificate attribute access control policy **myacp**.

```
[Device] ip https certificate access-control-policy myacp
```

6) Enable the HTTPS service

# Enable the HTTPS service.

```
[Device] ip https enable
```

7) Verify the configuration

Launch the IE explorer on Host, and enter https://10.1.1.1. You can log in to Device and control it.



#### Note

- The URL of the HTTPS server starts with https://,
  - For details of PKI commands, refer to *PKI Commands*.
  - For details of SSL commands, refer to *SSL Commands*.
-

# Table of Contents

|                         |            |
|-------------------------|------------|
| <b>1 Acronyms .....</b> | <b>1-1</b> |
|-------------------------|------------|

# 1 Acronyms

---

| Acronyms | Full spelling                                |
|----------|----------------------------------------------|
| <b>A</b> |                                              |
| 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>B</b> |                                              |
| BDR      | Backup Designated Router                     |
| <b>C</b> |                                              |
| CAR      | Committed Access Rate                        |
| CLI      | Command Line Interface                       |
| CoS      | Class of Service                             |
| <b>D</b> |                                              |
| DHCP     | Dynamic Host Configuration Protocol          |
| DR       | Designated Router                            |
| D-V      | Distance Vector Routing Algorithm            |
| <b>E</b> |                                              |
| EGP      | Exterior Gateway Protocol                    |
| <b>F</b> |                                              |
| FTP      | File Transfer Protocol                       |
| <b>G</b> |                                              |
| GARP     | Generic Attribute Registration Protocol      |
| GE       | Gigabit Ethernet                             |
| GVRP     | GARP VLAN Registration Protocol              |
| GMRP     | GARP Multicast Registration Protocol         |
| <b>H</b> |                                              |
| HGMP     | Huawei Group Management Protocol             |
| <b>I</b> |                                              |
| IAB      | Internet Architecture Board                  |
| ICMP     | Internet Control Message Protocol            |

| Acronyms | Full spelling                                    |
|----------|--------------------------------------------------|
| IGMP     | Internet Group Management Protocol               |
| IGP      | Interior Gateway Protocol                        |
| IP       | Internet Protocol                                |
| IRF      | Intelligent Resilient Framework                  |
| <b>L</b> |                                                  |
| LSA      | Link State Advertisement                         |
| LSDB     | Link State DataBase                              |
| <b>M</b> |                                                  |
| MAC      | Medium Access Control                            |
| MIB      | Management Information Base                      |
| <b>N</b> |                                                  |
| NBMA     | Non Broadcast MultiAccess                        |
| NIC      | Network Information Center                       |
| NMS      | Network Management System                        |
| NVRAM    | Nonvolatile RAM                                  |
| <b>O</b> |                                                  |
| OSPF     | Open Shortest Path First                         |
| <b>P</b> |                                                  |
| PIM      | Protocol Independent Multicast                   |
| PIM-DM   | Protocol Independent Multicast-Dense Mode        |
| PIM-SM   | Protocol Independent Multicast-Sparse Mode       |
| PoE      | Power over Ethernet                              |
| <b>Q</b> |                                                  |
| QoS      | Quality of Service                               |
| <b>R</b> |                                                  |
| RIP      | Routing Information Protocol                     |
| RMON     | Remote Network Monitoring                        |
| RSTP     | Rapid Spanning Tree Protocol                     |
| <b>S</b> |                                                  |
| SNMP     | Simple Network Management Protocol               |
| SP       | Strict Priority                                  |
| STP      | Spanning Tree Protocol                           |
| <b>T</b> |                                                  |
| TCP/IP   | Transmission Control Protocol/ Internet Protocol |
| TFTP     | Trivial File Transfer Protocol                   |



| Acronyms | Full spelling                      |
|----------|------------------------------------|
| ToS      | Type of Service                    |
| TTL      | Time To Live                       |
| <b>U</b> |                                    |
| UDP      | User Datagram Protocol             |
| <b>V</b> |                                    |
| VLAN     | Virtual LAN                        |
| VOD      | Video On Demand                    |
| VRRP     | Virtual Router Redundancy Protocol |
| <b>W</b> |                                    |
| WRR      | Weighted Round Robin               |
| <b>X</b> |                                    |
| XID      | Exchange Identification            |